

Power BI enterprise

Leverage the Power BI platform enterprise features and capabilities.

Power BI Premium Gen2

OVERVIEW

[Introducing Power BI Premium Gen2](#)

[Power BI Premium features](#)

CONCEPT

[Power BI Premium Gen2 architecture](#)

[Managing Premium Gen2 capacities](#)

[Power BI for US government](#)

HOW-TO GUIDE

[Use the Premium utilization and metrics app](#)

[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 with Power BI](#)

[Bring your own encryption keys](#)

Automation tools

REFERENCE

[Service principal authentication for read-only admin APIs](#)

[PowerShell cmdlets, REST APIs, and .NET Client library](#)

Automatic aggregations

Article • 12/01/2022 • 18 minutes to read

Automatic aggregations use state-of-the-art machine learning (ML) to continuously optimize DirectQuery datasets 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 dataset owners of any skill level to improve query performance, providing faster report visualizations for even the largest datasets.

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 cannot be 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 - Dataset owners can enable automatic aggregations training and schedule one or more refreshes for the dataset. With the first training and refresh, automatic aggregations begins 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 dataset 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 for your environment.

Requirements

Supported plans

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

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 datasets. Composite model datasets with both import tables and DirectQuery connections are supported, however automatic aggregations are supported for the DirectQuery connection only.

Permissions

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

Configuring automatic aggregations

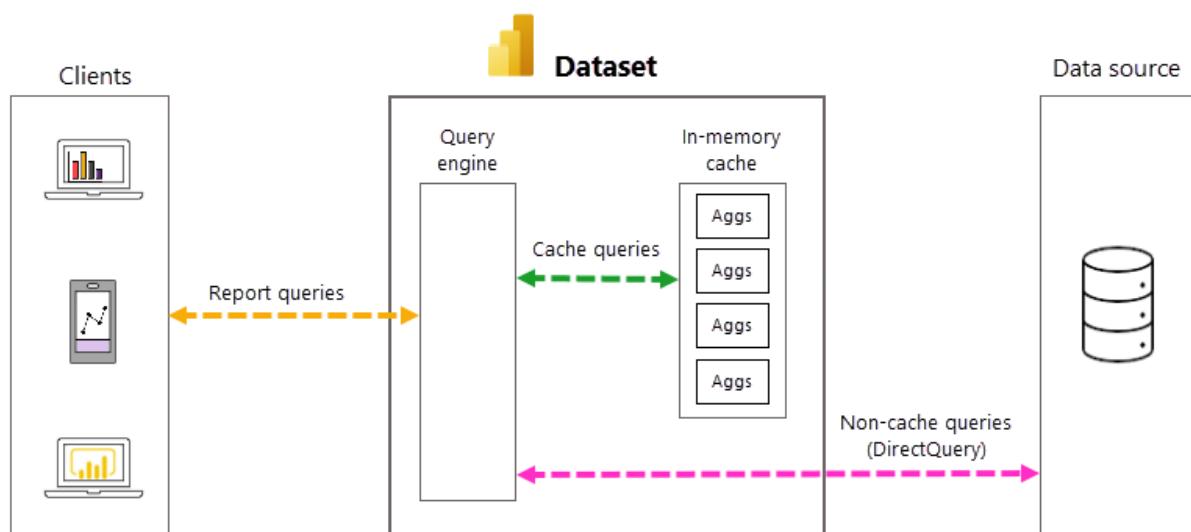
Automatic aggregations are configured in dataset Settings. Configuring is simple - enable automatic aggregations training and schedule one or more refreshes. But before you configure automatic aggregations for your dataset, be sure to entirely read through this article. It provides a good understanding 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 dataset user opens a report or interacts with a report visualization, DAX queries are passed to the query engine and then on to the backend data source as SQL queries. The data source must then calculate and return results for

each query. Compared to import mode datasets 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 dataset, 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 is not 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 aggregations 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

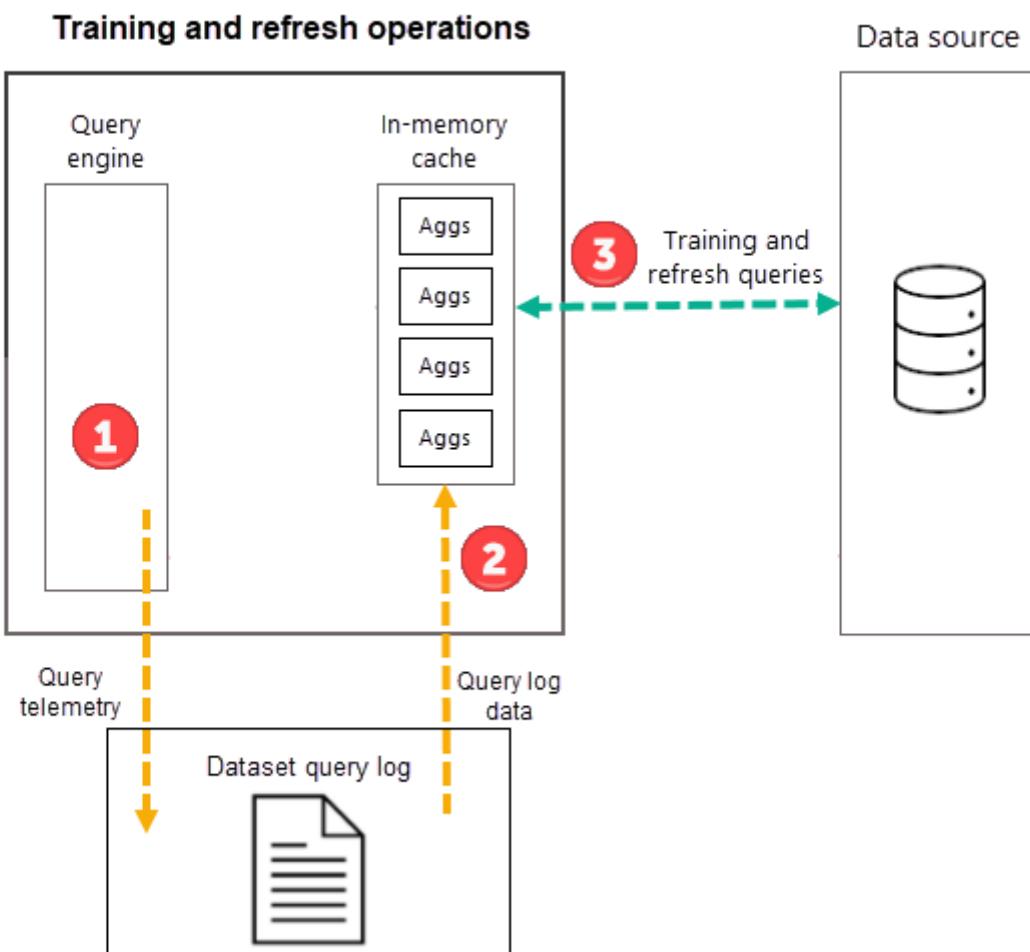
Power BI tracks dataset and user report queries in a query log. For each dataset, Power BI maintains seven days of query log data. Query log data is rolled forward each day.

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

Training operations

As part of the first scheduled dataset 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 aggregations 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, is not 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 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.



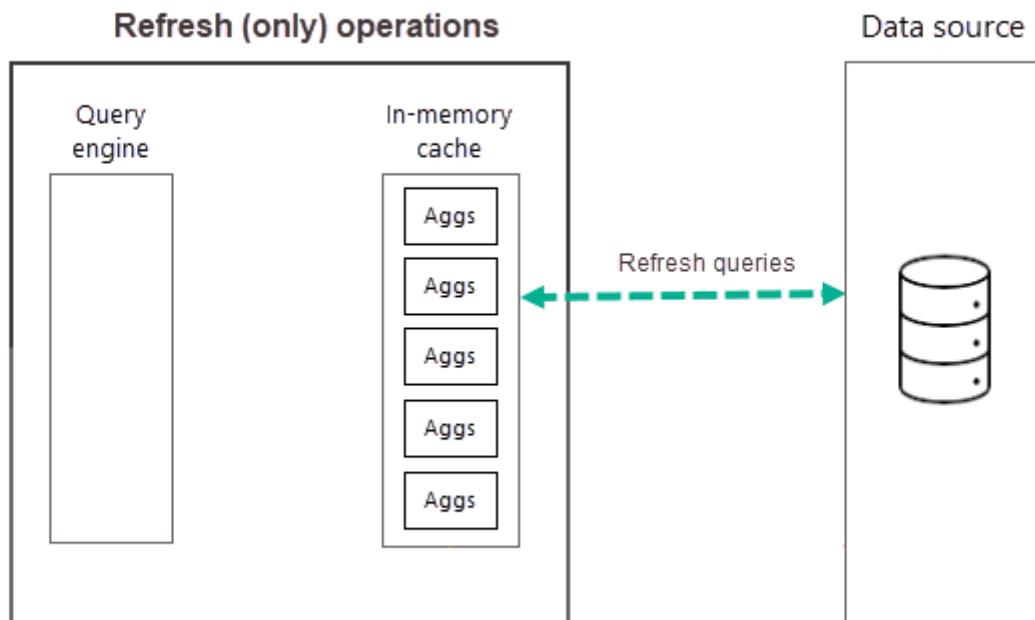
While training operations evaluate past queries from the query log, the results are sufficiently accurate to ensure future queries are covered. There is no guarantee

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 dataset Refresh history and training resumes the next time it is launched. The training cycle completes and replaces the existing automatic aggregations when the entire query log is processed.

Refresh operations

As described above, 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. Using our example above, 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 dataset

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 clicking on **Train and Refresh Now** in dataset Settings. Using **Train and Refresh Now** triggers both a training operation and a refresh operation. Check the dataset Refresh history to see if the current operation is finished before running an additional on-demand training and refresh operation, if necessary.

Refresh history

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

Refresh history

[Scheduled](#) [OneDrive](#)

Show	Scheduled	6/26/2021, 6:30:00 PM	6/26/2021, 6:31:58 PM	Completed	62.766 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/25/2021, 6:30:00 PM	6/25/2021, 6:32:06 PM	Completed	62.766 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/24/2021, 6:30:01 PM	6/24/2021, 6:32:56 PM	Completed	62.792 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/23/2021, 6:30:00 PM	6/23/2021, 6:32:26 PM	Completed	62.784 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/22/2021, 6:30:00 PM	6/22/2021, 6:32:09 PM	Completed	62.84 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/21/2021, 6:30:00 PM	6/21/2021, 6:32:09 PM	Completed	62.847 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/20/2021, 6:30:01 PM	6/20/2021, 6:31:20 PM	Completed	0 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/19/2021, 6:30:01 PM	6/19/2021, 6:30:51 PM	Completed	0 MB of aggregations created with 100% coverage of queries	
Show	Scheduled	6/18/2021, 6:30:00 PM	6/18/2021, 6:31:42 PM	Completed	62.86 MB of aggregations created with 100% coverage of queries	

[Close](#)

By regularly checking 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 dataset refresh for the day or week frequency you choose, these operations are implemented as separate transactions. If a training operation cannot 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 dataset without any aggregations.

Refresh history

Scheduled OneDrive

Details	Type	Start	End	Status	Message
Show	Scheduled	6/23/2021, 6:30:00 PM	6/23/2021, 6:32:26 PM	Partially completed	Refresh succeeded and training failed
Show	Scheduled	6/22/2021, 6:30:00 PM	6/22/2021, 6:32:09 PM	Completed	62.84 MB of aggregations created with 100% coverage of queries
Show	Scheduled	6/21/2021, 6:30:00 PM	6/21/2021, 6:32:09 PM	Completed	62.847 MB of aggregations created with 100% coverage of queries
Show	Scheduled	6/20/2021, 6:30:01 PM	6/20/2021, 6:31:20 PM	Completed	0 MB of aggregations created with 100% coverage of queries

[Close](#)

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 dataset 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 dataset refresh is marked as Failed because the result is an unavailable in-memory aggregations cache.

When scheduling refresh, you can specify email notifications in case of refresh failures.

User-defined and automatic aggregations

[User-defined aggregations](#) in Power BI can be manually configured based on hidden aggregated tables in the dataset. 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, datasets 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 dataset. 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 dataset. Both user-defined and automatic aggregations are refreshed with dataset 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 dataset 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 dataset, but it's likely not necessary.

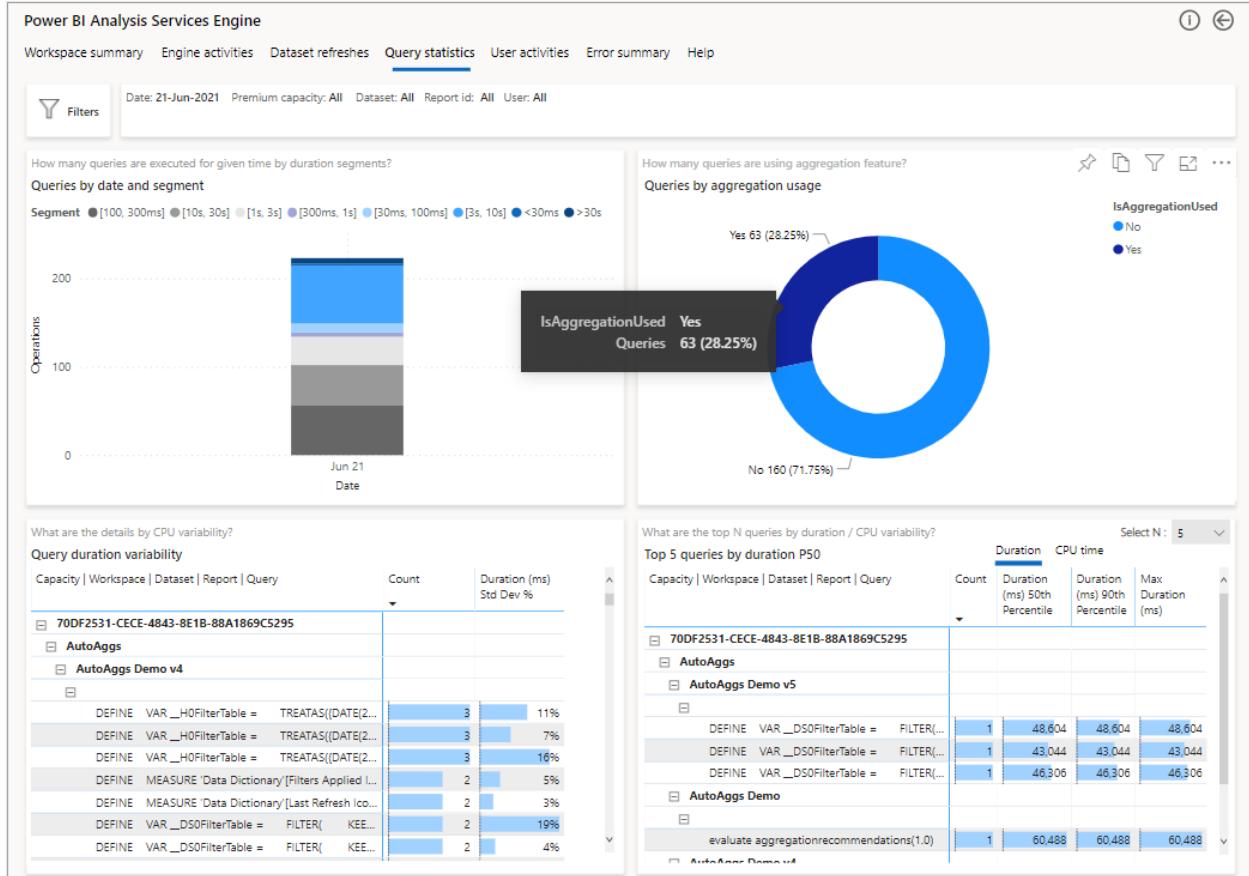
Monitor with Azure Log Analytics

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 from [here](#) and connect it to your log analytics account, as described in this [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 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**.

Power BI Analysis Services Engine | Query history

Workspace summary Engine activities Dataset refreshes Query statistics User activities Error summary Help

Date: 21-Jun-2021

Filters

What are the query execution details?

Query executions (4)

Start Date/Time	CPU Time (ms)	Duration (ms)	SE Duration (ms)	FE Duration (ms)	Is Aggregation Used	User	Executing User	Application	Dataset
21-Jun-21 2:48:49 PM	156	4,064		4,064	●	priyan@contoso.com	priyan@contoso.com	AutoAggs Demo	
21-Jun-21 2:49:42 PM	125	5,065		5,065	●	priyan@contoso.com	priyan@contoso.com	AutoAggs Demo	
21-Jun-21 2:55:39 PM	125	5,301		5,301	●	priyan@contoso.com	priyan@contoso.com	AutoAggs Demo	
21-Jun-21 2:57:56 PM	172	6,799		6,799	●	priyan@contoso.com	priyan@contoso.com	AutoAggs Demo	

4 Total Executions

391 CPU Time P50

438 CPU Time P90

5,183 Duration P50

6,350 Duration P90

(Blank) Aggregation hit %

What is duration/CPU time for given date?

Duration (ms) by date and time

Is Aggregation Used — No

Event Text

```
DEFINE VAR _H0FilterTable = TREATAS([DATE(2020, 10, 1)], 'Calendar'[Fiscal Month])
VAR __DSOFilterTable = FILTER(KEEPFILTERS(VALUES('Segment'[Field Summary Segment])), AND([NOT('Segment'[Field Summary Segment] IN ('SM&C SMB')), 'Segment'[Field Summary Segment] IN ('Enterprise Commercial', 'Enterprise Growth', 'Enterprise Public Sector', 'SM&C Corporate', 'SM&C SMB')))) VAR __DSOFilterTable2 = TREATAS([FY21-Q1, FY21-Q2, FY21-Q3], 'Calendar'[Fiscal Quarter]) VAR __DSOFilterTable3 = TREATAS(['Area Fct'], Forecast Type [Forecast Type]) VAR __DSOFilterTable4 = TREATAS(['APAC', 'Australia', 'Canada', 'Central and Eastern Europe', 'Japan', 'Latam', 'MEA', 'UK', 'United States', 'Western Europe', 'India', 'Greater China', 'Germany', 'France'], Geography [Area]) VAR __DSOFilterTable5 = TREATAS(['Field', 'Services', 'Stores', 'Field'], Business [Business Summary]) VAR __DSOFilterTable6 = TREATAS(['End Customer'], Perspective [Perspective]) VAR __DSOFilterTable7 = TREATAS(['CY', 'CY+1', 'CY-1'], Calendar [Relative Year]) VAR __DSOFilterTable8 = TREATAS(['N/A', 'Scheduled'], Future Flag [Future Flag]) VAR __DSOFilterTable9 = TREATAS(['N/A + Other'], ACR Adjustment Type [ACR Adjustment Type Group]) VAR __DSOCore = SUMMARIZECOLUMNS( Pricing Level [Pricing Level], <DSOFilterTable1>, <DSOFilterTable2>, <DSOFilterTable3>, <DSOFilterTable4>, <DSOFilterTable5>, <DSOFilterTable6>, <DSOFilterTable7>, <DSOFilterTable8>, <DSOFilterTable9> )
```

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

Power BI Analysis Services Engine | Query detail

Workspace summary Engine activities Dataset refreshes Query statistics User activities Error summary Help

Date: 21-Jun-2021

Filters

What are the query details?

Query

Start Date/Time	CPU Time (ms)	Total Duration	SE Duration	FE Duration	SE Cache Hit	Operation	Is Aggregation Used	Event Text
21-Jun-21 2:48:49 PM	438	4,064		4,064		QueryEnd	●	DEFINE VAR _H0FilterTable = TREATAS([DATE(2020, 10, 1)], 'Calendar'[Fiscal Month]) VAR __DSOFilterTable = FILTER(KEEPFILTERS(VALUES('Segment'[Field Summary Segment])), AND([NOT('Segment'[Field Summary Segment] IN ('SM&C SMB')), 'Segment'[Field Summary Segment] IN ('SM&C SMB'), 'Segment'[Field Summary Segment] IN ('Enterprise Commercial', 'Enterprise Growth', 'Enterprise Public Sector', 'SM&C Corporate', 'SM&C SMB')))) VAR __DSOFilterTable2 = TREATAS([FY21-Q1, FY21-Q2, FY21-Q3], 'Calendar'[Fiscal Quarter]) VAR __DSOFilterTable3 = TREATAS(['Area Fct'], Forecast Type [Forecast Type]) VAR __DSOFilterTable4 = TREATAS(['APAC', 'Australia', 'Canada', 'Central and Eastern Europe', 'Japan', 'Latam', 'MEA', 'UK', 'United States', 'Western Europe', 'India', 'Greater China', 'Germany', 'France'], Geography [Area]) VAR __DSOFilterTable5 = TREATAS(['Field', 'Services', 'Stores', 'Field'], Business [Business Summary]) VAR __DSOFilterTable6 = TREATAS(['End Customer'], Perspective [Perspective]) VAR __DSOFilterTable7 = TREATAS(['CY', 'CY+1', 'CY-1'], Calendar [Relative Year]) VAR __DSOFilterTable8 = TREATAS(['N/A', 'Scheduled'], Future Flag [Future Flag]) VAR __DSOFilterTable9 = TREATAS(['N/A + Other'], ACR Adjustment Type [ACR Adjustment Type Group]) VAR __DSOCore = SUMMARIZECOLUMNS(Pricing Level [Pricing Level], <DSOFilterTable1>, <DSOFilterTable2>, <DSOFilterTable3>, <DSOFilterTable4>, <DSOFilterTable5>, <DSOFilterTable6>, <DSOFilterTable7>, <DSOFilterTable8>, <DSOFilterTable9>)

What are the related query/aggregated details?

Aggregation Details

Start Date/Time	Operation	Operation Detail	Duration (ms)	Aggregation Status	Event Text
6/21/2021 2:48:45 PM	AggregateTable	RewriteAttempted	0	attemptFailed	{ "table": "Revenue", "matchingResult": "attemptFailed", "failureReasons": [{ "alter...
6/21/2021 2:48:48 PM	AggregateTable	RewriteAttempted	0	attemptFailed	{ "table": "Revenue", "matchingResult": "attemptFailed", "failureReasons": [{ "alter...

Related Queries Aggregation Details

priyan@contoso.com User Application

Application Lifecycle Management

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

Deployment pipelines

When using deployment pipelines, Power BI can copy the datasets with their dataset configuration from the current stage into the target stage. However, automatic aggregations must be reset in the target stage as the settings do not 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 dataset 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 dataset.

 Note

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

Altering a dataset

When altering a dataset 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

Datasets with automatic aggregations enabled contain unique system-generated aggregations tables. Aggregations tables aren't visible to users in reporting tools. They are however visible through the XMLA endpoint by using tools with [Analysis Services client libraries](#) version 19.22.5 and higher. When working with datasets 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 datasets.

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. Shown in the following code snippet, the `SystemManaged` property is 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 dataset resides>";
            string datasetName = "<Specify the name of your dataset>";

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

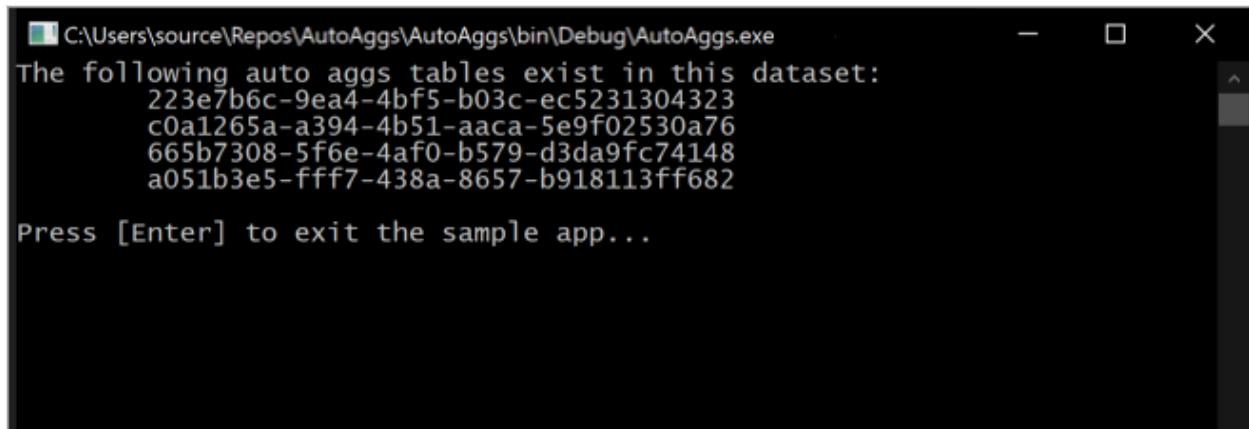
            // Enumerate system-managed tables.
            IEnumerable<Table> aggregationsTables =
dataset.Model.Tables.Where(tbl => tbl.SystemManaged == true);

            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 dataset in a console.



The following auto aggs tables exist in this dataset:
223e7b6c-9ea4-4bf5-b03c-ec5231304323
c0a1265a-a394-4b51-aaca-5e9f02530a76
665b7308-5f6e-4af0-b579-d3da9fc74148
a051b3e5-ffff7-438a-8657-b918113ff682
Press [Enter] to exit the sample app...

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

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

Considerations and limitations

When using automatic aggregations, keep the following in mind:

- 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 is 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 are not available with Power BI Pro, Azure Analysis Services, or SQL Server Analysis Services.
- Power BI does not support downloading datasets 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 is not yet 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 datasets using enhanced metadata. If you want to enable automatic aggregations for an older dataset, upgrade the dataset to enhanced metadata first. To learn more, see [Using enhanced dataset metadata](#).
- Do not 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 are not 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.
- Do not enable automatic aggregations if the dataset 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 therefore not 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 are not 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 will not hit the in-memory aggregations cache.
- Automatic aggregations are only available in the Power BI service. Power BI Desktop does not create system-generated aggregations tables.
- If you modify the metadata of a dataset 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 re-train.
- Do not modify or delete system-generated aggregations tables unless you have automatic aggregations disabled and are cleaning up the dataset. 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 additional 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 • 05/24/2022 • 6 minutes to read

Configuring automatic aggregations includes enabling training for a supported DirectQuery dataset and configuring one or more scheduled refreshes. After several iterations of the training and refresh operations have run, you can return to dataset 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 dataset Owner permissions to enable automatic aggregations. Workspace admins can take over dataset owner permissions.

1. In dataset Settings, expand **Scheduled refresh and performance optimization**.
2. Click the **Automatic aggregations training** slider to **On**. If the enable slider is greyed out, ensure Data source credentials for the dataset are configured and signed in.

▪ Scheduled refresh and performance optimization

To improve the performance of exploring reports, enable scheduled refresh and automatic aggregations and estimate how caching can improve query response times.

Automatic aggregations training (i)

To speed up exploring reports, Power BI can generate aggregations tables to cache some of the data for queries—your reports will run faster, and visuals with cached data will load more quickly. [Learn more](#)



On

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

Refresh frequency

Daily

Time zone

(UTC-08:00) Pacific Time (US and Canada)

Time

5 00 AM X

9 00 AM X

1 00 PM X

5 00 PM X

9 00 PM X

Add another time

Send refresh failure notifications to

Dataset owner

These contacts:

priyan@contoso.com X Enter email addresses

Apply Discard

The screenshot shows a configuration dialog for setting refresh frequencies. It includes a dropdown for frequency (set to Daily), a time zone dropdown (set to Pacific Time (US and Canada)), and a section for defining refresh times. There are five time slots defined: 5:00 AM, 9:00 AM, 1:00 PM, 5:00 PM, and 9:00 PM. Below these, there's a link to add more times. A note about sending failure notifications is present, with checkboxes for dataset owner and specific contacts (priyan@contoso.com). Finally, there are 'Apply' and 'Discard' buttons.

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. To learn more, see [Refresh operations](#).

5. Click **Apply**.

On-demand train and refresh

The first *scheduled* refresh operation for your chosen frequency includes a training operation. If that training operation does not complete within the 60 minute time limit, the subsequent refresh operation will not load or update aggregations in the cache. The

next training operation will not run until the first refresh operation of your chosen frequency.

In such cases, you may want to 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) does not 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, click **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 additional train and refresh operations until training completes successfully and aggregations are loaded or refreshed in the cache.

Using Train and Refresh Now can also be helpful when 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 dataset, contribute to the dataset size, and are subject to existing Power BI dataset size constraints. Aggregations processing also consumes resources and impacts dataset 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.

Adjusting the percentage

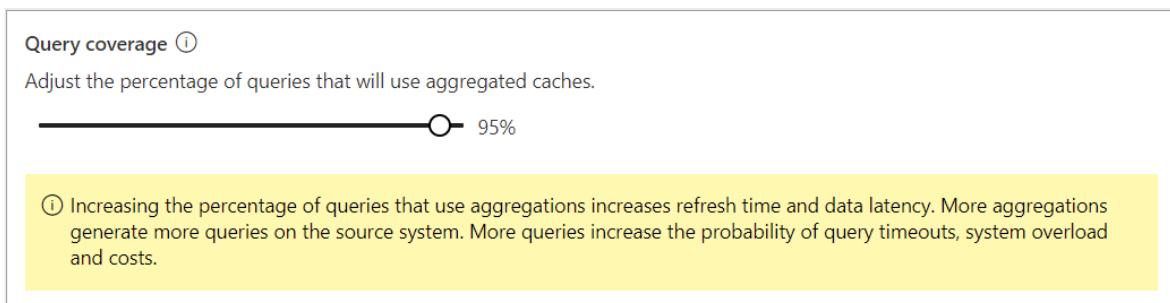
By default, the aggregations cache setting that determines the percentage of report queries that will use aggregations from the in-memory cache is 75%. Increasing the percentage means a greater number of report queries are ranked higher and therefore aggregations for them are included in the in-memory 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 be completed 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 may be different than others.

To adjust the percentage

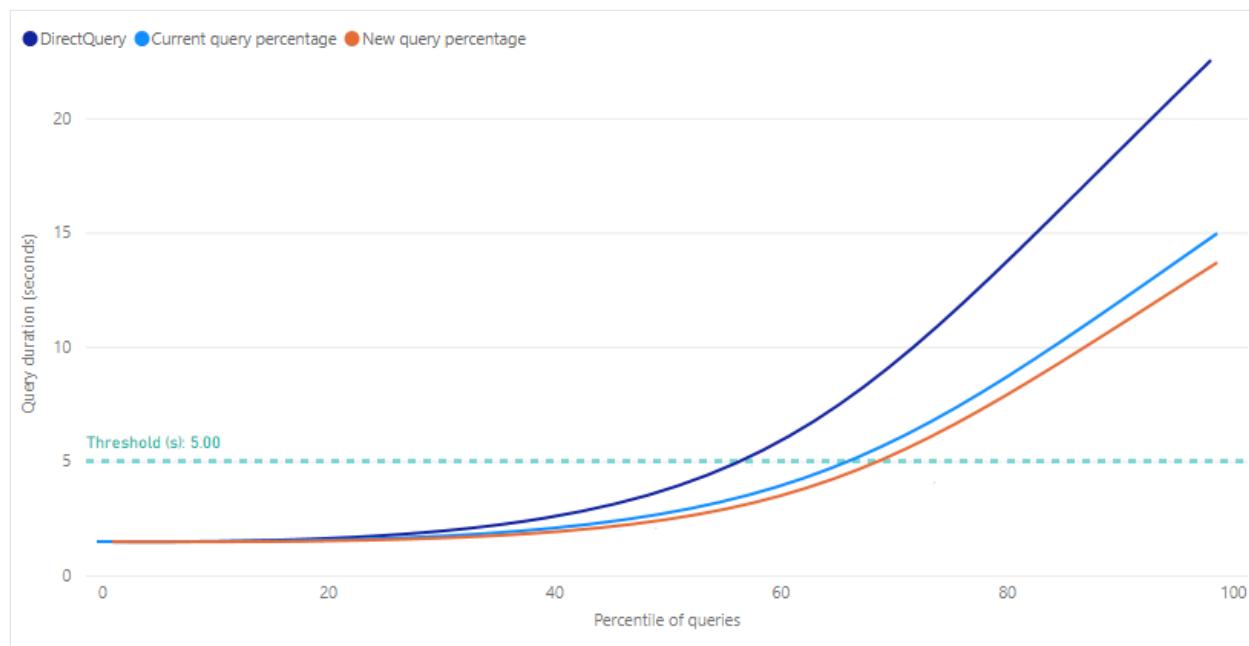
1. In dataset Settings, expand **Scheduled refresh and performance optimization**
2. In **Query coverage**, use the Adjust the percentage of queries that will use the aggregated caches slider to increase or decrease the percentage to the desired value. As you adjust the percentage, the Query performance impact lift chart provides estimated query response times.



3. Click Train and Refresh Now or Apply.

Estimating 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 cannot 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 dataset Owner permissions to disable automatic aggregations. Workspace admins can take over dataset owner permissions.

1. To disable, click the **Automatic aggregations training** slider to **Off**.

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

① Automatic aggregations training will be disabled when you click Apply, but the dataset might still contain automatic aggregations tables. Do you want to remove any existing automatic aggregations tables from the dataset?

Delete automatic aggregations tables

If you choose *not* to delete existing automatic aggregation tables, the tables will remain in the dataset and continue to be refreshed. However, because training has been 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 dataset is reverted back to its original state - without any automatic aggregations.

2. Click **Apply**.

See also

[Automatic aggregations](#)

[User-defined aggregations](#)

[DirectQuery in Power BI](#)

Power BI site reliability engineering (SRE) model

Article • 06/03/2022 • 17 minutes to read

This document describes the Power BI team's approach to maintaining a reliable, performant, and scalable service for customers. It describes monitoring service health, mitigating incidents, release management and acting on necessary improvements. Other important operational aspects such as security are outside of the scope of this document. This document was created to share knowledge with our customers, who often raise questions regarding site reliability engineering practices. The intention is to offer transparency into how Power BI minimizes service disruption through safe deployment, continuous monitoring, and rapid incident response. The techniques described here also provide a blueprint for teams hosting service-based solutions to build foundational live site processes that are efficient and effective at scale.

Author: Yitzhak Kesselman

Background

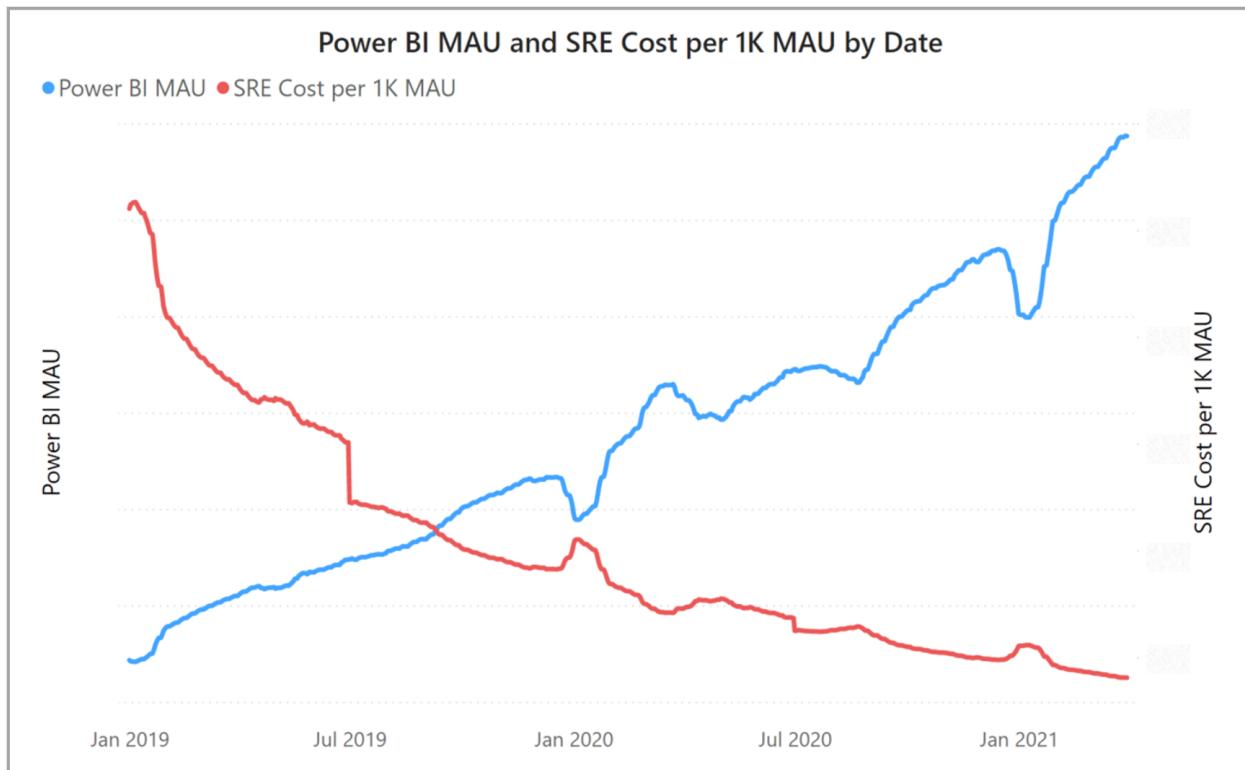
Power BI is a native cloud offering and global service, supporting the following customers and capabilities:

- Serving 260,000 organizations and 97% of Fortune 500 companies
- Deployed in 52 Azure regions around the world
- Executes nearly 20 million queries per hour at peak
- Ingests over 90 petabytes of data per month into customer datasets
- Employs 149 clusters powered by more than 350,000 cores

Despite absorbing six straight years of triple-digit growth and substantial new capabilities, the Power BI service exhibits strong service reliability and operational excellence. As the service grew and large enterprises deployed it at scale to hundreds of thousands of users, the need for exceptional reliability became essential. The reliability results shown in the following table are the direct consequence of engineering, tools, and culture changes made by the Power BI team over the past few years, and are highlighted in this article.

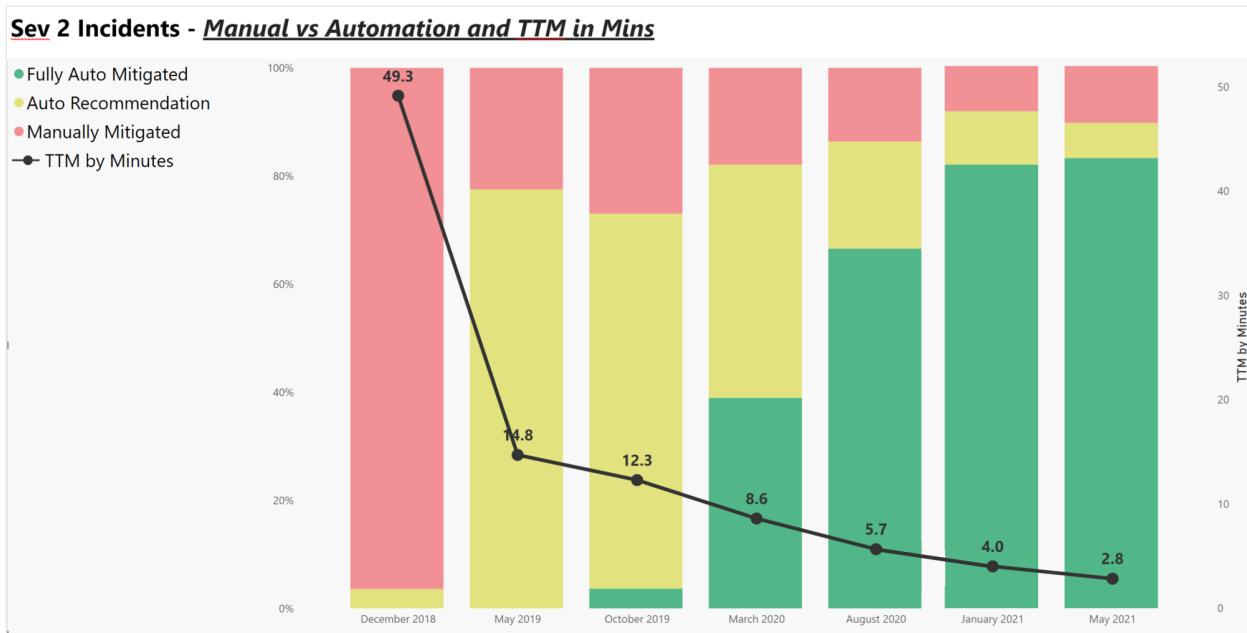
Metric	Actual (Dec 2018)	Actual (May 2021)	%
			Improvement
Time to Notify (TTN) Customers of Incidents – P75	110 min	14 min	87%
Time to Acknowledge (TTA) When Incidents Occur – P75	11 min	0.76 min	93%
Time to Mitigate (TTM) Issue - P50	49.3 min	2.8 min	94%
% Alerts Automated (Enrichment)	7%	88%	1,157%
% Alerts Mitigated w/o human intervention	0%	82%	New Capability
% Incidents Escalated to SMEs (Subject Matter Expert)	6.7%	0.34%	95%

Through solutions and disciplined operations, the Power BI team has sustained exponential growth and rapid update cycles without increasing overall cost or burden on live site management. In the following graph, you can see the continuous and significant decline in Service Reliability Engineering cost per monthly active user (MAU).



The efficiencies gained from site reliability engineering (SRE) team efforts offset the cost of funding such a team. The SRE team size, and its corresponding operational cost, has remained constant despite exponential service growth over the same period. Without such dedicated focus on efficiency, live site support costs would have grown substantially with increased service usage.

Further, an increasing percentage of Power BI live site incidents can now be addressed partially or completely through automation. The following chart shows a 90% decrease in Time to Mitigate (TTM) incidents over the past two years while usage has more than tripled. The same period saw the introduction of alert automation to deflect more than 82% of incidents.



These efforts have resulted in greatly improved service reliability to customers, approaching four nines (99.99%) success rate.

The remainder of this article describes the approach and best practices put in place that enabled the SRE team to achieve the previous chart's outcomes. The following sections include details on live site incident types, standard investigation processes, best practices for operationalizing those processes at scale, and the Objective Key Results (OKRs) used by the team to measure success.

Why incidents occur and how to live with them

The Power BI team ships weekly feature updates to the service and on-demand targeted fixes to address service quality issues. The release process includes a comprehensive set of quality gates, including comprehensive code reviews, ad-hoc testing, automated component-based and scenario-based tests, feature flighting, and regional safe deployment. However, even with these safeguards, live site incidents can and do happen.

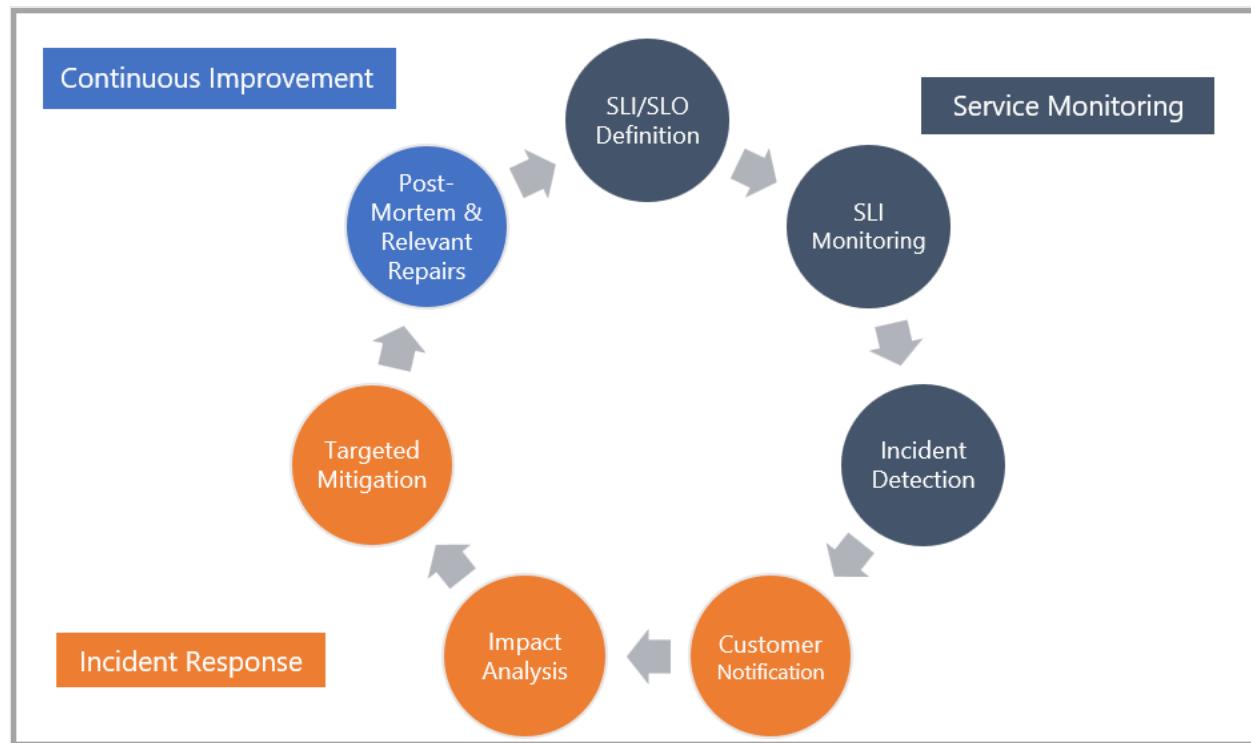
Live site incidents can be divided into several categories:

- Dependent-service issues (such as Azure AD, Azure SQL, Storage, virtual machine scale set, Service Fabric)
- Infrastructure outage (such as a hardware failure, data center failure)
- Power BI environmental configuration issues (such as insufficient capacity)
- Power BI service code regressions
- Customer misconfiguration (such as insufficient resources, bad queries/reports)

Reducing incident volume is one way to decrease live site burden and to improve customer satisfaction. However, doing so isn't always possible given that some of the incident categories are outside the team's direct control. Furthermore, as the service footprint expands to support rapid growth in usage, the probability of an incident occurring due to external factors increases. High incident counts can occur even in cases where the Power BI service has minimal service code regressions, and has met or exceeded its Service Level Objective (SLO) for overall reliability of 99.95%, which has led the Power BI team to devote significant resources to reducing incident costs to a level that is sustainable, by both financial and engineering measures.

Live site incident process

When investigating live site incidents, the Power BI team follows a standard operational process that's common across Microsoft and the industry. The following image summarizes the standard live site incident handling lifecycle.



In the first phase, which is the **service monitoring** phase, the SRE team works with engineers, program managers, and the Senior Leadership Team to define Service Level Indicators (SLIs) and Service Level Objectives (SLOs) for both major scenarios and minor scenarios. These objectives apply to different metrics of the service, including scenario/component reliability, scenario/component performance (latency), and resource consumption. The live site team and product team then craft alerts that monitor Service Level Indicators (SLIs) against agreed upon targets. When violations are detected, an alert is triggered for investigation.

In the second phase, which is the **incident response** phase, processes are structured to facilitate the following results:

- Prompt and targeted notification to customers of any relevant impact
- Analysis of affected service components and workflows
- Targeted mitigation of incident impact

In the final phase, which is the **continuous improvement** phase, the team focuses on completion of relevant post-mortem analysis and resolution of any identified process, monitoring, or configuration or code fixes. The fixes are then prioritized against the team's general engineering backlog based on overall severity and risk of reoccurrence.

Our practices for service monitoring

The Power BI team emphasizes a consistent, data-driven, and customer-centric approach to its live site operations. Defining Service Level Indicators (SLIs) and implementing corresponding live site monitoring alerts is part of the approval criteria for enabling any new Power BI feature in production. Product group engineers also include steps for investigation and mitigation of alerts when they occur using a template Troubleshooting Guide (TSG). Those deliverables are then presented to the Site Reliability Engineering (SRE) team.

One way in which the Power BI team enables exponential service growth is by using a SRE team. These individuals are skilled with service architecture, automation and incident management practices, and are embedded within incidents to drive end-to-end resolution. The approach contrasts with the rotational model where engineering leaders from the product group take on an incident manager role for only a few weeks per year. The SRE team ensures that a consistent group of individuals are responsible for driving live site improvements and ensuring that learnings from previous incidents are incorporated into future escalations. The SRE team also assists with large-scale drills that test Business Continuity and Disaster Recovery (BCDR) capabilities of the service.

SRE team members use their unique skill set and considerable live site experience, and also partner with feature teams to enhance SLIs and alerts provided by the product team in numerous ways. Some of the ways they enhance SLIs include:

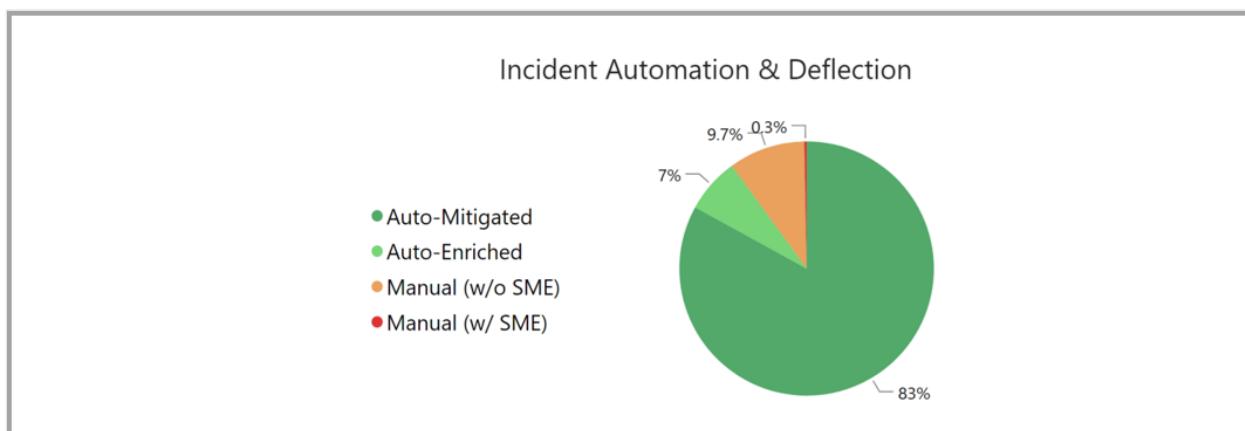
- **Anomaly Alerts:** SREs develop monitors that consider typical usage and operational patterns within a given production environment and alert when significant deviations occur. *Example: Datasets refresh latency increases by 50% relative to similar usage periods.*
- **Customer/Environment-Specific Alerts:** SREs develop monitors that detect when specific customers, provisioned capacities, or deployed clusters deviate from

expected behavior. *Example: A single capacity owned by a customer is failing to load datasets for querying.*

- **Fine-Grained Alerts:** SREs consider subsets of the population that might experience issues independently of the broader population. For such cases, specific alerts are crafted to ensure that alerts will in fact fire if those less common scenarios fail despite lower volume. *Example: Refreshing datasets that use the GitHub connector are failing.*
- **Perceived Reliability Alerts:** SREs also craft alerts that detect cases when customers are unsuccessful due to any type of error. This can include failures from user errors and indicate a need for improved documentation or a modified user experience. These alerts also can notify engineers of unexpected system errors that might otherwise be misclassified as a user error. *Example: Dataset refresh fails due to incorrect credentials.*

Another critical role of the SRE team is to automate TSG actions to the extent possible through Azure Automation. In cases where complete automation is not possible, the SRE team defines actions to *enrich* an alert with useful and incident-specific diagnostic information to accelerate subsequent investigation. Such enrichment is paired with prescriptive guidance in a corresponding TSG so that live site engineers can either take a specific action to mitigate the incident or quickly escalate to SMEs for more investigation. Alerts with enrichment are also candidates for complete automation when possible and when incident volume/severity provides a sufficiently high ROI.

As a direct result of these efforts, more than 82% of incidents are mitigated without any human interaction. The remaining incidents have enough enrichment data and supporting documentation to be handled without SME involvement in 99.7% of cases.



Live Site SREs also enforce alert quality in several ways, including the following:

- Ensuring that TSGs include impact analysis and escalation policy
- Ensuring that alerts execute for the absolute smallest time window possible for faster detection

- Ensuring that alerts use reliability thresholds instead of absolute limits to scale clusters of different size

Our practices for incident response

When an automated live site incident is created for the Power BI service, one of the first priorities is to notify customers of potential impact. Azure has a target notification time of 15 minutes, which is difficult to achieve when notifications are manually posted by incident managers after joining a call. Communications in such cases are at risk of being late or inaccurate due to required manual analysis. Azure Monitoring offers centralized monitoring and alerting solutions that can detect impact to certain metrics within this time window. However, Power BI is a SaaS offering with complex scenarios and user interactions that cannot be easily modeled and tracked using such alerting systems. In response, the Power BI team developed a novel solution called **TTN0**.

- **TTN0 (Time To Notify “0”)** is a *fully automated* incident notification service that uses our internal alerting infrastructure to identify specific scenarios and customers that are impacted by a newly created incident. It is also integrated with external monitoring agents outside of Azure to detect connectivity issues that might otherwise go unnoticed. TTN0 allows customers to receive an email when TTN0 detects a service disruption or degradation. With TTN0, the Power BI team can send reliable, targeted notifications within 10 minutes of impact start time (which is 33% faster than the Azure target). Since the solution is fully automated, there is minimal risk from human error or delays. As of May 2021, more than 8,000 companies have registered for TTN0 alerts.

As mentioned in the previous section, Power BI’s live site philosophy emphasizes automated resolution of incidents to improve overall scalability and sustainability of the SRE team. The emphasis on automation enables mitigation at scale and can potentially avoid costly rollbacks or risky expedited fixes to production systems. When manual investigation is required, Power BI adopts a tiered approach with initial investigation done by a dedicated SRE team. SRE team members are experienced in managing live site incidents, facilitating cross-team communication, and driving mitigation. In cases where the acting SRE team member requires more context on an impacted scenario/component, they may engage the Subject Matter Expert (SME) of that area for guidance. Finally, the SME team conducts simulations of system component failures to understand and to mitigate issues in advance of an active live site incident.

Once the affected component/scenario of the service is determined, the Power BI team has multiple techniques for quickly mitigating impact. Some of them are the following:

- **Activate side-by-side deployment infrastructure:** Power BI supports running different versioned workloads in the same cluster, allowing the team to run a new (or previous) version of a specific workload for certain customers without triggering a full-scale deployment (or rollback). The approach can reduce mitigation time to 15 minutes and lower overall deployment risk.
- **Execute Business Continuity/Disaster Recovery (BCDR) process:** Allows the team to fail over primary workloads to this alternate environment in three minutes if a serious issue is found in a new service version. BCDR can also be used when environmental factors or dependent services prevent the primary cluster/region from operating normally.
- **Leverage resiliency of dependent services:** Power BI proactively evaluates and invests in resiliency and redundancy efforts for all dependent services (such as SQL, Redis Cache, Key Vault). Resiliency includes sufficient component monitoring to detect upstream/downstream regressions as well as local, zonal, and regional redundancy (where applicable). Investing in these capabilities ensures that tooling exists for automatic or manual triggering of recovery operations to mitigate impact from an affected dependency.

Our practices for continuous improvement

The Power BI team reviews all customer-impacting incidents during a Weekly Service Review with representation from all engineering groups that contribute to the Power BI service. The review disseminates key learnings from the incident to leaders across the organization and provides an opportunity to adapt our processes to close gaps and address inefficiencies.

Prior to review, the SRE team prepares post-mortem content and identifies preliminary repair items for the live site team and product development team. Items may include code fixes, augmented telemetry, or updated alerts/TSGs. Power BI SREs are familiar with many of these areas and often proactively make the adjustments in real time while responding to an active incident. Doing so helps to ensure that changes are incorporated into the system in time to detect reoccurrence of a similar issue. In cases where an incident was the result of a customer escalation, the SRE team adjusts existing automated alerting and SLIs to reflect customer expectations. For the ~0.3% of incidents that require escalation to a Subject Matter Expert (SME) of the impacted scenario/component, the Power BI SRE team will review ways in which the same incident (or similar incidents) could be handled without escalation in the future. The detailed analysis by the SRE team helps the product development team to design a more resilient, scalable, and supportable product.

Beyond review of specific postmortems, the SRE team also generates reports on aggregate incident data to identify opportunities for service improvement such as future automation of incident mitigation or product fixes. The reporting combines data from multiple sources, including the customer support team, automated alerting, and service telemetry. The consolidated view provides visibility into those issues that are most negatively impacting service and team health, and the SRE team then prioritizes potential improvements based on overall ROI. For example, if a particular alert is firing too frequently or generating disproportionate impact on service reliability, the SRE team can partner with the product development team to invest in relevant quality improvements. Completing these work items drives improvement to service and live site metrics and directly contributes to organizational objective key results (OKRs). In cases where an SLI has been consistently met for a long period of time, the SRE team may suggest increases to the service SLO to provide an improved experience for our customers.

Measuring success through objective key results (OKRs)

The Power BI team has a comprehensive set of Objective Key Results (OKRs) that are used to ensure overall service health, customer satisfaction, and engineer happiness. OKRs can be divided into two categories:

- **Service Health OKRs:** These OKRs directly or indirectly measure the health of scenarios or components in the service and often are tracked by monitoring/alerting. *Example: A single capacity owned by a customer is failing to load datasets for querying.*
- **Live Site Health OKRs:** These OKRs directly or indirectly measure how efficiently and effectively live site operations are addressing service incidents and outages described in previous sections. *Example: Time To Notify (TTN) customers of an impacting incident.*

The following table shows the major live site health OKRs.

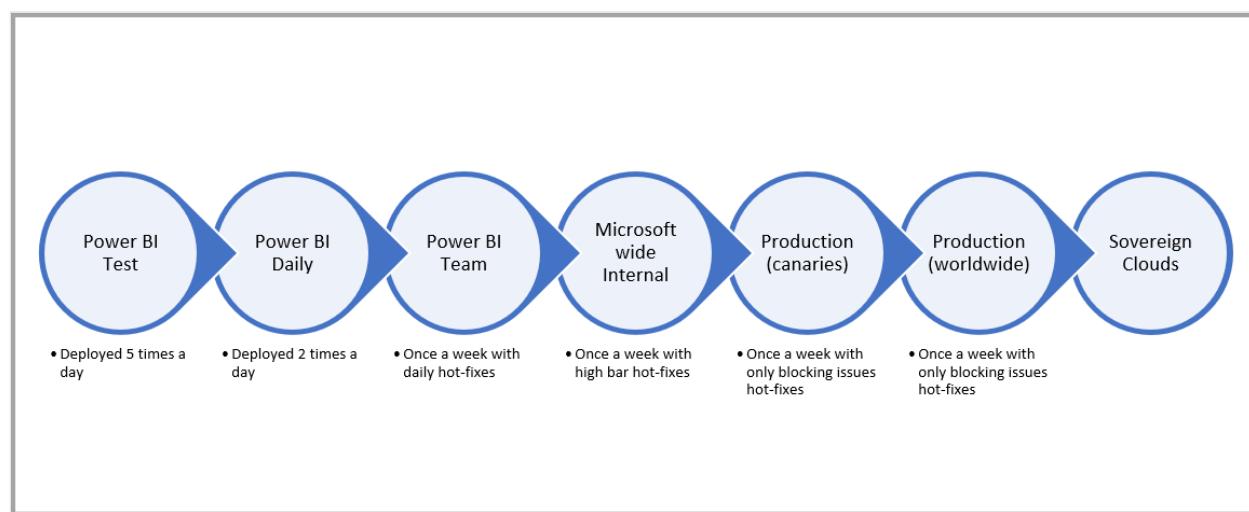
Metric	Actual (Dec 2018)	Actual (May 2021)	% Improvement
Time to Notify (TTN) Customers of Incidents – P75	110 min	14 min	87%
Time to Acknowledge (TTA) When Incidents Occur – P75	11 min	0.76 min	93%
Time to Mitigate (TTM) Issue - P50	49.3 min	2.8 min	94%
% Alerts Automated (Enrichment)	7%	88%	1,157%
% Alerts Mitigated w/o human intervention	0%	82%	New Capability
% Incidents Escalated to SMEs (Subject Matter Expert)	6.7%	0.34%	95%

The time required for the Power BI team to react to incidents as measured by TTN, TTA, and TTM significantly exceeds targets. Alert automation directly correlates with the team's ability to sustain exponential service growth, while continuing to meet or exceed target response times for incident alerting, notification, and mitigation. Over a two-year period, the Power BI SRE team added automation to deflect more than 82% of incidents and to enrich an additional six percent with details that empower engineers to quickly take action to mitigate incidents when they occur. The approach also enables SMEs to focus on features and proactive quality improvements instead of repeatedly being engaged for reactive incident investigations.

The above OKRs are actively tracked by the Power BI live site team, and the Senior Leadership Team, to ensure that the team continues to meet or exceed the baseline required to support substantial service growth, to maintain a sustainable live site workload, and to ensure high customer satisfaction.

Release management and deployment process

Power BI releases weekly feature updates to the service and on-demand targeted fixes to address service quality issues. The approach is intended to balance speed and safety. Any code change in Power BI passes through various validation stages before being deployed broadly to external customers, as described in the following diagram.



Every change to the Power BI code base passes through automated component and end-to-end tests that validate common scenarios and ensure that interactions yield expected results. In addition, Power BI uses a Continuous Integration/Continuous Deployment (CI/CD) pipeline on main development branches to detect other issues that are cost-prohibitive to identify on a per-change basis. The CI/CD process triggers a full cluster build out and various synthetic tests that must pass before a change can enter the next stage in the release process. Approved CI/CD builds are deployed to internal test environments for more automated and manual validation before being included in

each weekly feature update. The process means that a change will be incorporated into a candidate release within 1 to 7 days after it is completed by the developer.

The weekly feature update then passes through various official deployment rings of Power BI's safe deployment process. The updated product build is applied first to an internal cluster that hosts content for the Power BI team followed by the internal cluster that is used by all employees across Microsoft. The changes wait in each of these environments for one week prior to moving to the final step: production deployment. Here, the deployment team adopts a gradual rollout process that selectively applies the new build by region to allow for validation in certain regions prior to broad application.

Scaling this deployment model to handle exponential service growth is accomplished in several ways, as the following bullets describe:

- **Comprehensive Dependency Reviews:** Power BI is a complex service with many upstream dependencies and nontrivial hardware capacity requirements. The deployment team ensures the availability and necessary capacity of all dependent resources and services in a target deployment region. Usage models project capacity needs based on anticipated customer demands.
- **Automation:** Power BI deployments are essentially *zero-touch* with little to no interaction required by the deployment team. Prebuilt rollout specifications exist for multiple deployment scenarios. Deployment configuration is validated at build-time to avoid unexpected errors during live deployment roll-outs.
- **Cluster Health Checks:** Power BI deployment infrastructure checks internal service health models before, during, and after an upgrade to identify unexpected behavior and potential regressions. When possible, deployment tooling attempts auto-mitigation of encountered issues.
- **Incident Response Process:** Deployment issues are handled like other live site incidents using techniques that are discussed in more detail in the following sections of this article. Engineers analyze issues with a focus on immediate mitigation and then follow up with relevant manual or automated process changes to prevent future reoccurrence.
- **Feature Management/Exposure Control:** Power BI applies a comprehensive framework for selectively exposing new features to customers. Feature exposure is independent of deployment cadences and allows code for new scenario code to be deployed in a disabled state until it has passed all relevant quality bars. In addition, new features can be exposed to a subset of the overall Power BI population as an extra validation step prior to enabling globally. If an issue is detected, the Power BI feature management service provides the ability to disable an offending feature in

seconds without waiting for more time-consuming deployment rollback operations.

These features have enabled the Power BI team to improve the success rate of deployments by 18 points while absorbing a 400% year-over-year growth in monthly deployments.

What's next

Another high priority item on the SRE team roadmap is the reduction of system *noise* from false positive alerts or ignorable alerts. In addition, the team will inventory *transient* alerts, drive RCAs, and determine if there are underlying systemic issues that need to be addressed.

Finally, a foundational element of Power BI service resiliency is ensuring that the service is compartmentalized such that incidents only impact a subset of the users. Doing so enables mitigation by redirecting impacted traffic to a healthy cluster. Supporting this holistically requires significant architectural work and design changes but should yield even higher SLOs than are attainable today.

Next steps

For more information related to this article, check out the following resources:

- [Power BI adoption roadmap: Governance](#)
- [White papers for Power BI](#)
- Questions? [Try asking the Power BI Community](#) ↗
- Suggestions? [Contribute ideas to improve Power BI](#) ↗

Bring your own encryption keys for Power BI

Article • 12/15/2022 • 7 minutes to read

Power BI encrypts data *at-rest* and *in process*. 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 is imported into a dataset (see [Data source and storage considerations](#) for more information). This approach is often described as *bring your own key* (BYOK).

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 is 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 cannot use BYOK in the following scenarios:

- Analysis Services Live Connection
- Excel workbooks (unless data is first imported into Power BI Desktop)
- [Push datasets](#)
- [Streaming datasets](#)
- [Power BI goals](#) do not currently support bring your own key (BYOK).

BYOK applies only to datasets. Push datasets, Excel files, and CSV files that users can upload to the service are not 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

In this section you learn 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 instructions in this section 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.

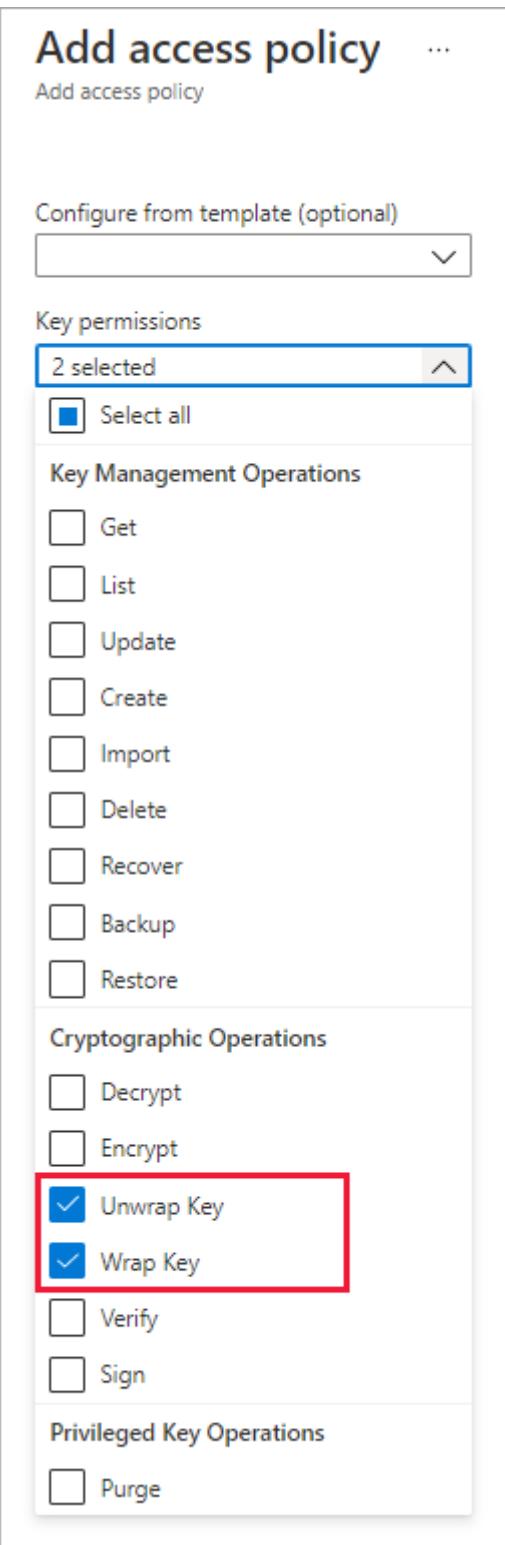
 **Important**

Power BI BYOK supports only RSA keys with a 4096-bit length.

3. (Recommended) Check that the key vault has the [*soft delete*](#) option enabled.

Add the service principal

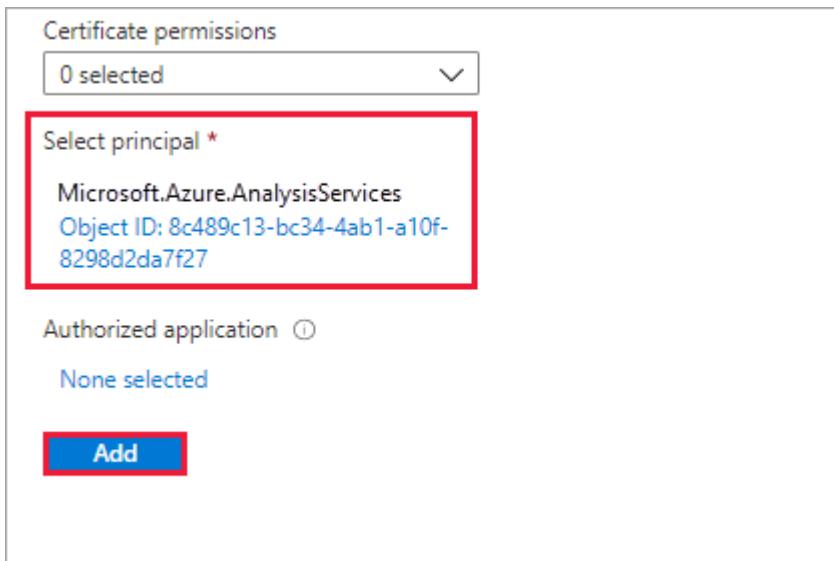
1. In the Azure portal, in your key vault, under **Access policies**, select **Add Access Policy**.
2. Under **Key permissions**, select **Unwrap Key** and **Wrap Key**.



3. Under **Select principal**, 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.



4. Select **Add**, then **Save**.

ⓘ Note

To revoke access of Power BI to your data in the future 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.

Create a key ...

Options

Generate 

Name * 

sample-key 

Key type 

- RSA
 EC

RSA key size

- 2048
 3072
 4096

Set activation date 

Set expiration date 

Enabled

Yes No

Create

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.

Properties

Key type RSA

RSA key size 4096

Created 6/29/2021, 11:13:06 AM

Updated 6/29/2021, 11:13:06 AM

Key Identifier

<https://powerbikeyvaultjp.vault.azure.net/keys/sample-key/b2189c5ec5dc4303a860f0dddd298b70> 

Settings

Set activation date 

Set expiration date 

Enabled

 Yes  No

Tags >

0 tags

Permitted operations

Encrypt

Decrypt

Sign

Verify

Wrap Key

Unwrap Key

Soft delete option

We recommend that you enable [soft-delete](#) on your key vault, to protect from data loss in case of accidental key – or key vault – deletion. You must use [PowerShell to enable the "soft-delete" property](#) on the key vault, because this option is not available from the Azure portal yet.

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

Enabling firewall rules on your key vault is optional. 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 enables Power BI to access your key vault without specifying end point connections.

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

1. Log into the [Azure portal](#).
2. Search for **Key Vaults**.
3. Select the key vault you want to allow access to Power BI (and all other trusted Microsoft services).
4. Select **Networking** and then select **Firewalls and virtual networks**.
5. From the *Allow access from* option, select **Selected networks**.

The screenshot shows the 'media | Networking' page for a Key vault. The left sidebar has a 'Networking' section highlighted with a red box. The main area shows the 'Firewalls and virtual networks' tab selected, also highlighted with a red box. Under 'Allow access from:', the 'Selected networks' radio button is selected, also highlighted with a red box. The 'Virtual networks' section shows a table with columns for Virtual network, Subnet, Resource group, and Subscription, all currently empty. The 'Firewall:' section shows an 'IP address or CIDR' input field with a placeholder 'IP address or CIDR'.

6. In the *firewall* section, in the *Allow trusted Microsoft services to bypass this firewall*, select **Yes**.

Firewall: ⓘ

IP address or CIDR

IP address or CIDR

Exception

Allow trusted Microsoft services to bypass this firewall ⓘ

Yes

No

i This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

7. Select Save.

/working ...

Firewalls and virtual networks

Private endpoint connections

 Save

 Discard changes

 Refresh

Allow access from:

All networks

Selected networks

i Only networks you choose can access this key vault. [Learn more](#)

Virtual networks: ⓘ

[Add existing virtual networks](#)

[Add new virtual network](#)

Virtual network

Subnet

Resource group

Subscription

No virtual networks are selected.

Firewall: ⓘ

IP address or CIDR

IP address or CIDR

Enable BYOK on your tenant

You enable BYOK at the tenant level with [PowerShell](#), by first introducing to your Power BI tenant the encryption keys you created and stored in Azure Key Vault. 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 cannot 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 cannot *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 shared, reports and datasets will become inaccessible, as they are 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 will be 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 will be encrypted using the key you specify (or an updated default key). You cannot

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 is currently using:

```
PowerShell
```

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

- Use [Get-PowerBIEncryptionKey](#) to get the key that your tenant is currently using:

```
PowerShell
```

```
Get-PowerBIEncryptionKey
```

- Use [Get-PowerBIWorkspaceEncryptionStatus](#) to see whether the datasets 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 dataset 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'
```

Please note that the current key should be enabled.

Next steps

[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](#)

Power BI Premium Generation 2

Distribute Power BI content to external guest users with Azure AD B2B

Article • 12/15/2022 • 11 minutes to read

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

By default, external guests have mostly consumption experiences. You can also choose to provide external users with elevated permissions to the workspaces to experience "Edit and Manage" privileges. Additionally, by enabling the [Allow external guest users to edit and manage content in the organization](#) feature setting, you can allow guest users outside your organization to browse and request access to your organization's content.

Another way to share content with external guest users is in-place dataset 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 dataset sharing, see [About Power BI in-place dataset sharing with guest users in external organizations](#).

This article provides a basic introduction to Azure AD B2B in Power BI. For more information, see [Distribute Power BI content to external guest users using Azure Active Directory B2B](#).

Enable access

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 Azure Active Directory to invite guest users.

The option to [allow external guest users to edit and manage content in the organization](#) lets you give guest users the ability to see and create content in workspaces, including browsing your organization's Power BI. The guest user can only be subscribed to content in workspaces that are backed by a Premium capacity.

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 an Azure AD 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 will also appear in people pickers. To prevent guest users from accessing Power BI, use an Azure AD 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. Azure AD B2B calls these addresses *social identities*.

You can't invite users that are associated with a government cloud, like [Power BI for US Government](#).

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

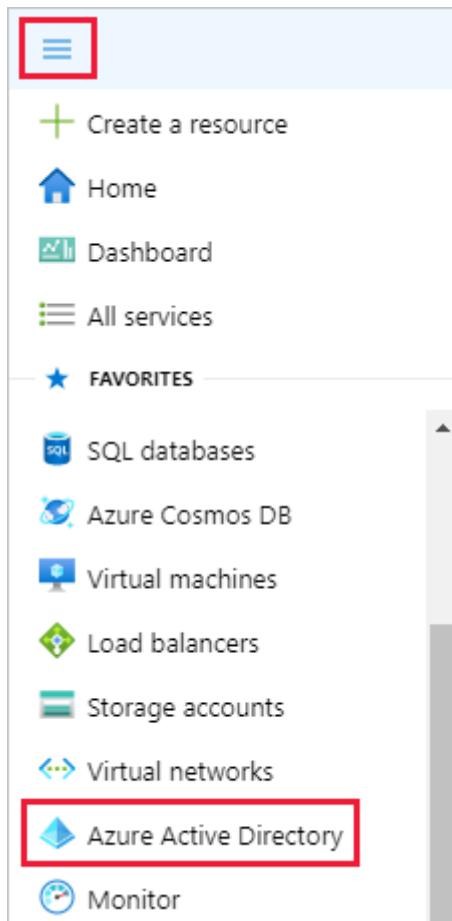
Ad hoc invites aren't supported in the workspace access list. Use the [planned invites approach](#) to add these users to your organization. After the external user becomes a guest in your organization, add them to the workspace access list.

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 **Azure Active Directory**.



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

A screenshot of the 'Users | All users (Preview)' page in the Azure Active Directory. The left sidebar shows 'Contoso | ...' and a 'Manage' section with 'Users' (red-bordered) selected. The main area shows a list of users with columns: Name, User principal name, User type, and Directory synced. A red-bordered '+' button labeled 'New guest user' is located at the top right of the user list. The user list contains 34 entries, each with a checkbox, a small profile picture, the user's name, their email address, their user type (e.g., Member), and a 'No' under 'Directory synced'.

Name	User principal name	User type	Directory synced
Adele Vance	AdeleV@M365x44772...	Member	No
Alex Wilber	AlexW@M365x4477...	Member	No
Allan Deyoung	AllanD@M365x4477...	Member	No
Automate Bot	AutomateB@M365x...	Member	No
Bianca Pisani	BiancaP@M365x447...	Member	No
Brian Johnson...	BrianJ@M365x44772...	Member	No
Cameron White	CameronW@M365x...	Member	No
Christie Cline	ChristieC@M365x44...	Member	No
Conf Room A...	Adams@M365x4477...	Member	No

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

New user ...

Contoso

 Got feedback?

Identity

Name (i)

Email address * (i)

First name

Last name

Personal message

Hi Lucy,

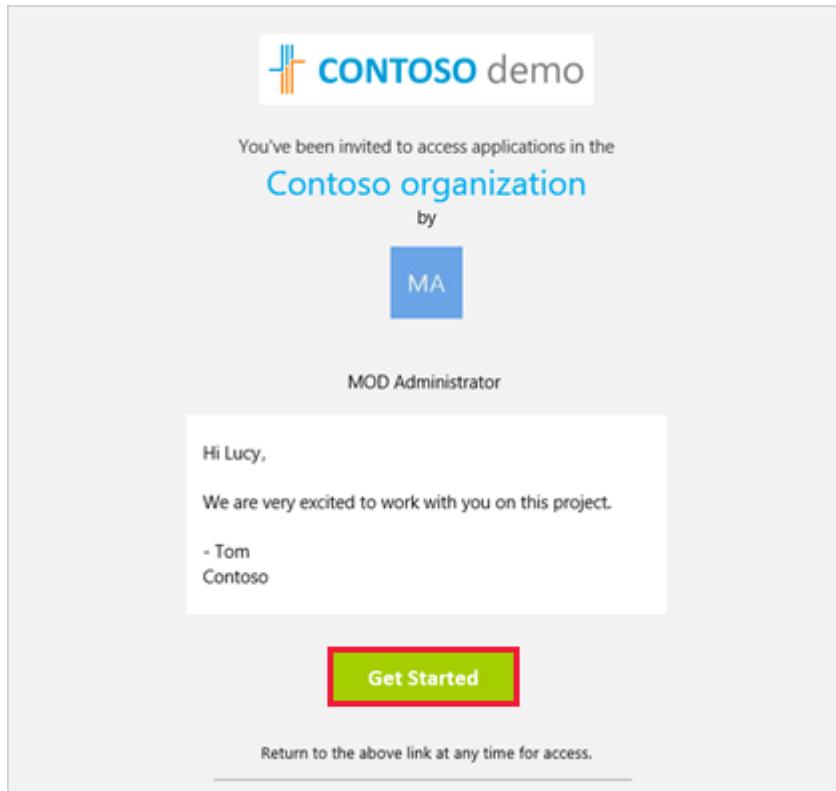
Contoso is really excited to have you work with us on this project.

- Tom
Contoso

4. Select Invite.

To invite more than one guest user, use PowerShell or create a bulk invite in Azure AD. To use PowerShell for the bulk invite, follow the steps in [Tutorial: Use PowerShell to bulk invite Azure AD B2B collaboration users](#). To use the Azure portal for the bulk invite, follow the steps in [Tutorial: Bulk invite Azure AD 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 screenshot shows the 'Access' page for the 'SalesAndMarketing' app. At the top, there is a navigation bar with icons for Search, Notifications, Settings, Download, Help, and User. Below this, there are two buttons: 'Settings' and 'Access'. A red arrow points from the 'Access' button to the 'Add' button in the invite form. The invite form has fields for 'Enter email addresses' (containing 'jim@otics.com') and 'Member' (selected from a dropdown). A large yellow 'Add' button is at the bottom.

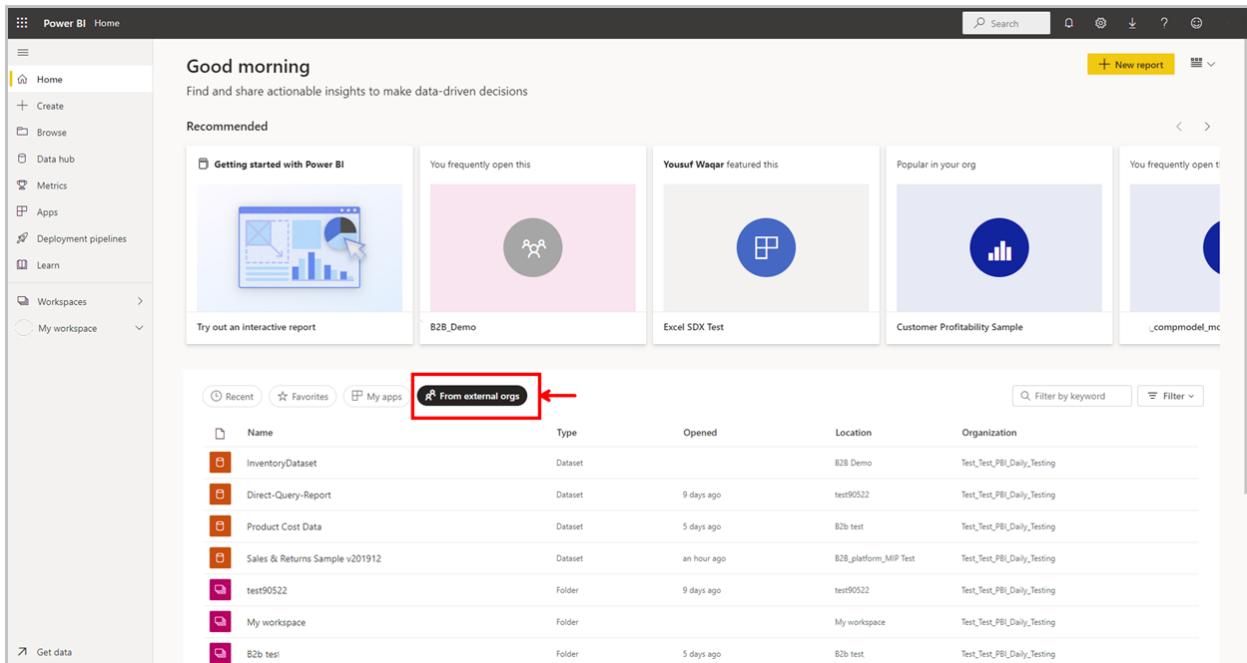
The guest user gets an email indicating that you shared the app with them.

A screenshot of an email inbox showing a shared Power BI app. The subject line is "Megan Bowen has shared Power BI App 'BI Portal' with you". The email is from "Microsoft Power BI <no-reply-powerbi@azureemail.mic" sent at "7:01 PM (0 minutes ago)". The body of the email contains the text "Here's the App that Megan shared with you" and a link "View App in Power BI: BI Portal". Below the link is the Microsoft logo and company information: "Microsoft Corporation, One Microsoft Way, Redmond, WA, 98052". There are also links for "Privacy policy" and "Terms and conditions".

The guest user must sign in with their organization email address. They'll receive a prompt to accept the invitation after signing in. After signing 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

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 will now see a new tab on their home page (in their home tenant) called *From external orgs*. When you select the tab, it will list 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 will open and take 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:

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
My Workspace	All Users	Not Supported	Not Supported	Not 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

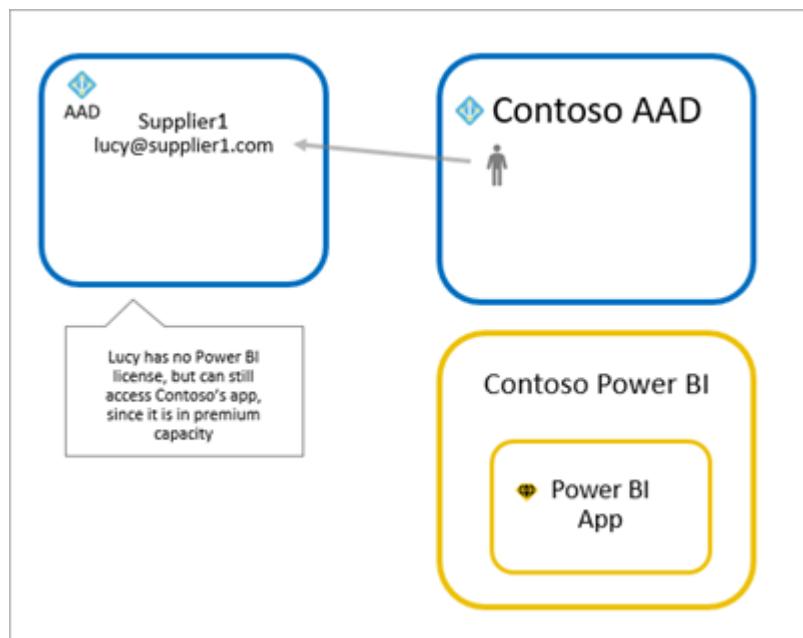
As noted above, the guest user must have the proper licensing in place to view the content that you shared. There are a few ways to make sure the user has a proper license:

- 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.

[Guest users who can edit and manage content in the organization](#) need a Power BI Pro or Premium Per User (PPU) license to contribute content to workspaces or share content with others.

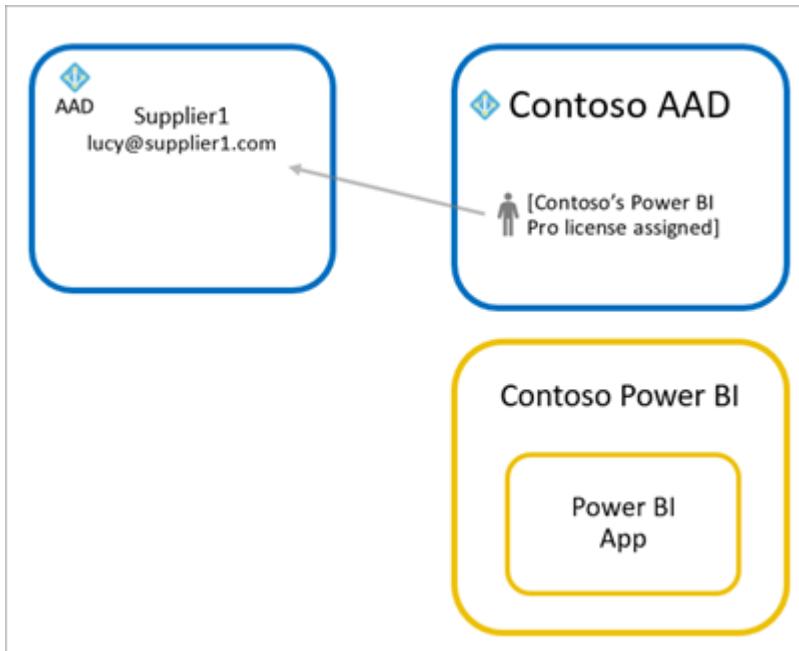
Use Power BI Premium capacity

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.



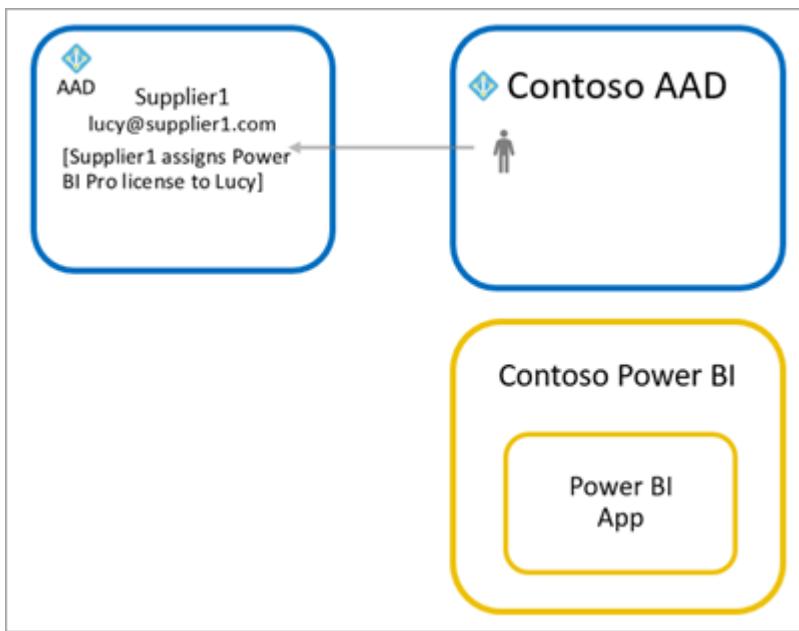
Assign a Power BI Pro or Premium Per User (PPU) license to guest user

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.



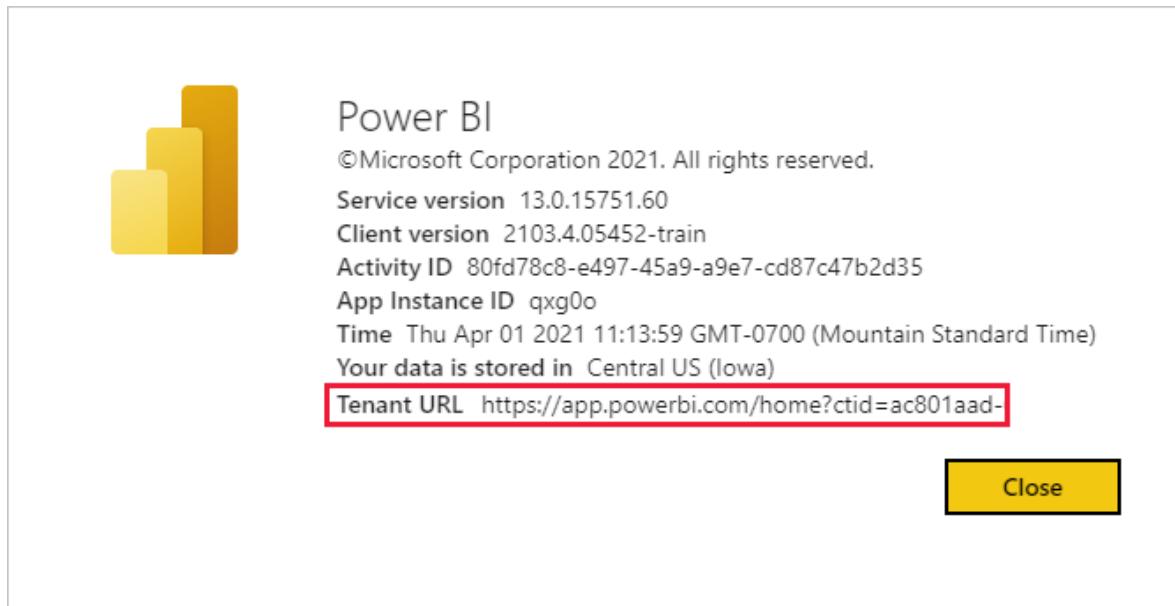
Guest users who can edit and manage content

When using the [allow external guest users to edit and manage content in the organization](#) feature, the specified guest users get additional access to your organization's Power BI. Allowed guests can see any content that they have permissions for, access Home, browse workspaces, install apps, see where they are on the access list, and contribute content to workspaces. They can create or be an Admin of workspaces.

Some limitations apply. The [Considerations and Limitations](#) section lists those restrictions.

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. 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.

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:

- Allow Azure Active Directory guest users to access Power BI
- Invite external users to your organization
- Allow external guest users to edit and manage content in the organization
- Show Azure Active Directory guests in lists of suggested people

There are also Azure Active Directory 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 dataset sharing, tenant admins need to enable the following settings:

- [Allow guest users to work with shared datasets in their own tenants](#)
- [Allow specific users to turn on external data sharing](#)

Considerations and Limitations

- External Azure AD B2B guests can view apps, dashboards, reports, and export data. They can't access workspaces or publish their own content. To remove these restrictions, you can use the [Allow external guest users to edit and manage content in the organization](#) feature.
- Information protection in Power BI doesn't support B2B and multi-tenant scenarios. This means that although external users may be able to see sensitivity labels in Power BI:
 - They can't set labels
 - [Mandatory](#) and [default label](#) policies won't be enforced for them
 - While they can view a report that has a label with protection settings, if they export data from that report to a file, they may not be able to open the file, as it

has the Azure Active Directory permissions of the original organization that it got due to the label on the report.

- Some experiences aren't available to [guest users who can edit and manage content in the organization](#). 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 datasets in the Power BI service
 - Sending ad hoc invites isn't supported for workspace access lists
 - Power BI Publisher for Excel isn't supported for guest users
 - 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 will 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 will send 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.

Next steps

For more detailed info, including how row-level security works, check out the whitepaper: [Distribute Power BI content to external guest users using Azure AD B2B](#).

For information about Azure AD B2B, see [What is Azure AD B2B collaboration?](#).

For information about in-place dataset sharing, see [Power BI in-place dataset sharing with guest users in external organizations\(preview\)](#).

Use customer-managed keys in Power BI

Article • 12/22/2022 • 2 minutes to read

Power BI encrypts data at rest and in process. By default, Power BI uses Microsoft-managed keys to encrypt your data. You can choose to use your organization's keys for encryption of user content at rest across Power BI, from report images to imported datasets in Premium capacities.

Why use customer-managed keys

With Power BI customer-managed keys (CMK), your organization can meet compliance requirements for data encryption at rest with your cloud service provider (in this case, Microsoft). CMK is only offered to new Power BI Premium customers. It enables your organization to encrypt Power BI user content with a key that you provide and manage. Revoking a customer-managed key makes user content within Power BI unreadable for everyone within an hour, including Microsoft. Compared to a bring-your-own-key (BYOK) offering, CMK covers user content that is generated by the service, and customer data that is imported into reports and datasets hosted on Premium capacities. It enforces stricter caching policies, and you can only apply a single key to encrypt all the data.

How to use customer-managed keys

To opt in to Power BI customer-managed keys, contact your Microsoft account manager to validate that your organization meets the size requirements that are required for enabling CMK.

Next steps

The following links provide information that can be useful for customer-managed keys:

- [Bring your own encryption keys for Power BI](#)
- [Configure Multi-Geo support for Power BI Premium](#)
- [Power BI security white paper](#)

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 through redundancy and logical isolation of services.

For more information, see [What are Azure regions and availability zones?](#)

What is a Power BI failover?

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.

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, 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.

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?

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, see [Monitor Premium capacities with the 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.

Migrate Azure Analysis Services to Power BI (preview)

Article • 11/22/2022 • 10 minutes to read

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 dataset 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.

ⓘ Important

The Azure Analysis Services to Power BI Premium migration feature is currently in preview. While in preview, functionality and documentation are likely to change.

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 dataset 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 dataset.

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 dataset 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.
- Dataset Build permissions are set for members of Read model roles.
- Dataset 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 dataset in Power BI.
- Server redirection enabling client applications, tools, and automation processes to be automatically redirected to the newly migrated dataset in Power BI are not included in the migration step. Redirection is enabled separately, after migration is completed.

After migration, the dataset in Power BI is backwards compatible with the same tools used with Azure Analysis Services. Modifying dataset 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 datasets in Power BI that have metadata modified through the XMLA endpoint, migrated datasets can't be downloaded as a Power BI Desktop file. To learn more about dataset 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 dataset in Power BI. If a server alias is configured for the Azure Analysis Services server, it too will redirect to the migrated dataset in Power BI.

Client applications and tools connecting to a migrated dataset 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 dataset 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 Preview 4 (Not yet released)
SQL Server Management Studio (SSMS)	19 Preview 4 (Not yet released)
Visual Studio with Analysis Services projects (SSDT)	3.0.6

Note

PowerShell cmdlets, SQL Server Management Studio, and Server Profiler (installed with SSMS) versions that support server redirect 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 dataset in Power BI. You aren't billed while your server is paused. Deleting servers with server redirect is currently not supported.

Caution

During preview, do not delete your Azure Analysis Services server! Doing so will cause redirection to fail and there is no way to recover redirection.

Report rebind

During preview, Live connect reports in the Power BI service connected to an Azure Analysis Services model database being migrated with the feature aren't automatically rebound to the new dataset in Power BI. Use the [Reports - Rebind Report](#) Power BI REST API to create a new binding to the new dataset.

After rebind by using the API, changes to the Live connect reports can only be made in the Power BI service. Currently, you can't make report changes in a Power BI Desktop file that was previously bound to the model in Azure Analysis Services and then republish to the service.

Important considerations

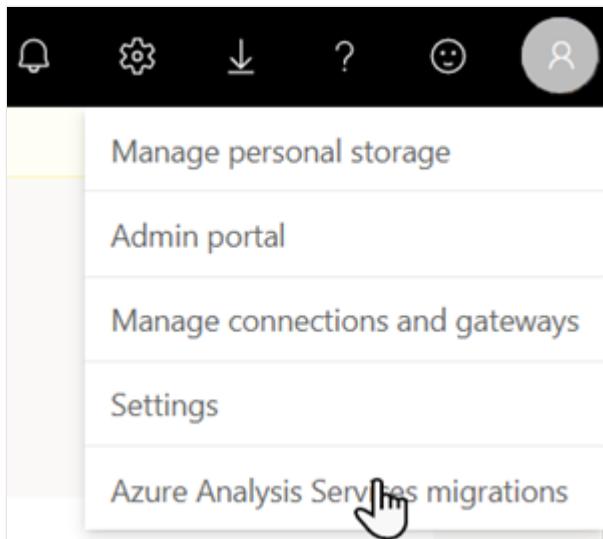
- During preview, if you use the [Reports - Rebind Report](#) Power BI REST API to create a new binding to the migrated dataset, you can't make changes to reports in a Power BI Desktop .pbix that were previously bound to the model in Azure Analysis Services and then republish to Power BI. Report changes for a migrated dataset can be made in the Power BI service.
- During preview, do not delete your Azure Analysis Services server! Doing so will cause redirection to fail and there is no way to recover redirection.
- Datasets 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 dataset metadata, use Visual Studio, the open-source ALM Toolkit, or the open-source Tabular Editor.

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:

Create Azure Analysis Services migration

X

Azure Analysis Services Server

Connect to Azure

Subscription

Adventure Works Subscription

Resource group

Adventure Works RG1

Server name

Adventure Works Sales Server 1

Workspace

Create new Premium workspace

Workspace name

Adventure Works Sales WS1

Available

Description

Workspace for migrations from Azure AS

License mode

- Pro
- Premium per user
- Premium per capacity
- Embedded

ⓘ Confirming that we will create both a Premium per user workspace and a migration in the workspace.

Create

Cancel

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 **Datasets**.

The screenshot shows the 'Migration Details' page in the Power BI service. On the left is a sidebar with navigation icons. The main area has two columns: 'Azure Analysis Services Server' and 'Power BI Premium Workspace'. Under 'Azure Analysis Services Server', it lists 'Azure Analysis Services Server' (azures://eastus.asazure.windows.net/testasmigration), 'Azure Region' (East US), 'Backup Storage' (Enabled), 'Server SKU' (D1), 'Server Firewall' (Firewall Disabled), and 'Gateway'. Under 'Power BI Premium Workspace', it lists 'Power BI Workspace' (Adventure Works Sales WS1), 'Capacity Region' (East US 2 EUAP), 'ADLS Gen 2 Storage' (Enabled), 'Capacity SKU' (P1), and 'XMLA Endpoint' (Read Only). Below these columns are two status messages: a red box with 'X XMLA read/write must be enabled on the capacity.' and a yellow box with '⚠️ Server and workspace regions are not the same.' At the bottom is a 'Datasets' section with a table:

Name	Status	Include in Migration	Exists in Workspace
adventureworks	Successfully migrated	<input checked="" type="checkbox"/> Yes	Yes

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

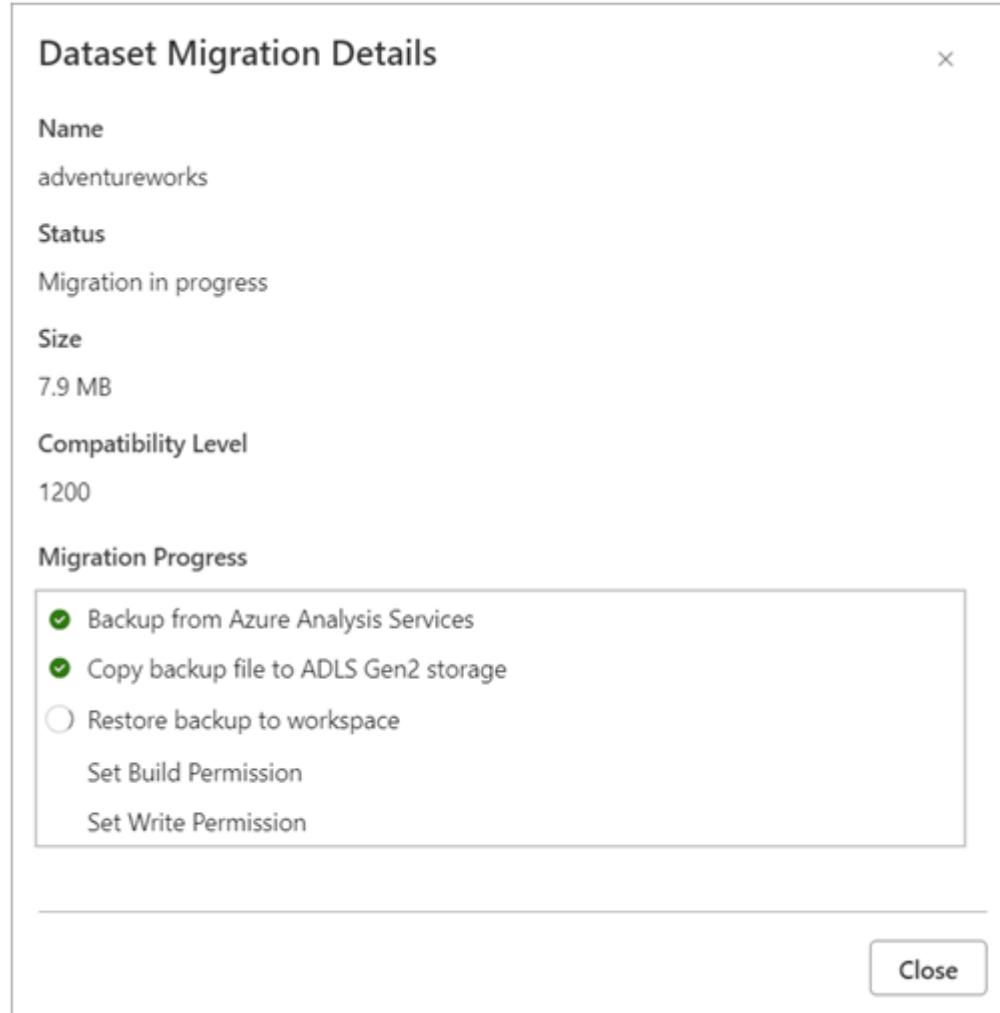
Model databases are migrated in parallel, to reduce impact on your target capacity the maximum number of model databases that can be migrated concurrently is five.

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 dataset in Power BI.

Monitor migration

On the **Migration Details** page, in **Datasets**, select the model database you are migrating to show the **Dataset 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.

Dataset Migration Details

×

Name

[adventureworks](#)

Status

Successfully migrated

Size

7.9 MB

Compatibility Level

1200

Migration Progress

- ✓ Backup from Azure Analysis Services
- ✓ Copy backup file to ADLS Gen2 storage
- ✓ Restore backup to workspace
- ✓ Set Build Permission
- ✓ Set Write Permission

⚠ This model contains at least one role with permissions other than Read, which is not supported in Power BI. Here is a list of supported model permissions(see <https://docs.microsoft.com/en-us/dotnet/api/microsoft.analysisservices.tabular.modelpermission>). Unsupported roles will be missing from the migrated dataset. Please ensure the necessary accounts are given access through workspace roles.

[Close](#)

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 dataset 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**.

The screenshot shows the 'Azure Analysis Services to Power BI Premium' migration page. On the right, there is a yellow button labeled '+ New Migration'. Below it, a search bar has the placeholder 'Search'. Under the heading 'All migrations', there is a table with three columns: 'Azure Analysis Services Server', 'Power BI Premium Workspace', and 'Server Redirection Enabled'. The first row shows 'asazure://westus.asazure.windows.net/advworkstestmigration', 'ProBIUE', and a yellow toggle switch labeled 'On' with a hand cursor icon pointing at it.

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**.

This screenshot is similar to the one above, but a context menu is open over the first row of the 'All migrations' table. The menu items are 'Delete' and 'Redirection status', with a hand cursor icon pointing at 'Redirection status'.

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

The flyout window has a title 'Server Redirection Enabled' and a close button 'X'. It contains the message 'Server redirect enabled on 11/9/2022, 7:33:41 PM.' and 'XMLA based client tools referring to the Azure Analysis Services server name will be automatically redirected to the target workspace.' At the bottom right is a yellow 'OK' button.

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.

Rebind

During preview, Live connect reports in the Power BI service connected to an Azure Analysis Services model database being migrated aren't automatically rebound to the new dataset in Power BI. Use the [Reports - Rebind Report](#) Power BI REST API to create a binding to the new dataset.

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.

⊗ Caution

During preview, do not delete your Azure Analysis Services server! Doing so will cause redirection to fail and there is no way to recover redirection.

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 \(ADLS Gen 2\)](#)

Get a Power BI service subscription for your organization

Article • 11/14/2022 • 3 minutes to read

Administrators can sign up for the Power BI service from the [Purchase services](#) page of the Microsoft 365 admin center. As an administrator, after signing up for Power BI you can assign licenses to users in your organization.

Users in your organization can sign up for Power BI on the Power BI website. When a user signs up for Power BI, they automatically receive a Power BI license. Administrators can turn off these self-service capabilities by following [Enable or disable self-service sign-up and purchasing](#).

Sign up through Microsoft 365

Global and billing administrators can get a Power BI subscription for their organization. For more information, see [Who can purchase and assign licenses?](#)

Note

A Microsoft 365 E5 subscription includes Power BI Pro licenses. To learn how to manage licenses, see [View and manage user licenses](#).

To purchase Power BI Pro licenses on the Microsoft 365 admin center:

1. From your administrator account, sign in to the [Microsoft 365 admin center](#).
2. On the navigation menu, select **Billing > Purchase services**.

The screenshot shows the Microsoft 365 admin center sidebar. The 'Purchase services' option is highlighted with a red box. Other visible options include Home, Users, Groups, Billing, Your products, Licenses, Bills & payments, Billing accounts, Payment methods, and Billing notifications.

3. Search for **Power BI** or select **Power BI** from the **View by category** section.
4. Select multiple offers to compare or select **Details** to purchase an offer.
5. Under **Select license quantity**, select the number of licenses you want to buy, and then select a billing frequency. Select **Buy**. If you haven't previously used it, you can start a **Power BI (free)** trial subscription. The free trial subscription includes 25 user licenses and expires after one month. You can only get one free trial.

The screenshot shows the Power BI Pro product details page. It includes fields for selecting license quantity (set to 25), selecting billing frequency (set to license/month), and a subtotal before applicable taxes. The 'Start free trial' button is highlighted with a red box.

6. Complete the information on the checkout page, and then select **Place order**.

7. To verify your purchase, go to **Billing > Your products** and scroll to **Power BI Pro**.

For more information about how your organization can get and use the Power BI service, see [Power BI in your organization](#).

More ways to get Power BI for your organization

If you're not a Microsoft 365 subscriber, you can [Sign up for a new Microsoft 365 trial](#), and then add Power BI.

To sign up for a Power BI subscription, you need a work or school email address. Email addresses provided by consumer email services or telecommunications providers aren't supported. If you don't have a work or school email address, you can create one during sign-up.

To sign up for Power BI Pro:

1. Go to [Power BI Pro signup](#) and enter an email address. Select **Next**.

The screenshot shows the initial step of a three-step sign-up process. At the top, there are three circular progress indicators: the first is blue and filled, while the second and third are white with a grey outline. Below the indicators, the steps are labeled: "About you", "Sign-in details", and "Complete & get started". The main heading "Let's get you started" is displayed prominently. Below it, instructions advise entering a work or school email address. A large input field is provided for the email address, which is currently empty. A blue "Next" button is located at the bottom of the form.

2. The email address you entered is evaluated. Select **Set up account** or **Change my email** to enter a different address.

! Note

If your email address is already in use with another Microsoft service, you can [Sign in](#) or [Create a new account instead](#). If you choose to create a new account, continue to the next step.

3. Complete the **Tell us about yourself** form and select **Next**. The country/region selected determines where your data is stored. For more information, see [Find the default region for your organization](#). The country/region doesn't have to match your physical location, but should match the location for most of your users.

The screenshot shows a progress bar at the top with three steps: 'About you' (selected), 'Sign-in details', and 'Complete & get started'. Below the progress bar is the heading 'Tell us about yourself'. The form contains fields for 'First name' (with a placeholder '_'), 'Middle name (Optional)', 'Last name' (in a large input field), 'Business phone number' (in a large input field), 'Company name' (in a large input field), 'Company size' (a dropdown menu with 'Select one from below'), and 'Country or Region' (a dropdown menu with 'United States'). A red box highlights the 'Country or Region' section. Below the form is a statement: 'I understand that Microsoft may contact me about my trial.' followed by 'I will receive information, tips, and offers about Power BI, solutions for businesses and organizations, and other Microsoft products and services. [Privacy Statement](#)'. There is also a checkbox for opting into partner communications. At the bottom is a blue 'Next' button.

About you Sign-in details Complete & get started

Tell us about yourself

First name

Middle name (Optional)

Last name

Business phone number

Company name

Company size

Country or Region

I understand that Microsoft may contact me about my trial.
I will receive information, tips, and offers about Power BI, solutions for businesses and organizations, and other Microsoft products and services. [Privacy Statement](#).

I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services. To learn more, or to unsubscribe at any time, view the [Privacy Statement](#).

Next

4. Select whether you want to receive a verification code by text or call. Enter a phone number where the verification code will be sent. Select **Send verification code**.
5. Enter the verification code, and then select **Verify**.
6. Complete the **How you'll sign in** form. This step creates your user ID and password to sign in to your account. You can change the pre-filled username and domain. Domain name is validated to ensure that it isn't a duplicate. Once validated, the

domain name is used to create your organization in the datacenter as a subdomain of [onmicrosoft.com](#). Create and confirm a password. Select **Next**.

The screenshot shows a progress bar at the top with three steps: 'About you' (completed), 'Sign-in details' (current), and 'Complete & get started'. The 'Sign-in details' section contains fields for 'Username' ('username'), 'Domain name' ('@ domain .onmicrosoft.com'), and a 'Save' button. Below these are fields for 'Password' and 'Confirm password', each with an 'Eye' icon for visibility. A note below the fields states: 'By selecting **Next**, you agree to our [trial agreement](#)'. A large blue 'Next' button is at the bottom.

About you Sign-in details Complete & get started

How you'll sign in

This username is what you'll use to sign in each time you use your apps. The domain name is a suggestion. You can change your domain now, or later at any time with your own custom domain.

Username Domain name

username @ domain .onmicrosoft.com Save

Password

.....

Confirm password

By selecting **Next**, you agree to our [trial agreement](#).

Next

Review the confirmation details. The account you created is now the global admin of a new Power BI Pro trial tenant. Sign in to the [Microsoft 365 admin center](#) to add more users, set up a custom domain, purchase more services, and manage your Power BI subscription.

Next steps

- [View and manage user licenses](#)
- [Enable or disable self-service sign-up and purchasing](#)
- [Business subscriptions and billing documentation](#)

Purchase and assign Power BI Pro user licenses

Article • 11/22/2022 • 3 minutes to read

Important

This article is for administrators. To upgrade to a Power BI Pro license, go to [Get started with Power BI Pro](#) to set up your account.

This article explains how to purchase Power BI Pro user licenses in the Microsoft 365 admin center. After purchasing, you can assign licenses to users from either the Microsoft 365 admin center or the Azure portal.

Power BI Pro is an individual user license that lets users read and interact with reports and dashboards that others have published to the Power BI service. Users with this license can share content and collaborate with other Power BI Pro users. Only Power BI Pro users can publish or share content with other users or use content that's created by others, unless a Power BI Premium capacity hosts that content. For more information about the available types of licenses and subscriptions, including Premium Per User (PPU) licenses, see [Power BI licensing in your organization](#).

Self-service purchase, subscription, and license management capabilities for Power Platform products (Power BI, Power Apps, and Power Automate) are available for commercial cloud customers. For more information:

- [Self-service purchase FAQ](#)
- [Enable or disable self-service sign-up and purchasing](#)

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 Azure Active Directory lookups.

Purchase licenses in Microsoft 365

To Purchase Power BI Pro licenses in the Microsoft 365 admin center:

1. Sign in to the [Microsoft 365 admin center](#).
2. On the navigation menu, select **Billing**, and then select **Purchase services**.
3. Search for **Power BI** or select **Power BI** from the **View by category** section.
4. Scroll to **Power BI Pro**, and select **Details**.
5. Select the number of licenses you want to purchase.
6. Under **Select billing frequency**, select if you want to be billed monthly or annually.
An annual commitment is required.
7. Select **Buy**.
8. On the **Checkout** page:
 - a. Verify your organization and contact information.
 - b. Enter payment information, and then select **Save**.
 - c. Review your order information.
 - d. Select **Place order**.
9. To verify your purchase, on the navigation menu, select **Billing**, and then select **Your Products**.
10. To add licenses, from **Billing**, select **Licenses**.

 **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

For 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 Pro licenses to guest users, contact your Microsoft account representative to make sure you're in compliance with the terms of your agreement.

Assign licenses in the Azure portal

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

1. Sign in to the [Azure portal](#).
2. Search for and select **Azure Active Directory**.
3. Select **View** under **Manage Azure Active Directory**.

4. In the navigation pane, under **Manage**, select **Licenses**.
5. Select **All products**.
6. Select **Power BI Pro**, and then select **+ Assign**.
7. On the **Assign license** page, select a user or select **+ Add users and groups**. Add users.
8. Select **Assignment options** and set both options to **On**.
9. Select **Review + Assign**, and then select **Assign**.

Next steps

- [Power BI licensing in your organization](#)
- [Find Power BI users who have signed in](#)
- [Sign up for Power BI as an individual](#)

More questions? [Try asking the Power BI Community ↗](#)

Licensing the Power BI service for users in your organization

Article • 12/15/2022 • 6 minutes to read

Everyone who uses the Power BI service must have a license. What a user can do depends on the type of **per-user license** that they have. Licenses are free, Pro, or Premium Per User (PPU). The level of access provided by their license depends on whether the workspace is a **Premium** workspace or not.

There are two ways for users to get a license, from an administrator or self-service. Self-service sign up capabilities and a work or school email account are needed for users to get their own free, Pro, or Premium Per User license. Administrators can get a Power BI license subscription and then assign licenses to users.

This article is for administrators who can purchase services and per-user licensing. For more information about how users can get their own license, see [Signing up for Power BI as an individual](#).

Who can purchase and assign licenses

You must belong to an admin role to purchase or assign licenses for your organization. Admin roles are assigned from the Azure Active Directory admin center or the Microsoft 365 admin center. For more information about admin roles in Azure Active Directory, see [View and assign administrator roles in Azure Active Directory](#). To learn more about admin roles in Microsoft 365, including best practices, see [About admin roles](#).

The following roles are required to manage licensing for an organization.

- To purchase services and licenses:
 - Billing administrator
 - Global administrator
- To manage user licenses:
 - License administrator
 - User administrator
 - Global administrator

For information about Power BI service admin roles, see [Understanding Power BI service administrator roles](#).

Get Power BI for your organization

For information about pricing, see [Pricing & Product Comparison](#).

If you're not ready to purchase, select the Power BI Pro trial. You'll get 25 licenses to use for one month. For step-by-step instructions on how to sign up, see [Get a Power BI subscription for your organization](#).

About self-service sign-up

Individual users can get their own Power BI license by signing up with their work or school email account. With a free license, users can explore Power BI for personal data analysis and visualization using My Workspace, but they can't share content with others. A Power BI Pro or Power BI Premium Per User license is required before users can share content. For descriptions of the license types, see [license types for the Power BI service](#).

Users can upgrade their license type, or sign up for a different license directly, if the organization is using the commercial cloud. Direct purchase, or upgrade to Pro isn't available to educational organizations or organizations deployed to Azure Government or Azure China 21Vianet clouds.

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

To assign a **Power BI (free)** license to all existing users:

1. From your global admin or billing admin account, sign in to the [Microsoft 365 admin center](#).
2. On the navigation menu, select **Billing** and then select **Purchase services**.
3. Search or scroll to locate the Power BI (free) offer. Select **Details**.
4. Select the number of licenses you want, and then select **Buy**.

The screenshot shows the Microsoft 365 Admin Center interface for purchasing a Power BI (free) license. At the top, there's a heading 'Power BI (free)' with a small icon. Below it is a brief description: 'A cloud-based business analytics service that enables anyone to visualize and analyze data with greater speed, efficiency, and understanding. It connects users to a broad range of live data through easy-to-use dashboards, provides interactive reports, and delivers compelling visualizations that bring data to life.' Underneath, there are three sections: 'Select license quantity' (with a dropdown set to '1'), 'Select billing frequency' (with a radio button selected for '\$0.00 license/month Pay month to month'), and 'Subtotal before applicable taxes' (\$0.00). A large blue 'Buy' button is at the bottom right.

5. Complete the information on the **Checkout** page, and then select **Place order**.

6. Select **Licenses** from the left sidebar, and then select **Power BI (free)** from the subscriptions.

7. Select **Assign licenses** and assign the licenses to users.

To see which users in your organization already have a license, see [View and manage user licenses](#).

License types and capabilities

There are three kinds of Power BI per-user licenses: free, Pro, and Premium Per User. The type of license a user needs is determined by where content is stored, how they'll interact with that content, and if that content uses Premium features. Where an organization stores content is determined by [subscription license type](#).

One type of organizational subscription, [Power BI Premium](#), is a capacity-based license. Premium capacity allows users with Pro and Premium Per User licenses to share content and collaborate with others who have free and Premium Per User licenses.

For detailed information about licensing, see [Licenses for the Power BI](#).

Content created by a user who is assigned a Premium Per User license can only be shared with other users who have a Premium Per User license. Content that is saved in a workspace hosted with Premium capacity can be shared with users who don't have a Premium Per User license. For a detailed breakdown of feature availability per license type, see [Features by license type](#).

Subscription license types

All user-based, commercial licenses from Microsoft are based on Azure Active Directory identities. To use the Power BI service, sign in with an identity that Azure Active Directory supports for commercial licenses. You can add Power BI to any Microsoft license that uses Azure Active Directory for identity services. Some licenses, such as Office 365 E5, include a Power BI Pro license.

There are two kinds of Power BI subscription licenses for organizations: standard and premium.

- Standard - With a standard, self-service Power BI subscription, administrators can assign per user licenses. There's a per user monthly fee for Power BI Pro licenses. This license type enables collaboration, publishing, sharing, and ad-hoc analysis. Content is saved to shared storage capacity that is fully managed by Microsoft.

- Premium - A Power BI Premium subscription license allocates a capacity to an organization. This subscription type is suitable for enterprise BI, big data analytics, cloud and on-premises reporting. Premium provides advanced administration and deployment controls. Reserved compute and storage resources are managed by capacity admins in your organization. There's a monthly cost for this reserved environment. In addition to other Premium advantages, content stored in Premium capacity can be accessed by and distributed to users who don't have Power BI Pro licenses. At least one user must have a Power BI Pro license assigned to use Premium, and content creators and developers need a Power BI Pro license.

The two types of subscriptions aren't mutually exclusive. You can have both Power BI Premium and standard. In this configuration, content stored in Premium capacity can be shared with all users and shared capacity is available. For information about capacity limits, see [Manage data storage in Power BI workspaces](#).

 **Note**

Power BI Premium Gen2 improves the Power BI Premium experience with improvements in the following areas:

- Performance
- Per-user licensing. For more information, see [Power BI Premium Per User](#).
- Greater scale
- Improved metrics
- Autoscaling
- Reduced management overhead

For more information about Power BI Premium Gen2, see [Power BI Premium Generation 2](#).

To compare product features and pricing, see [Power BI pricing](#).

Guest user access

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. Azure Active Directory Business-to-business (Azure AD 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 Azure AD B2B](#).

Purchase Power BI Pro licenses

As an administrator, you can purchase Power BI Pro licenses through Microsoft 365 or through a Microsoft partner. After your purchase, you can assign them to individual users. For more information, see [Purchase and assign Power BI Pro licenses](#).

Power BI Pro license expiration

There's a grace period after a Power BI Pro 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.

Power BI Pro 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](#).

Next steps

- [Purchase and assign Power BI Pro licenses](#)
- [Business subscriptions and billing documentation](#)
- [Find Power BI users that have signed in](#)
- More questions? [Try asking the Power BI Community](#) ↗

View and manage Power BI user licenses

Article • 07/12/2022 • 2 minutes to read

This article explains how admins can use the Microsoft 365 admin center or the Azure portal to view and manage user licenses for the Power BI service.

ⓘ Note

It's possible for a user to have both a Power BI (free) and another Power BI Pro license assigned. This can happen when a user signs up for a free license and then is later assigned a Pro or Premium license. The highest licensing level takes effect in this case.

View your subscriptions

To see which Power BI 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 Power BI subscriptions are listed along with any other subscriptions you have. You may see an unexpected subscription for Power BI (free), as shown here.

The screenshot shows a subscription card for 'Power BI (free)'. The card includes the following details:

- Licenses:** 999,999 available of 1,000,000 (1 used).
- Billing:** Free subscription, No expiration.
- Settings & Actions:** Delete subscription.
- A callout box highlights the text: " ⓘ This is a free subscription activated by users in your company. [Get more info](#)".

This type of subscription is created for you when users take advantage of self-service sign-up. To read more, see [Power BI in your organization](#).

Manage user licenses in Microsoft 365

To use Microsoft 365 admin center to manage user licenses, see the [Business subscriptions and billing documentation](#).

Manage user licenses in Azure portal

Follow these steps to view and assign Power BI licenses using the Azure portal.

1. Sign in to the [Azure portal](#).
2. Search for and select **Azure Active Directory**.
3. Under **Manage** on the Azure Active Directory resource menu, select **Licenses**.
4. Select **All products** from the resource menu, then select a Power BI license type to display the list of licensed users.
5. To assign a license, from the command bar, select **+ Assign**. On the **Assign license** page, choose a user then select **Assignment options** to turn on a Power BI license for the selected user account.
6. To remove a license, select the checkbox next to the user's name, then select **Remove license**.

Next steps

- [Purchase Power BI Pro](#)
- [Licensing for your organization](#)

Enable or disable self-service sign-up and purchasing

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

Administrators can determine whether to enable or disable self-service sign-up. As an administrator, you can 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 Power BI (free) licenses for your organization and assign them to all users.

ⓘ Note

If you acquired Power BI through a Microsoft Cloud Solution Provider (CSP), the setting might be disabled to block users from signing up individually. Your CSP can act as the global 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 sign-up when

- Your large and decentralized organization (work or school) gives individuals the flexibility to 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 Power BI free or Pro license want to create and share content and upgrade to a Power BI Premium Per User 60 day trial.

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 the Power BI service due to data privacy or other concerns and needs to closely control the assignment of Power BI 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 Power BI free license are prompted to try or directly purchase a Power BI Pro license. Your organization might not want these users to upgrade because of security, privacy, or expense.

Use PowerShell, Azure AD, and Microsoft 365 to enable and disable self-service

Use PowerShell commands to change the settings that control self-service sign-up and purchasing.

- If you want to disable all self-service sign-ups: In Azure Active Directory, change the **AllowAdHocSubscriptions** setting using the MSOL PowerShell module. For instructions, see [Set MsolCompanySettings](#). This option turns off self-service sign-up for *all* Microsoft cloud-based apps and services.
- If you want to prevent users from purchasing their own Pro license: Change the **AllowSelfServicePurchase** setting using MSCommerce PowerShell commands. This setting turns off self-service purchase for specific products. For instructions, see [Use AllowSelfServicePurchase for the MSCommerce PowerShell module](#).

Signing up for Power BI with a new Microsoft 365 Trial

Article • 03/09/2022 • 2 minutes to read

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.

If you're having problems signing up for Power BI with your email address, first make sure it's an [email address that can be used with Power BI](#). If that's not successful, sign up for a Microsoft 365 trial and create a work account. Then, use that new work account to sign up for the Power BI service. You'll be able to use Power BI even after the Microsoft 365 trial expires.

Sign up for a Microsoft 365 trial of Office

Sign up for a Microsoft 365 trial [on the Microsoft 365 web site](#). If you don't already have an account, Microsoft will walk you through the steps to create one. Since commercial email accounts (such as Hotmail and Gmail) won't work with Microsoft 365, you'll create a new account that will. That email account will look something like zalan@onmicrosoft.com.

The screenshot shows two side-by-side pricing cards for Microsoft 365. The left card is for 'Office 365 E3' and the right card is for 'Office 365 E5'. Both cards feature a large blurred image at the top. Below the image, each plan is described with its features. At the bottom of each card are four buttons: 'Buy now' (blue), 'Try for free >' (red outline), 'Learn more >' (blue), and 'Contact sales >' (blue).

Plan	Description	Cost	Action Buttons
Office 365 E3	All the features included in Microsoft 365 Apps for enterprise and Office 365 E1 plus security and compliance ¹ .	user/month (annual commitment)	Buy now, Try for free >, Learn more >
Office 365 E5	All the features of Office 365 E3 plus advanced security, analytics, and voice capabilities ¹ .	user/month (annual commitment)	Buy now, Try for free >, Contact sales >, Learn more >

If you select **Office 365 E5**, your trial will include Power BI Pro. The Power BI Pro trial will expire at the same time as your Office 365 E5 trial, which is currently 30 days. If, instead, you select **Office 365 E3**, you'll be able to sign up for Power BI as a *free* user and upgrade to **Premium Per User** for a 60-day trial. For more information about Premium Per User (PPU), see [Power BI Premium Per User](#).

1. Enter your email address. Microsoft will let you know if that email address will work with Microsoft 365 or if you'll need to create a new email address.

The screenshot shows the first step of a four-step account setup process. At the top left is the Microsoft logo. Below it, the text "Thank you for choosing **Office 365 E3**" is displayed. A vertical dotted line on the left side has four numbered circles (1, 2, 3, 4) aligned with the steps. Step 1 is titled "Let's set up your account". It contains the instruction "Enter your work or school email address, we'll check if you need to create a new account for Office 365 E3." Below this is a text input field with the placeholder "Enter your email address". A blue "Next" button is located below the input field. Steps 2, 3, and 4 are listed below step 1: "Tell us about yourself", "Create your business identity", and "You're all set".

Microsoft

Thank you for choosing **Office 365 E3**

- 1 Let's set up your account

Enter your work or school email address, we'll check if you need to create a new account for Office 365 E3.

Next

- 2 Tell us about yourself
- 3 Create your business identity
- 4 You're all set

If you need a new email address, Microsoft will walk you through the steps. First step, creating a new account. Select **Set up account**.



Thank you for choosing **Office 365 E3**

1 Let's set up your account

Looks like you need to create a new account. Let's get you started!

Continue as **pradtanna@** .com [Not you?](#)

[Set up account](#)

2 Tell us about yourself



2

Tell us about yourself



First name

Pradtanna

Last name

Kurasatta

Business phone number

xxxxxxxxxx



Company name

fıgsales

Company size

5-9 people



Country or region

United States



[Next](#)

2. Enter details about the new account.
3. Create your new email address and password. Create a new sign-in name that looks like you@yourcompany.onmicrosoft.com. This is the sign-in you'll use with your new work or school account and with Power BI.

3

Create your business identity



Now create your user ID and password to sign in to your account.

Name
pradtanna

@figsales.onmicrosoft.com

Password
••••••••••



Confirm password
••••••••••



By clicking **Sign up**, you agree to our [trial agreement](#).

I will receive information, tips, and offers about Microsoft Online Services and other Microsoft products and services. [Privacy Statement](#).

I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services. To learn more, or to unsubscribe at any time, view the privacy statement.

Sign up

4. That's it! You now have an email address that you can use to sign up for Power BI.

Head on over to [Sign up for the Power BI service as an individual](#)



Thank you for choosing **Office 365 E3**

- 1 Signup started
- 2 Nice to meet you, Pradtanna
- 3 Thanks for creating an account with us, Pradtanna
- 4 You're all set

Save this info. You'll need it later.

Your user ID
pradtanna@figsales.onmicrosoft.com

[Go to Setup](#)

[Manage your subscription](#)

You may have to wait while your new tenant gets created.

Important considerations

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

By using this signup method, you are creating a new organizational tenant and you'll become the User 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](#).

Next steps

[What is Power BI administration?](#)

[Power BI licensing in your organization](#)

[Signing up for Power BI as an individual](#)

More questions? [Try asking the Power BI Community](#)

Add Power BI to a Microsoft 365 partner subscription

Article • 11/15/2022 • 2 minutes to read

Microsoft 365 enables companies to resell Microsoft 365 bundled and integrated with their own solutions, providing customers with a single point of contact for purchasing, billing, and support.

If you're interested in adding Power BI to your Microsoft 365 subscription, we recommend you contact your partner to do so. If your partner doesn't currently offer Power BI, you can pursue the options described in this article.

Work with your partner to purchase Power BI

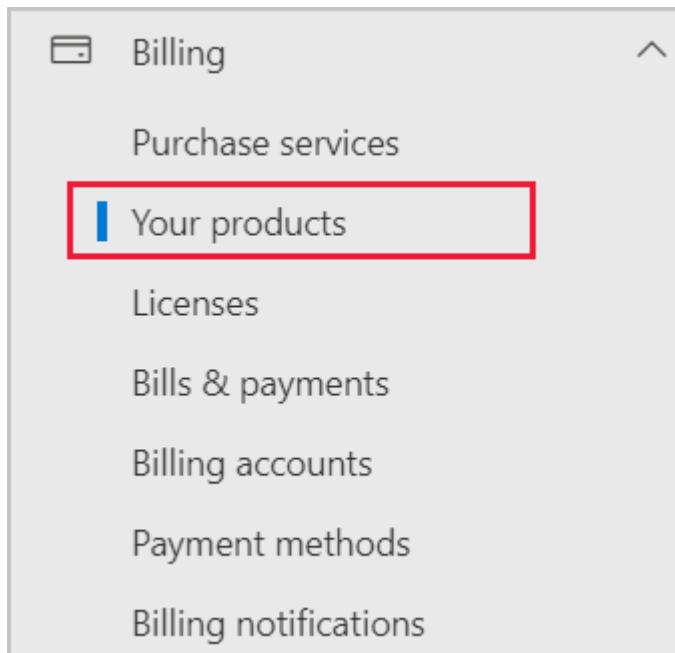
If you want to buy a subscription to Power BI Pro or Power BI Premium, work with your partner to consider what options you have:

- Your partner agrees to add Power BI to their portfolio so that you can purchase from them.
- Your partner can transition you to a model where you can buy Power BI directly from Microsoft or another partner who offers Power BI.

Purchase from Microsoft or another channel

Depending on the relationship with your partner, you might be able to purchase Power BI directly from Microsoft or another partner. You can verify whether you can add Power BI subscriptions in the Microsoft 365 admin center (requires membership in the global admin or billing admin role).

1. Go to the [Microsoft 365 admin center](#).
2. In the left menu, open **Billing**, then select **Your products**:



3. Look for **Subscriptions** in the menu. If you see **Subscriptions**, you can acquire the service from Microsoft directly, or you can contact another partner that offers Power BI.

Your products

[Subscriptions](#) [Apps](#) [Software](#) [Azure](#) [Benefits](#)

If you don't see **Subscriptions**, you can't buy from Microsoft directly or from another partner.

If your partner doesn't offer Power BI and you can't buy directly from Microsoft or another partner, consider signing up for a free trial.

Sign up for a free trial

You can sign up for a free trial of Power BI Premium Per User. If you don't purchase Power BI at the end of the trial period, your license returns to the version you had prior to starting the trial. You still have a Pro or free license that offers many of the features of Power BI. For more information, see [Sign up for Power BI as an individual](#).

Enable ad-hoc subscriptions

By default, individual sign-ups (also known as ad-hoc subscriptions) are disabled. In this case, you see the following message when you try to sign up: *Your IT department has*

turned off signup for Microsoft Power BI.

Microsoft Power BI

Sorry...

We can't [finish](#) signing you up.

Your IT department has turned off signup for Microsoft Power BI. Contact them to [complete](#) signup.

[Learn about other ways to get Office](#)

To enable ad-hoc subscriptions, you can contact your partner and request that they turn them on. If you're an administrator of your tenant, and know how to use Azure Active Directory (Azure AD) PowerShell commands, you can enable ad-hoc subscriptions yourself. For more information, follow the steps in [Enable or disable self-service purchasing](#).

Next steps

- [Power BI licensing in your organization](#)
- [Purchase and assign Power BI Pro licenses](#)

More questions? [Try asking the Power BI Community](#) ↗

Use an alternate email address

Article • 11/14/2022 • 2 minutes to read

When you sign up for Power BI, you provide an email address. By default, Power BI uses this address to send you updates about activity in the service. For example, when someone sends you a sharing invitation, it goes to this address.

In some cases, you might want these emails delivered to an alternate email address rather than the one you signed up with. This article explains how to specify an alternate address in Microsoft 365 and in PowerShell. The article also explains how Azure Active Directory (Azure AD) resolves an email address.

ⓘ Note

Specifying an alternate address doesn't affect which email address Power BI uses for e-mail subscriptions, service updates, newsletters, and other promotional communications. Those communications are always sent to the email address you used when you signed up for Power BI.

Use Microsoft 365

To specify an alternate address in Microsoft 365, follow these steps.

1. Open the [personal info](#) page of your account. If the app prompts you, sign in with the email address and password you use for Power BI.
2. On the left menu, select **Personal info**.
3. In the **Contact details** section, select **Edit**.

If you can't edit your details, an admin manages your email address. Contact your admin to update your alternate email address.

Contact details

Email
MeganB@M365x447726.OnMicrosoft.com

Alias
MeganB

Mobile

Phone

Alternate email
otheremail@somedomain.com

4. In the **Alternate email** field, enter the email address you'd like Microsoft 365 to use for Power BI updates.

Use PowerShell

To specify an alternate address in PowerShell, use the [Set-AzureADUser](#) command.

PowerShell

```
Set-AzureADUser -ObjectId john@contoso.com -OtherMails  
"otheremail@somedomain.com"
```

Email address resolution in Azure AD

To capture an Azure AD embed token for Power BI, you can use one of three different types of email addresses:

- The main email address associated with your Azure AD account
- The UserPrincipalName (UPN) email address
- The *other email address* array attribute

Power BI selects which email to use based on the following sequence:

1. If the mail attribute in the Azure AD user object is present, then Power BI uses that mail attribute for the email address.

2. If the UPN email isn't a *.onmicrosoft.com domain email address (the information after the "@" symbol), then Power BI uses that mail attribute for the email address.
3. If the *other email address* array attribute in the Azure AD user object is present, then Power BI uses the first email in that list (since there can be a list of emails in this attribute).
4. If none of the above conditions are present, then Power BI uses the UPN address.

More questions? [Ask the Power BI Community](#) ↗

Close your Power BI account

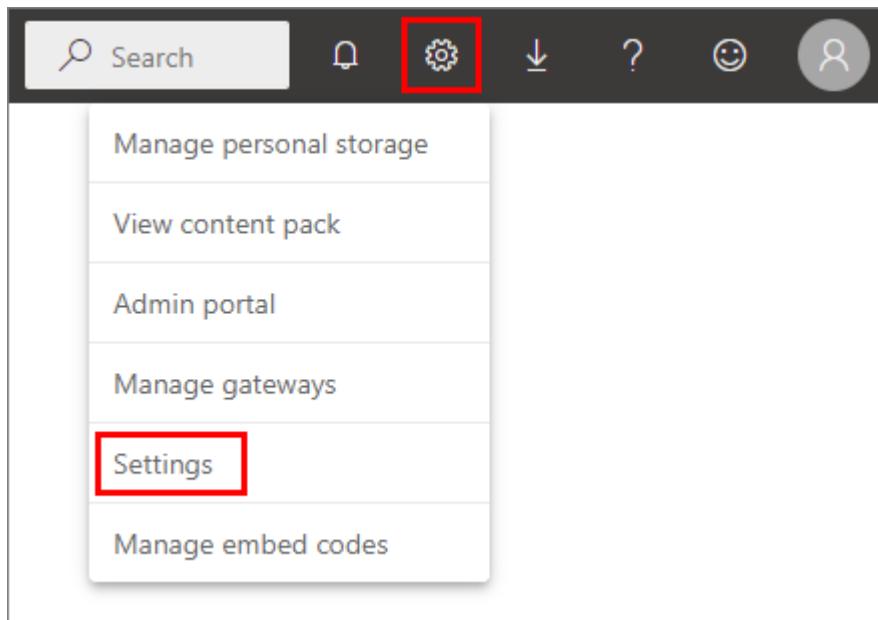
Article • 11/15/2022 • 2 minutes to read

If you don't want to use Power BI any longer, you can 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.

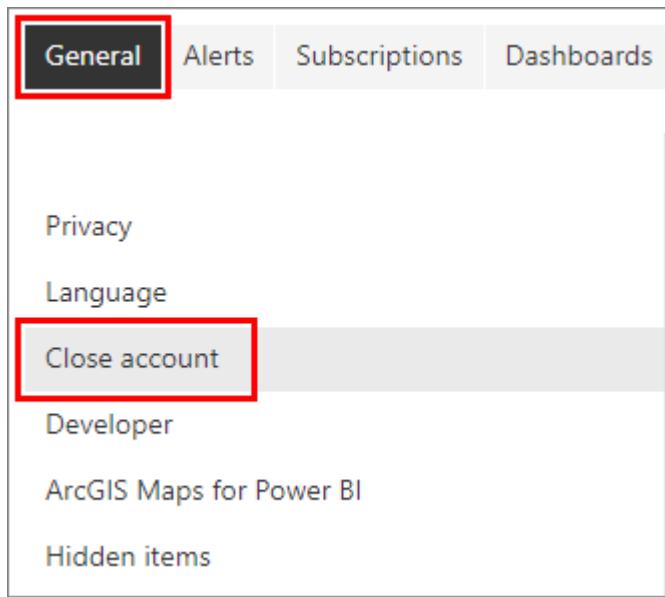
Individual Power BI users

If you signed up for Power BI as an individual, you can close your account from the **Settings** screen.

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**.

Close account

You can close your Power BI account. You will no longer be able to access Power BI and any content you created will be deleted.

Why are you closing your account?

Select a reason (optional) ▾

Anything else you would like to tell us?

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.



Your account is closed.

Didn't mean to close your account? [Reopen your account](#)

Managed users

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

[Close account](#)

ⓘ Your account is managed by your organization's IT department. Please contact your administrator to request changes.

[Close account](#)

More questions? [Try asking the Power BI Community](#) ↗

Power BI for US government customers

Article • 12/08/2022 • 7 minutes to read

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 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've deployed 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

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

Purpose	Destination
Back-end APIs	GCC: *.analysis.usgovcloudapi.net GCC High: *.high.analysis.usgovcloudapi.net DoD: *.mil.analysis.usgovcloudapi.net
Back-end APIs	All: *.pbidicated.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
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 a 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:

Key	Description
✓	The feature is available in the environment, and any exceptions are defined in footnotes.

Key	Description
✖	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.

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 Protection (MIP labels)	✓	✓	✓
Dataflows - Direct Query	✓	✓	Not planned
Dataflows - SQL Compute engine optimization	✓	✓	Not planned
Power BI tab in Teams	✓	✓	✓
Large models	✓	✓	Not planned
Call Quality Data Connector	✓ 3	✖ 3	✖ 3
Bring your own storage (Azure Data Lake Gen 2)	✖	✓	✓
Autoscale	✖	✓	✓

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 Currently available / planned for Power BI Desktop only. Publishing to the Power BI Service is not yet available.

For more information about support for Power BI components in Power Apps, see [Power Apps US Government feature limitations](#).

Next steps

- 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](#)

Enroll your US government organization in the Power BI service

Article • 11/22/2022 • 3 minutes to read

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.

Tell us about your organization

My Organization is:

Select Organization

U.S. Federal, State, Local or Tribal Government Entity

Solution provider serving U.S. Federal, State, Local or Tribal Government Entity

Customers handling Government regulated data

First Name

Last Name

Confirm E-mail Address

Phone Number

Organization Website

Please provide your business address

Please provide your business address

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 choose **Try** or **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 • 11/22/2022 • 2 minutes to read

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 mainland 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.

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	Metrics	Public preview	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	

Product area	Feature or scenario	Commercial cloud status	21Vianet availability	More information
Power BI and Office	PowerPoint - embed live data	Public preview	Not available	Feature availability is dependent on Office add-in readiness in China.
Power BI scalability	Large models	Generally available	Not available	

Next steps

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](#)

Move between regions

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

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

Important

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

Prerequisites

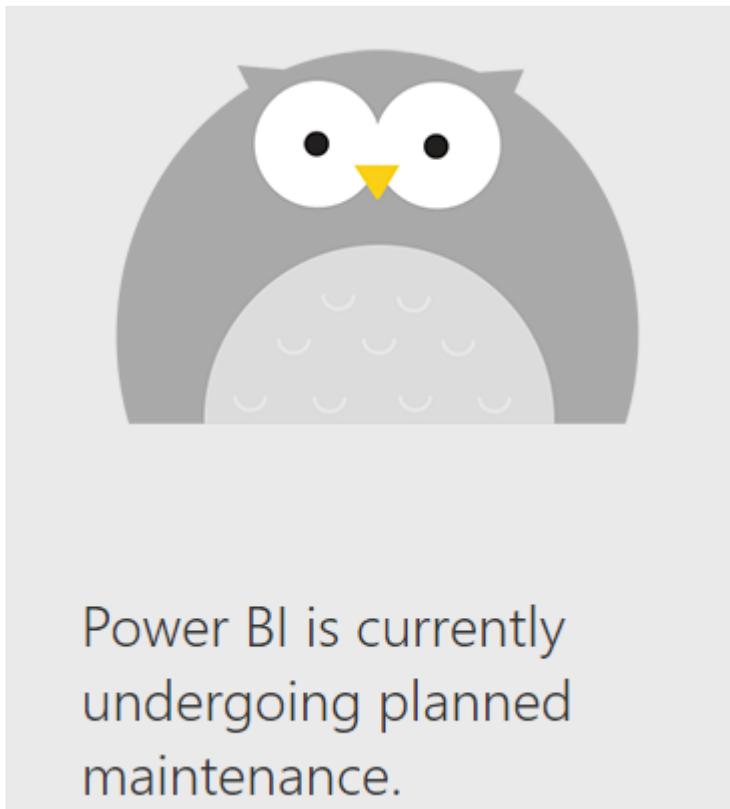
- The person who requests the data region move must be assigned the global administrator role. You can learn more about the different admin roles and what they can do in [Understanding Power BI administrator roles](#). We can't help identify your global administrator for you. Look for global administrator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

Prepare

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

Awareness

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



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

- Dataset and workspace storage modes shouldn't be changed one day before the migration. Changing the storage mode before the migration can leave the datasets unusable after the migration. For more information, read [Dataset modes in the Power BI service](#) and [Manage data storage in Power BI workspaces](#).
- Some usage data collected before migration is unavailable after migration. Usage data in the following sources will be lost:
 - [Power BI Activity Log](#)
 - View count in [Lineage view](#)
 - [Data protection metrics report](#)
 - [Usage metrics\(preview\)](#)

Preparation steps

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

- We can't migrate capacities and Premium workspaces, so you have to delete all capacities before migration. After the region move, these resources can be recreated. If you move resources from a Premium workspace to a shared workspace, datasets larger than 1 GB can't be viewed until they're moved back to Premium capacity.
- Gateways should be deleted in the target region to avoid conflicts during migration.
- To keep user activity logs, follow the steps in [Track user activities in Power BI](#). You can get log data from either the Power BI activity log or the Unified audit log.

Request a region move

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

1. Go to [Power Platform Admin Center Help + support](#) and sign in using admin credentials.
2. Select **New support request**, then select the following options to request a region move:
 - Product: Power BI Pro
 - Tell us what you need help with: Move to a different region

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

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

New support request

If you are a Microsoft partner or delegated admin, [request support at Partner Center](#).

Basics [Solutions](#) [Details](#) [Contact info](#)

Tell us about the issue

What product were you using when the issue occurred? *

Power BI Pro

Tell us what you need help with *

Text will be used to recommend solutions. Please add a brief summary and possibly an error message. Do not include personal data or confidential/proprietary information.

Move to a different region

230/256 characters remaining

Problem type *

Administration

Problem subtype *

Tenant Management

It looks like our new virtual agent can help you resolve this problem, would you like to try it?

Open the Virtual Agent

Are you contacting us to move your tenant to a different region? *

Yes

See solutions

Cancel

Legal | Privacy

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

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

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

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

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

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

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

During the region move

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

After the region move

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

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

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

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

Frequently asked questions

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

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

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

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

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

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

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

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

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

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

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

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

Why do I need to provide three proposed migration dates?

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

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

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

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

Follow the steps in [Find where data is stored](#). You should see the new region next to Your data is stored in.

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

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

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

Refresh in the old region should stop after migration.

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

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

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

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

Power BI Premium features

Article • 12/15/2022 • 2 minutes to read

This article lists the main Power BI Premium features. Most of the features apply to all the Power BI Premium licenses, [Premium Gen2](#), [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

Feature	Description
Advanced AI	Use artificial intelligence (AI) with dataflows
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 Gen2 only
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 Gen2 and Embedded
Dataflows	<ul style="list-style-type: none">• 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
DirectQuery with dataflows	Connect directly to your dataflow without having to import its data
Hybrid tables (preview)	Incremental refresh augmented with real-time data
Insights (preview)	Explore and find insights such as anomalies and trends in your reports

Feature	Description
Model size limit	<p>Available memory is set to:</p> <p><i>Premium Gen2</i> - The limit of memory footprint of a single Power BI dataset; see the column <i>Max memory per dataset</i> in the Capacities and SKUs table</p> <p><i>Premium Per User (PPU)</i> - See Considerations and limitations</p> <p><i>Embedded</i> - See the column <i>Max memory per dataset</i> in the SKU memory and computing power table</p>
Multi-geo	<p>Deploy content to data centers in regions other than the home region of your tenant</p> <p>Available for Premium Gen2 and Embedded</p>
On-demand loading capabilities for large models	<p>Improve report load time by loading datasets to memory on demand</p>
Power BI Report Server	<p>On-premises report server</p> <p>Available for Premium Gen2 only</p>
Refresh rate	<p>The ability to refresh more than eight times a day</p>
Query caching	<p>Speed up reports by using local caching</p>
Storage	<p>Manage data storage</p>
Streaming dataflows (preview)	<p>Connect to, ingest, mash up, model, and build reports using near real-time data</p>
Unlimited content sharing	<p>Share Power BI content with anyone</p> <p>Available for Premium Gen2 only</p>
Virtual network data gateway (preview)	<p>Connect from Microsoft Cloud to Azure using a virtual network (VNet)</p>
XMLA read/write	<p>Enable XMLA endpoint</p>

Next steps

[What is Power BI Premium Gen2?](#)

What is Power BI Premium Gen2?

Article • 12/19/2022 • 7 minutes to read

Power BI Premium Generation 2, referred to as *Premium Gen2*, is the second generation of Power BI Premium. Premium Gen2 provides additional enhancements to Power BI, and a comprehensive portfolio of [Premium features](#).

The following table lists some of the Premium Gen2 enhancements.

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 Power BI Premium Capacity Utilization and 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 memory and computing power. The type of SKU you require, depends on the type of solution you wish to deploy.

The table below describes the resources and limits of each SKU.

Capacity	Dataset	Dataflow	Export API

Capacity		Dataset				Dataflow	Export API
Capacity SKUs	V-cores	Max memory (GB) ^{1, 2, 3}	DirectQuery/Live connection (per second) ^{1, 2}	Max memory per query (GB) ^{1, 2}	Model refresh parallelism ²	Dataflow parallel tasks ⁵	Max concurrent pages ⁶
EM1/A1	1	3	3.75	1	5	4	20
EM2/A2	2	5	7.5	2	10	8	25
EM3/A3	4	10	15	2	20	16	35
P1/A4	8	25	30	6	40	32	55
P2/A5	16	50	60	6	80	64	95
P3/A6	32	100	120	10	160	64	175
P4/A7 ⁴	64	200	240	10	320	64	200
P5/A8 ⁴	128	400	480	10	640	64	200

¹ The [Power BI Premium Utilization and Metrics app](#) doesn't currently expose these metrics.

² These limits only apply to the datasets workload per capacity.

³ The *Max memory per dataset (GB)* column represents an upper bound for the dataset size. However, an amount of memory must be reserved for operations such as refreshes and queries on the dataset. The maximum dataset size permitted on a capacity may be smaller than the numbers in this column. For more information, see [Memory allocation](#).

⁴ 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.

⁵ Learn more about [parallel tasks in dataflows](#).

⁶ See [Export Power BI report to file](#) for more information about Power BI interactive (not paginated) reports.

Subscriptions and licensing

Power BI Premium Gen2 is a tenant-level Microsoft 365 subscription, available in two SKU (Stock-Keeping Unit) families.

P	EM
Range	P1-P5
Use	Enterprise features and embedding
Commitment	Monthly or yearly
Billing	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.

Purchasing

Power BI Premium subscriptions are purchased by administrators in the Microsoft 365 admin center. Specifically, only global administrators or billing administrators can purchase SKUs. When purchased, the tenant receives a corresponding number of v-cores to assign to capacities, known as *v-core pooling*. For example, purchasing a P3 SKU provides the tenant with 32 v-cores. To learn more, see [How to purchase Power BI Premium](#).

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.

Dataset memory allocation

With *Premium Gen2* and *Embedded Gen2*, there's a limit on the memory available for each dataset based on the SKU. For example, in a Premium Gen2 P1 capacity, any dataset that exceeds 25 GB in memory usage would result in failures. You can find the dataset memory upper limits for each SKU, in the *Max memory per dataset* column of the [Capacities and SKUs](#) table.

Dataset operations such as queries are subject to individual memory limits. To illustrate the restriction, consider a dataset 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 dataset. Three separate actions determine the amount of memory attributed to the original dataset, which may be larger than two times the dataset size. The total amount of memory used by one Power BI item can't exceed the SKU's *Max memory per dataset* allocation.

- **Loading the dataset** - The first action is loading the dataset into the memory.
- **Refreshing the dataset** - The second action is refreshing the dataset after it's loaded into the memory. The refresh operation will cause the memory used by the dataset to double. The required memory doubles because the original copy of data is still available for active queries, while another copy is being processed by the refresh. Once the refresh transaction commits, the memory footprint will reduce.
- **Interacting with the report** - The third action is caused by the user's interaction with the report. During the dataset 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 dataset is added to the memory needed to load the dataset, and refresh it.

Refreshes

Premium Gen2 and [Embedded Gen 2](#) don't require cumulative memory limits, and therefore concurrent dataset refreshes don't contribute to resource constraints.

However, refreshing individual datasets 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 Premium Gen2 and [Embedded Gen2](#), 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 [Power BI Premium Capacity Utilization and Metrics](#) app.

To install the app, see [Install the Gen2 metrics app](#). You can learn how to use the app in the article [Use the Gen2 metrics app](#).

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

- **Premium Gen2** - If enabled, [autoscale](#) kicks in. If autoscale isn't enabled, your capacity throttles its [interactive operations](#).
- **Embedded Gen2** - Your capacity throttles its [interactive operations](#). To autoscale in Embedded Gen2, see [Autoscaling in Embedded Gen2](#).

Paginated reports

When using [Premium Gen2](#) and [Embedded Gen2](#), Power BI [paginated reports](#) benefit from the architectural and engineering improvements reflected in Premium Gen2.

- **Memory** - There's no memory management for Paginated reports.
- **SKU availability** - Paginated reports running on Premium Gen2 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.

Considerations and limitations

The following known limitations currently apply to Premium Gen2.

- **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.
- **Client library version** - [Client applications and tools](#) that connect to and work with datasets on Premium Gen2 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.

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](#).

Next steps

[Power BI Premium Per User](#)

[Managing Premium Gen2 capacities](#)

[Power BI Embedded Generation 2](#)

Power BI Premium Gen2 architecture

Article • 12/12/2022 • 4 minutes to read

Power BI Premium Generation 2, referred to as **Premium Gen2** for convenience, is an improved and architecturally redesigned generation of Power BI Premium.

Architectural changes in Premium Gen2, especially around how CPU resources are allocated and used, enables more versatility in offerings, and more flexibility in licensing models. For example, the new architecture enables offering Premium on a per-user basis, offered as [Premium Per User](#). The architecture also provides customers with better performance, and better governance and control over their Power BI expenses.

The most significant update in the architecture of Premium Gen2 is the way capacities' v-cores are implemented:

In the original version of Power BI Premium, v-cores were reserved physical computing nodes in the cloud, with differences in the number of v-cores and the amount of onboard memory according to the customer's licensing SKU. Customer administrators were required to keep track of how busy these nodes were, using the *Premium metrics app*. They had to use the app and other tools to determine how much capacity their users required to meet their computing needs.

In Premium Gen2, v-cores are implemented on regional clusters of physical nodes in the cloud, which are shared by all tenants using Premium capacities in that Power BI region. The regional cluster is further divided into specialized groups of nodes, where each group handles a different Power BI workload (datasets, dataflows, or paginated reports). These specialized groups of nodes help avoid resource contention between fundamentally different workloads running on the same node.

Note

Power BI Gen2 provides logical segregation of data between different customers, and is compliant with ISO 27017. For more details see [ISO/IEC 27017:2015](#).

In both Premium Gen1 and Gen2 versions, administrators have the ability to [tweak and configure workload settings](#) for their capacity. This can be used to reduce resource contention between workloads (datasets, dataflows, paginated reports, and AI), and adjust other settings such as memory limits and timeouts based on the capacity usage patterns.

The contents of workspaces assigned to a Premium Gen2 capacity is stored on your organization's capacity's storage layer, which is implemented on top of capacity-specific Azure storage blob containers, similar to the original version of Premium. This approach enables features like BYOK to be used for your data.

When the content needs to be viewed or refreshed, it is read from the storage layer and placed on a Premium Gen2 node for computing. Power BI uses a placement mechanism that assures the optimal node is chosen within the proper group of computing nodes. The mechanism typically places new content on the node with the most available memory at the time the content is loaded, so that the view or refresh operation can gain access to the most resources and can perform optimally.

As your capacity renders and refreshes more content, it uses more computation nodes, each with enough resources to complete operations fast and successfully. This means your capacity may use multiple computational nodes and in some cases, content might even move between nodes due to the Power BI service performing internal load-balancing across nodes or resources. When such load balancing occurs, Power BI makes sure content movement doesn't impact end-user experiences.

There are several positive outcomes from distributing the processing of content (datasets, dataflows, paginated reports and other workloads) across multiple nodes.

- The shared nodes are at least as large as an original Premium P3 node, which means there are more v-cores to perform any operations, which can increase performance by up to 16x when comparing to an original Premium P1.
- Whatever node your processing lands on, the placement mechanism makes sure memory remains available for your operation to complete, within the applicable memory constraints of your capacity. (see limitations section of this doc for full detail of memory constraints)
- Cross-workloads resource contention is prevented by separating the shared nodes into specialized workload groups. As a result of this separation, there are no controls for paginated report workloads.
- The limitations on different capacity SKUs are not based on the physical constraints as they were in the original version of Premium; rather, they are based on an expected and clear set of rules that the Power BI Premium service enforces:
 - Total capacity CPU throughput is at or below the throughput possible with the v-cores your purchased capacity has.
 - Memory consumption required for viewing and refresh operations remains within the memory limits of your purchased capacity.

- Because of this new architecture, customer admins do not need to monitor their capacities for signs of approaching the limits of their resources, and instead are provided with clear indication when such limits are met. This significantly reduces the effort and overhead required of capacity administrators to maintain optimal capacity performance.

Next steps

[What is Power BI Premium Gen2?](#)

[Premium Gen2 capacity load evaluation](#)

[Using Autoscale with Power BI Premium](#)

[Power BI Premium Gen2 FAQ](#)

[Power BI Premium Per User FAQ](#)

[Add or change Azure subscription administrators](#)

More questions? [Try asking the Power BI 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 paginated reports, 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 paginated reports, 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:

Feature description	Per User	Per Capacity
Model size limit	100 GB	25-400 GB ¹
Refresh rate	48/day	48/day
Paginated reports	✓	✓
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 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.

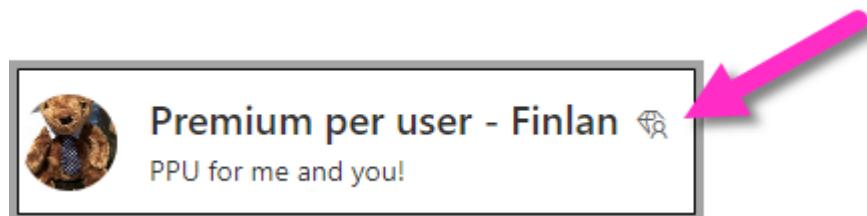
Unlike Premium capacity settings, PPU licenses don't require memory management or CPU management, similar to how Pro licenses don't require such management. Tenant administrators can select feature settings for PPU licenses, but can't disable specific workloads.

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 PPU license (or Premium capacity) is required. A PPU license doesn't allow sending e-mail subscriptions to external users. The content must be hosted in a Premium capacity to offer subscriptions to external users.

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, Premium Gen2, 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.*

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](#)

How to purchase Power BI Premium

Article • 12/15/2022 • 4 minutes to read

This article describes how to purchase a Power BI Premium capacity for your organization. The article covers using P SKUs for typical production scenarios. P SKUs require a monthly or yearly commitment, and are billed monthly.

For more information about Power BI Premium, see [What is Power BI Premium?](#). For current pricing and planning information, see the [Power BI pricing page](#). Content creators still need a [Power BI Pro license](#), even if your organization uses Power BI Premium. Ensure you purchase at least one Power BI Pro license for your organization.

ⓘ Note

If a Premium subscription expires, you have 30 days of full access to your capacity. After that, your content reverts to a shared capacity where it will continue to be accessible. However, you will not be able to view reports that are based on datasets that are greater than 1 GB or reports that require Premium capacities to render.

ⓘ Note

Power BI Premium recently released a new version of Premium, called **Premium Gen2**. Premium Gen2 simplifies the management of Premium capacities, and reduces management overhead. For more information, see [Power BI Premium Generation 2](#).

Purchase P SKUs for typical production scenarios

You can create a new tenant with a Power BI Premium P1 SKU configured, or you can purchase a Power BI Premium capacity for an existing organization. In both cases, you can then add capacity if you need it.

Create a new tenant with Power BI Premium P1

If you don't have an existing tenant and want to create one, you can purchase Power BI Premium at the same time. The following link walks you through the process of creating a new tenant and enables you to purchase Power BI Premium: [Power BI Premium P1](#)

[offer](#). When you create your tenant, you will automatically be assigned to the Microsoft 365 Global Administrator role for that tenant.

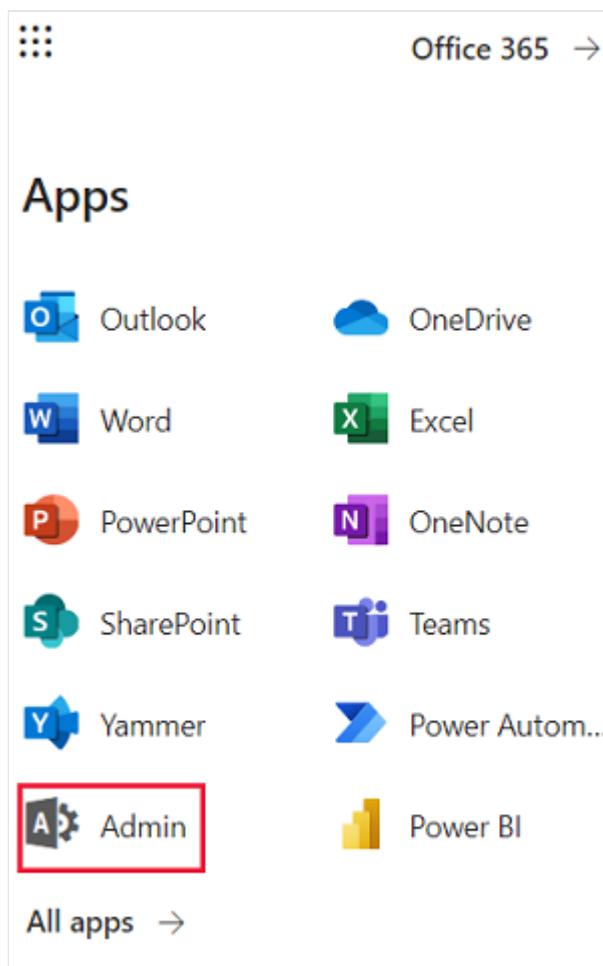
After you purchase capacity, learn how to [manage capacities](#) and [assign workspaces](#) to a capacity.

Purchase a Power BI Premium capacity for an existing organization

If you have an existing organization (tenant), you must be in the Microsoft 365 Global Administrator role or Billing Administrator role to purchase subscriptions and licenses. For more information, see [About Microsoft 365 admin roles](#).

To purchase Premium capacity, follow these steps.

1. From within the Power BI service, select the Microsoft 365 app picker, and then select Admin.



Alternatively, you can browse to the Microsoft 365 admin center.

2. Select **Billing > Purchase services**.

3. Under Power BI, look for Power BI Premium offerings. This will list as P1 through P3, EM3 and P1 (month to month).
4. Select **Details** under the service you want, select a license quantity, and then select **Buy**.

<p>Power BI Premium P1 (Month to Month)</p> <p>Power BI capacity for your organization's needs, unlocking unlimited content distribution and all premium features. P1 can utilize up to 8 virtual core...</p> <p>From <price> instances/month</p> <p>Details <input type="checkbox"/> Compare</p>	<p>Power BI Premium P1</p> <p>Power BI capacity for your organization's needs, unlocking unlimited content distribution and all premium features. P1 can utilize up to 8 virtual core...</p> <p>From <price> instances/month</p> <p>Details <input type="checkbox"/> Compare</p>
--	---

5. Follow the steps to complete the purchase.

After you have completed the purchase, the **Purchase services** page shows that the item is purchased and active.

Purchased

Power BI Premium P1

Active

<price> instance/month
Auto-renews April 18, 2018
1 instance purchased

Office 2016 desktop & mobile apps
Not included

Office 365 services

...

After you purchase capacity, learn how to [manage capacities](#) and [assign workspaces](#) to a capacity.

Purchase additional capacities

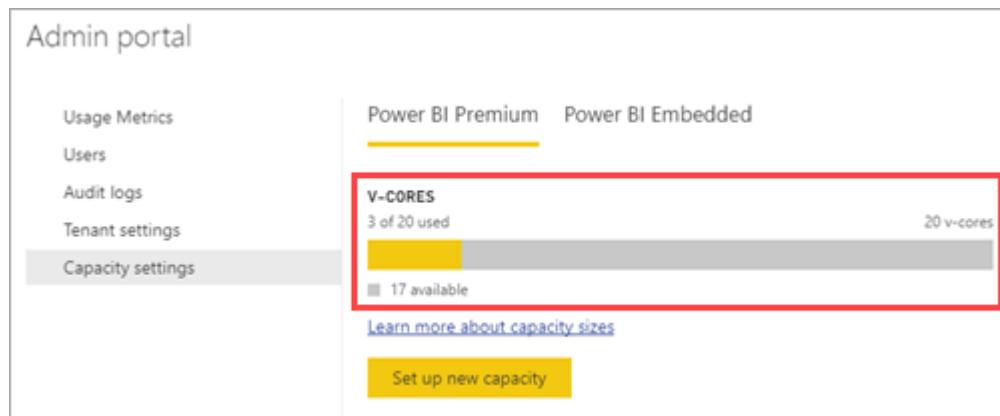
Now that you have a capacity, you can add more as your needs grow. You can use any combination of Premium capacity SKUs (P1 through P3) within your organization. The different SKUs provide different resource capabilities.

1. In the Microsoft 365 admin center, select **Billing > Your products**.
2. Select the Power BI Premium service you want to add capacity to.
3. Select **Buy licenses**.
4. Change the number of instances that you want to have for this item. Then select **Submit** when finished.

ⓘ Important

Selecting **Submit** charges the credit card on file.

The **Your products** page will then indicate the number of instances you have. Within the Power BI admin portal, under **Capacity settings**, the available v-cores reflects the new capacity purchased.



Cancel your subscription

You can cancel your subscription from within the Microsoft 365 admin center. To cancel your Premium subscription, do the following.

1. Browse to the Microsoft 365 admin center.
2. Select **Billing > Your products**.
3. Select your Power BI Premium product from the list.
4. Under **Subscription status**, select **Cancel subscription**.

5. The **Cancel subscription** page will indicate whether or not you are responsible for an [early termination fee](#).
6. Read through the information, and if you want to proceed, select **Cancel subscription**.

When canceling or your license expires

When you cancel your Premium subscription, or your capacity license expires, you can continue to access your Premium capacities for a period of 30 days from the date of cancellation or license expiration. After 30 days, your workspaces will move to a shared capacity and will still be accessible. However, you will not be able to view reports that are based on datasets that require Premium capacities to render. This includes datasets larger than 1GB and refreshes of those datasets.

Purchase A SKUs for testing and other scenarios

You can also purchase A SKUs for testing and other scenarios, which provides Premium capacity on an hourly basis. For more information and steps, see [Purchase Power BI Premium for testing](#).

Purchase Premium Per User (PPU) licenses

You can purchase Power BI Premium for individual users, using the Premium Per User (PPU) license model. For more information about Premium Per User, see [Power BI Premium Per User](#).

Next steps

[Configure and manage capacities in Power BI Premium](#)

[Power BI pricing page](#)

[Power BI Premium FAQ](#)

[Planning a Power BI Enterprise Deployment whitepaper](#)

More questions? [Try asking the Power BI Community](#)

Power BI has released Power BI Premium Gen2, which improves the Power BI Premium experience with improvements in the following:

- Performance
- Per-user licensing
- Greater scale
- Improved metrics
- Autoscaling
- Reduced management overhead

For more information about Power BI Premium Gen2, see [Power BI Premium Generation 2](#).

Purchase Power BI Premium for testing

Article • 12/15/2022 • 2 minutes to read

This article describes how to purchase Power BI Premium A SKUs for testing scenarios, and for cases where you don't have the permissions necessary to purchase P SKUs (Microsoft 365 Global Administrator role or Billing Administrator role). A SKUs require no time commitment, and are billed hourly. You purchase A SKUs in the [Azure portal](#).

For more information about Power BI Premium, see [What is Power BI Premium?](#). For current pricing and planning information, see the [Power BI pricing page](#). Content creators still need a [Power BI Pro license](#), even if your organization uses Power BI Premium. Ensure you purchase at least one Power BI Pro license for your organization. With A SKUs, *all users* who consume content also require Pro licenses.

ⓘ Note

If a Premium subscription expires, you have 30 days of full access to your capacity. After that, your content reverts to a shared capacity. Models that are greater than 1 GB are not supported in shared capacity.

Purchase A SKUs for testing and other scenarios

A SKUs are made available through the Azure Power BI Embedded service. You can use A SKUs in the following ways:

- Enable embedding of Power BI in third party applications. For more information, see [Power BI Embedded](#).
- Test Premium functionality before you buy a P SKU.
- Create development and test environments alongside a production environment that uses P SKUs.
- Purchase Power BI Premium even though you're not a Microsoft 365 Global Administrator role or Billing Administrator role.

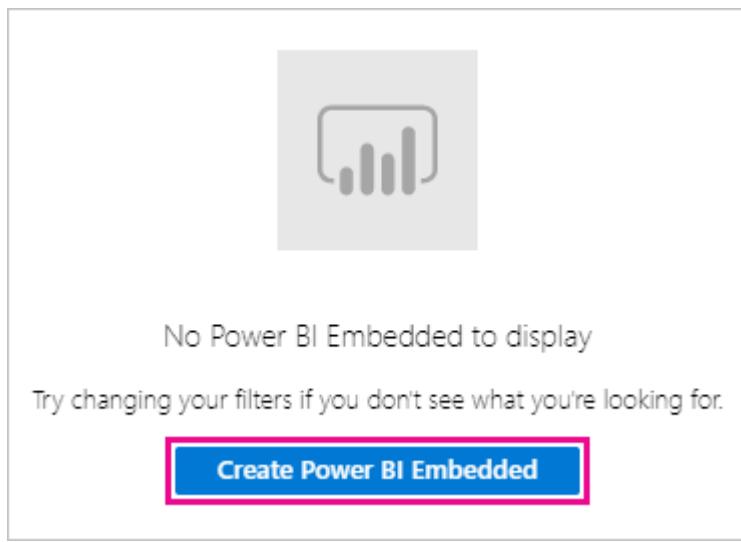
ⓘ Note

If you purchase an A4 or higher SKU, you can take advantage of all Premium features except for unlimited sharing of content. With A SKUs, *all users* who consume content require Pro licenses.

Follow these steps to purchase A SKUs in the Azure portal:

1. Sign in to the [Azure portal](#) with an account that has at least capacity admin permissions in Power BI.
2. Search for *Power BI Embedded* and select the service in the search results.

3. Select **Create Power BI Embedded**.

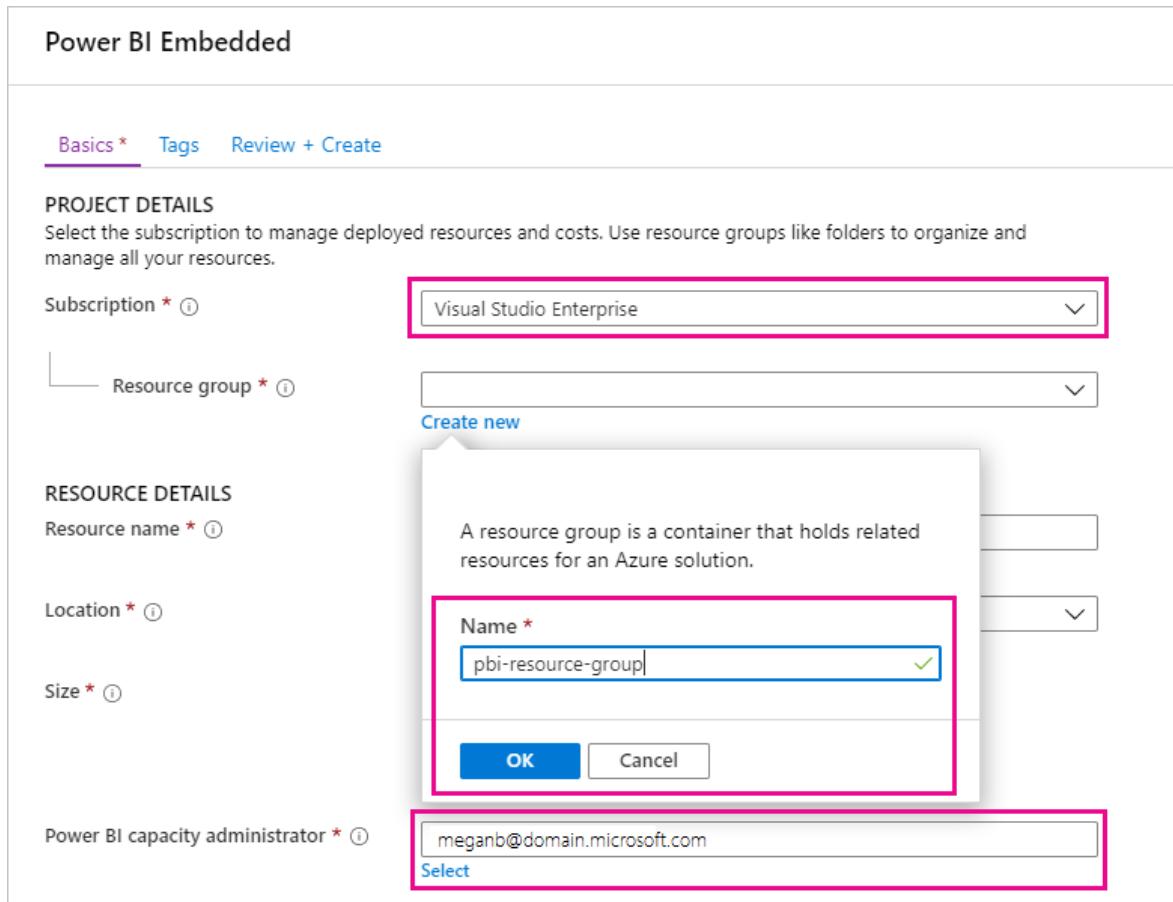


4. On the **Power BI Embedded** create screen, specify the following information:

- The **Subscription** in which to create the Power BI Embedded service.
- The physical **Location** in which to create the resource group that contains the service. For better performance, this location should be close to the location

of your Azure Active Directory tenant for Power BI.

- The existing **Resource group** to use, or create a new one as shown in the example.
- The **Power BI capacity administrator**. The capacity admin must be a member user or a service principal in your Azure AD tenant.



5. If you want to use all features of Power BI Premium (except unlimited sharing), you need at least an A4 SKU. Select **Change size**.

Power BI Embedded

Basics * Tags Review + Create

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Visual Studio Enterprise

Resource group * ⓘ

(New) pbi-resource-group

Create new

RESOURCE DETAILS

Resource name * ⓘ

pbitestcapacity

Location * ⓘ

West Central US

Size * ⓘ

A1

1 v-core, Up to 3 GB Cache

[Change size](#)

Power BI capacity administrator * ⓘ

meganb@domain.microsoft.com

Select

[Review + Create](#)

[Next : Tags >](#)

6. Select a capacity size of A4, A5, or A6, which correspond to P1, P2, and P3. Prices in the following image are examples only.

Select the resource size

SKU	VIRTUAL CO...	MEMORY	DEDICATED INFRASTR...	COST (ESTIMATED/MONTH)
A1	1	Up to 3 GB Cache	No	\$750.03
A2	2	Up to 5 GB Cache	No	\$1,494.03
A3	4	Up to 10 GB Cache	Yes	\$2,994.00
A4	8	Up to 25 GB Cache	Yes	\$5,994.04
A5	16	Up to 50 GB Cache	Yes	\$11,994.02
A6	32	Up to 100 GB Cache	Yes	\$23,994.45

[Select](#)

Prices presented here are estimates in your local currency that include only Azure infrastructure costs and any subscription or location discounts. Final charges will be provided in your local currency, in cost analysis and billing views. [View the Azure pricing calculator.](#)

7. Select **Review + Create**, review the options you chose, then select **Create**.

Power BI Embedded

Basics * Tags Review + Create

BASICS

Subscription	Visual Studio Enterprise
Resource group	pbi-resource-group
Location	West Central US
Resource name	pbitestcapacity
Size	A3
Power BI capacity administrator	meganb@domain.microsoft.com

TAGS

(none)

Create

< Previous : Tags

Automation template

8. It can take a few minutes to complete the deployment. When it's ready, select **Go to resource**.

✓ Your deployment is complete



Deployment name: Microsoft.PowerBIDedicated
Subscription: Visual Studio Enterprise
Resource group: pbi-resource-group

Start time: 12/10/2019, 11:12:32 AM
Correlation ID: 2d24e4cc-e65e-44ca-9939-897646761028

▼ Deployment details ([Download](#))

^ Next steps

[Go to resource](#)

9. On the management screen, review the options you have for managing the service, including pausing the service when you're not using it.

The screenshot shows the Azure portal interface for managing a Power BI capacity named 'pbitestcapacity'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Scale (with Change size), Settings (Quick Start, Power BI capacity administrators, Properties, Locks, Export template), Monitoring (Alerts, Metrics, Diagnostic settings), and Support + troubleshooting (Resource health, New support request). The main content area is titled 'Essentials' and displays resource details:

	Resource name
Resource group (change)	pbi-resource-group
Status	SKU
Active	A3
Location	West Central US
Subscription name (change)	Visual Studio Enterprise
Subscription ID	ca116574-d723-4366-ab7b-a8c8f32b5dcc

After you purchase capacity, learn how to [manage capacities](#) and [assign workspaces](#) to a capacity.

Next steps

[What is Power BI Premium?](#) [How to purchase Power BI Premium](#) [Configure and manage capacities in Power BI Premium](#)

[Power BI pricing page ↗](#)

[Power BI Premium FAQ](#)

[Planning a Power BI Enterprise Deployment whitepaper ↗](#)

More questions? [Try asking the Power BI Community ↗](#)

Plan your transition to Power BI Premium Gen2

Article • 12/19/2022 • 4 minutes to read

This article provides information about key dates for migrating Power BI Premium capacity to the latest platform.

Over the last several months, we've been working to make many improvements to Power BI Premium. Changes include updates to licensing, performance, scaling, management overhead, and improved insight to utilization metrics. This next generation of Power BI Premium, referred to as Power BI Premium Gen2, has officially moved from preview to general availability as of October 4, 2021. You can learn more about the Premium Gen2 enhancements in the [Gen2 fundamentals and capacity analytics deep dive](#) webinar.

If your organization is using the [original version](#) of Power BI Premium, you're required to migrate to the modern Gen2 platform. Microsoft began migrating all Premium capacities to Gen2. If you have a Premium capacity that requires migrating, you'll receive an email notification 60 days before the migration is scheduled to start.

Premium Gen2 prerequisites

Power BI Premium Gen2 and [Embedded Gen2](#) support open-platform connectivity from Microsoft and third-party client applications and tools by using XMLA endpoints.

The article [Dataset connectivity with the XMLA endpoint](#) lists the minimum requirements for Power BI Premium, Premium Per User (PPU) and Embedded connectivity. In addition to these requirements, for dataset connectivity in Premium Gen2, you need to have the following:

- **Microsoft Excel** - Version 16.0.13612.10000 or higher
- **PowerShell cmdlets** - Version 21.1.18256 or higher
- **Server Profiler** - Version 18.9 or higher
- **SQL Server Management Studio (SSMS)** - Version 18.9 or higher
- **Visual Studio with Analysis Services projects (SSDT)** - Version 2.9.16 or higher

You also need to use the following [client libraries](#) when working with Gen2 capacities:

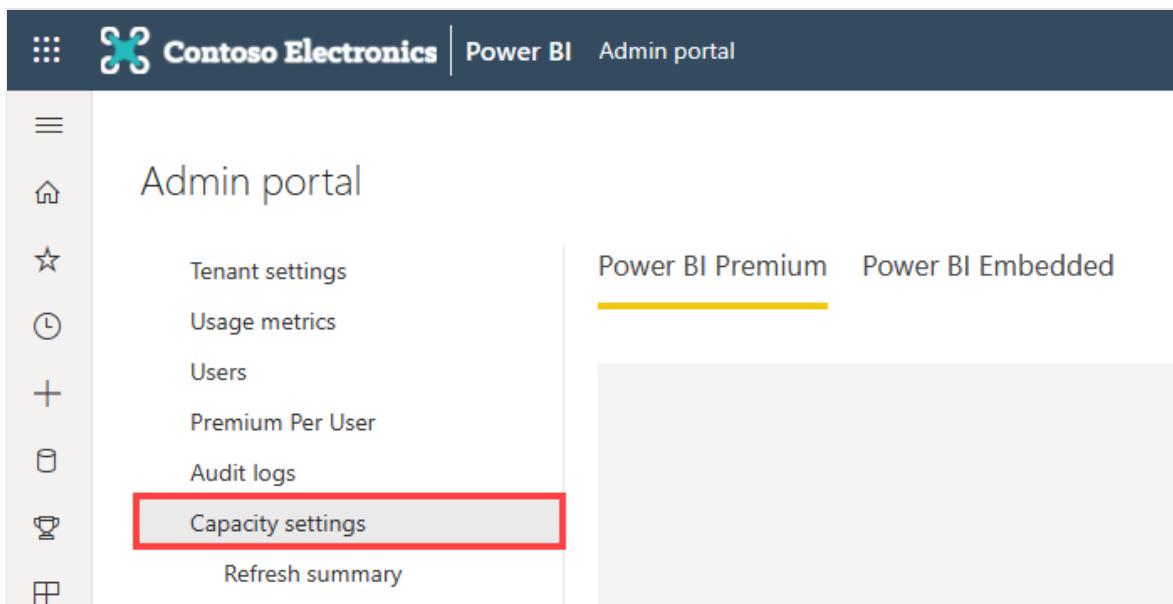
- ADOMD - Version 19.12.7.0 or higher
- AMO - Version 19.12.7.0 or higher
- MSOLAP - Version 15.1.65.22 or higher

Self-migration to Premium Generation 2

If you want to perform your own migration to the latest platform, it's easy to transition. You simply need to enable Premium Gen2 in the Power BI admin portal. Migrating doesn't interrupt your Power BI service and doesn't involve any additional costs. The change typically completes within a minute.

Ready for the next generation? Follow these steps:

1. Sign in to the [Power BI service](#) as a Power BI capacity admin.
2. From the navigation bar, select **Settings > Admin portal > Capacity settings**.



3. Select **Power BI Premium**.
4. If you have already allocated capacity, select it.
5. The section **Premium Generation 2** appears.
6. Select the slider to switch the setting to **Enabled**.

Transition from preview to Premium Gen 2 general availability

Customers using Power BI Premium Gen2 in preview don't need to take any action to transition to the general availability release. However, there are some key dates to consider if you've been using **Autoscale** to balance your capacity needs.

To date, organizations that have enabled Autoscale for capacities have gotten the burst processing benefits of Autoscale for free. Beginning **November 4, 2021** we'll begin charging for Autoscale cores. Take one of the following actions:

- You can continue to use Autoscale to enable the automatic use of additional cores during periods of higher-than normal demand on your capacities. Review the [pricing details for Premium per capacity add-ons](#) so that you're aware of upcoming charges.
- Or, to avoid Autoscale charges, disable the feature. Autoscale is an optional feature and benefit of the Premium Gen2 platform. You can choose to not use it.

Migration notification

Following the general availability of gen2, we'll begin to notify affected customers so that you can prepare your organization for changes. We'll post additional awareness, along with specific migration timelines to Microsoft 365 Message Center. Admins will receive 60 days advance notice of changes. The timeline will vary by cloud.

National cloud supportability

The following table describes Gen2 national cloud supportability. If a certain cloud environment has unsupported Gen2 features, they're also listed in the table.

 **Important**

China North isn't supported for any Gen2 features.

Environment	Supported	Unsupported features
U.S. Government Community Cloud (GCC)	✓	Autoscale
U.S. Government Community Cloud High (GCC High)	✓	

Frequently asked questions

This section answers frequently asked questions related to the migration.

- **Can I go back to Gen1?**

No.

- **Will I notice downtime during the migration?**

No downtime is expected. During a short interval that could last up to a minute, queries may take longer to run. If you're running refresh operations during the migration, they will stop and run again after the migration.

- **Do I need to prepare anything or make any changes before the migration?**

No. You don't need to move workspaces before the migration, or reassign workspaces after the migration.

- **Why do I need to change to Gen 2?**

Power BI is migrating everyone to Gen2.

- **What differences in Power BI can I expect after the migration?**

To see a full list of Gen2 benefits, see [What is Power BI Premium Gen2?](#) and [Power BI Premium Gen2 architecture](#).

- **Does Gen2 have limitations?**

For a full list of considerations and limitations, see [Considerations and limitations](#).

- **Do I need to update the capacity metrics app for Gen2?**

Yes, the Premium Gen2 platform requires that you download and use the [Power BI Premium Utilization and Metrics app](#).

Next steps

[What is Power BI Premium Gen2?](#)

[Using Autoscale with Power BI Premium](#)

[Install the Gen2 metrics app](#)

Managing Premium Gen2 capacities

Article • 12/15/2022 • 8 minutes to read

Managing Power BI Premium involves creating, managing, and monitoring Premium capacities. This article provides an overview of capacities; see [Configure and manage capacities](#) for step-by-step instructions.

Creating and managing capacities

The **Capacity Settings** page of the Power BI Admin portal displays the number of v-cores purchased and Premium capacities available. The page allows Global administrators or Power BI service administrators to create Premium capacities from available v-cores, or to modify existing Premium capacities.

Note

Power BI Premium recently released a new version of Premium, called **Premium Gen2**. Premium Gen2 simplifies the management of Premium capacities, and reduces management overhead. For more information, see [Power BI Premium Generation 2](#).

Note

You can also get Premium Per User (PPU) licenses for individuals, which provides many of the features and capabilities of a Premium capacity, and also incorporates all functionality included with a Power BI Pro license. For more information, see [Power BI Premium Per User](#).

When creating a Premium capacity, administrators are required to define:

- Capacity name (unique within the tenant).
- Capacity admin(s).
- Capacity size.
- Region for data residency.

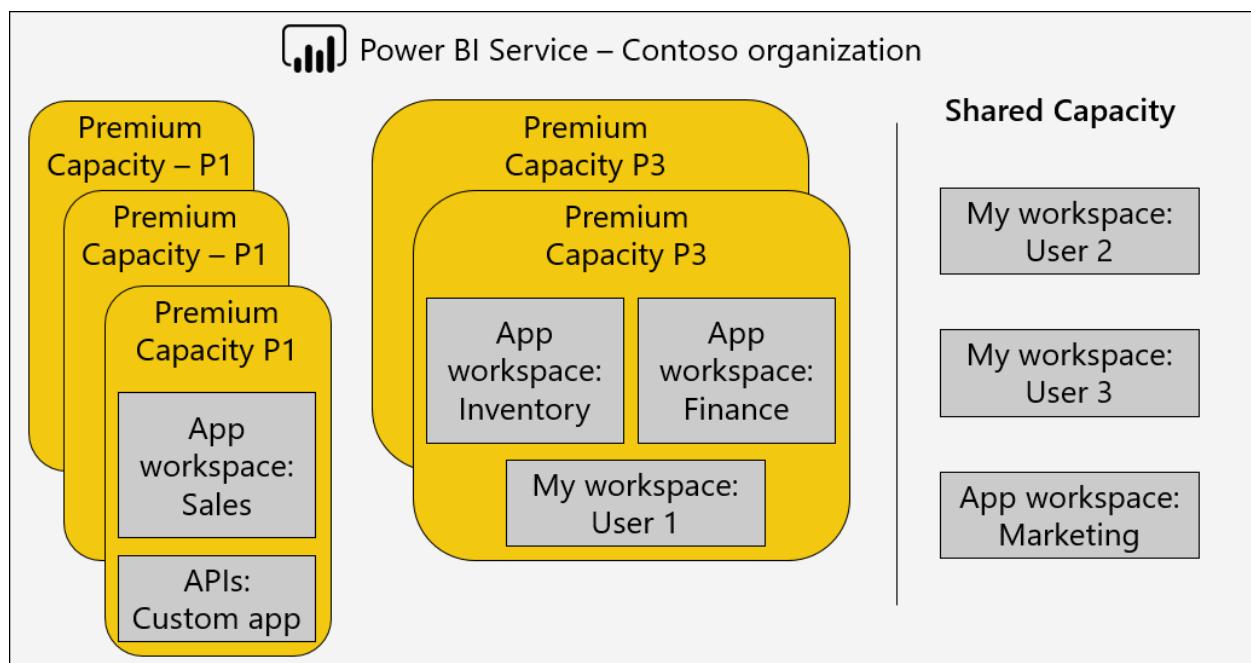
At least one Capacity Admin must be assigned. Users assigned as Capacity Admins can:

- Remove assigned workspaces from the capacity
- Manage user permissions and assign:
 - Additional Capacity Admins

- Contributors - Users who are allowed to assign workspaces to that capacity (Capacity Admins are automatically also Contributors)
- Manage Autoscale settings for that capacity
- Setup email alerts for resource utilization level
- Track capacity resources usage using the dedicated out of the box app

Capacity Admins cannot access workspace content unless explicitly assigned in workspace permissions. They also don't have access to all Power BI admin areas (unless explicitly assigned) such as usage metrics, audit logs, or tenant settings. Importantly, Capacity Admins do not have permissions to create new capacities or scale existing capacities. Admins are assigned on a per capacity basis, ensuring that they can only view and manage capacities to which they are assigned.

Capacity size is selected from an available list of SKU options, which is constrained by the number of available v-cores in the pool. It's possible to create multiple capacities from the pool, which could be sourced from one or more purchased SKUs. For example, a P3 SKU (32 v-cores) could be used to create three capacities: one P2 (16 v-cores), and two P1 (2 x 8 v-cores). The following image shows an example setup for the fictitious Contoso organization consisting of five Premium capacities (3 x P1, and 2 x P3) with each containing workspaces, and several workspaces in shared capacity.



A Premium capacity can be assigned to a region other than the home region of the Power BI tenant, known as multi-geo. Multi-geo provides administrative control over which datacenters within defined geographic regions your Power BI content resides. The rationale for a multi-geo deployment is typically for corporate or government compliance, rather than performance and scale. Report and dashboard loading still involves requests to the home region for metadata. To learn more, see [Multi-Geo support for Power BI Premium](#).

Power BI service administrators and Global Administrators can modify Premium capacities. Specifically, they can:

- Change the capacity size to scale-up or scale-down resources.
- Add or remove Capacity Admins.
- Add or remove users that have assignment permissions.

Note

Service and global administrators do not have access to capacity metrics unless explicitly added as capacity admins.

Contributor assignment permissions are required to assign a workspace to a specific Premium capacity. The permissions can be granted to the entire organization, specific users, or groups.

By default, Premium capacities support workloads associated with running Power BI queries. Premium capacities also support additional workloads: **AI (Cognitive Services)**, **Paginated Reports**, and **Dataflows**.

Deleting a Premium capacity is possible and won't result in the deletion of its workspaces and content. Instead, it moves any assigned workspaces to shared capacity. When the Premium capacity was created in a different region, the workspace is moved to shared capacity of the home region.

Capacities have limited resources, defined by each capacity SKU. Resources consumption by Power BI items (such as reports and dashboards) across capacities can be tracked using the [metrics app](#).

Assigning workspaces to capacities

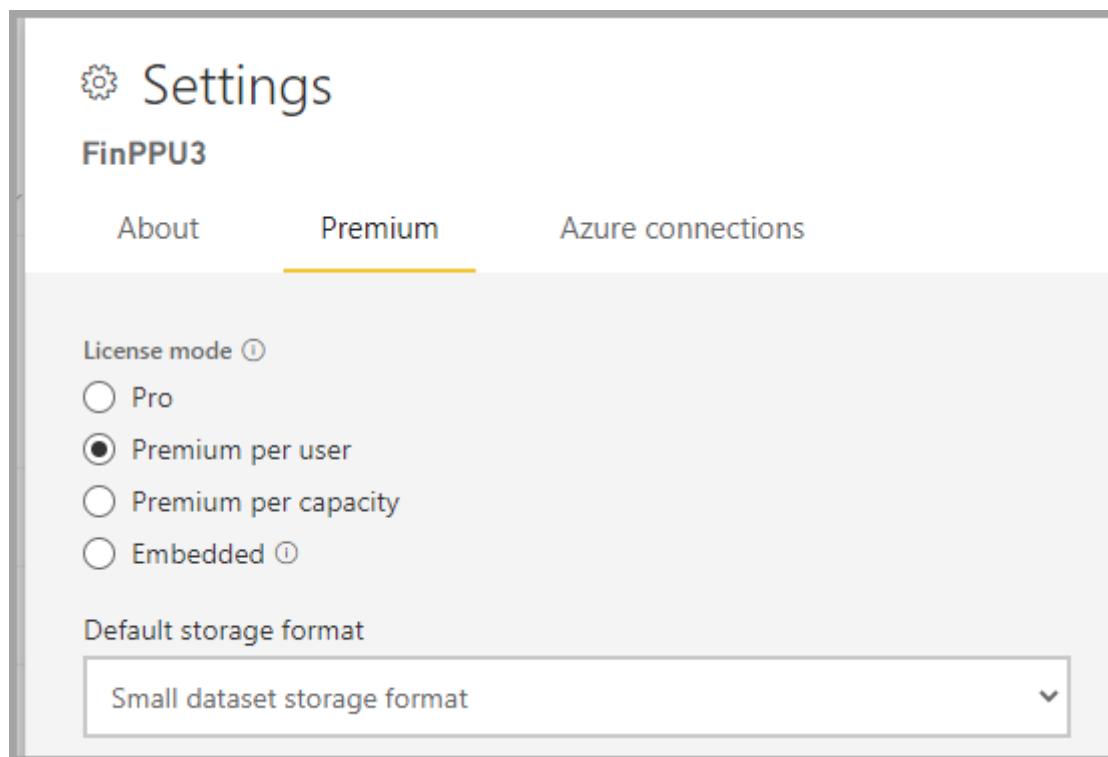
Workspaces can be assigned to a Premium capacity in the Power BI Admin portal or, for a workspace, in the **Workspace** pane.

Capacity Admins, as well as Global Administrators or Power BI service administrators, can bulk assign workspaces in the Power BI Admin portal. Bulk assigned can apply to:

- **Workspaces by users** - All workspaces owned by those users, including personal workspaces, are assigned to the Premium capacity. This will include the reassignment of workspaces when they are already assigned to a different Premium capacity. In addition, the users are also assigned workspace assignment permissions.

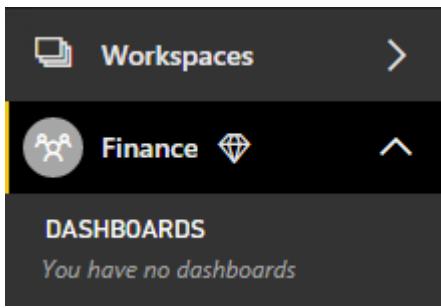
- Specific workspaces
- The entire organization's workspaces - All workspaces, including personal workspaces, are assigned to the Premium capacity. All current and future users are assigned workspace assignment permissions. This approach is not recommended. A more targeted approach is preferred.

You can enable Premium capabilities in a workspace by setting the proper license mode. To set a license mode, you must be both a workspace admin, and have assignment permissions. To enable Premium capabilities for P and EM SKUs, set the license mode to Premium per capacity. To enable Premium capabilities for A SKU's, set the license mode to Embedded. To enable Premium capabilities for Premium Per User (PPU), mark the license mode as Premium Per User. To remove a workspace from Premium, mark the workspace license mode as Pro.



Workspace admins can remove a workspace from a capacity (to shared capacity) without requiring assignment permission. Removing workspaces from reserved capacities effectively relocates the workspace to shared capacity. Note that removing a workspace from a Premium capacity may have negative consequences resulting, for example, in shared content becoming unavailable to Power BI Free licensed users, or the suspension of scheduled refresh when they exceed the allowances supported by shared capacities.

In the Power BI service, a workspace assigned to a Premium capacity is easily identified by the diamond icon that adorns the workspace name.



Planning your capacity size in advance

Different Premium capacity SKUs have different amounts of resources that are made available to support Power BI items (such as reports, dashboards and datasets) processed by each capacity. The SKUs differentiate by the number of standard v-cores they have. The most influential resources to consider when sizing in advance are:

- **CPU power** – The amount of CPU power each capacity has is a function of its base v-core and the number of [autoscale](#) cores it has (purchased in-advance and allocated in advance during capacity instantiation). The CPU power exhaustion of a capacity is measured by aggregating CPU power used across all the Power BI items it processes. The more operations done against more items, the higher the CPU spend.
- **Item size** - The size of a Power BI item relates to the amount of data available for processing inside the item. Size can have multiple dimensions depending on the item. Datasets size for example is determined by the footprint the dataset has in memory while being processed. Different items may have size measures that are defined differently. The size footprint across the capacity, unlike CPU, is not aggregated across all active items but is evaluated per item only. This means a capacity can support multiple items running concurrently if neither of those items exceeds the capacity size limit.

Due to the individually enforced nature of a Power BI item's size measure, the size usually dictates how big a capacity should be. For example, if you have a P1 SKU, datasets are supported up to a [limit of 25Gb](#). As long as your datasets do not exceed this value, the SKU should meet your needs. You can evaluate a typical dataset's size by measuring the memory footprint of the Power BI Desktop tool. A typical item's usage pattern will dictate its CPU power spend, which if exhausted can severely degrade report interaction performance for end-users. Therefore, once you have a typical report for evaluation, it will be beneficial to use that report in a load test, and evaluate the results to determine whether a higher SKU size or turning on autoscale is required.

How to decide when to turn on autoscale?

Using the Power BI Premium [Capacity Utilization and Metrics app](#) will indicate cases of overload impact in the *overloaded minutes* visual, in the overview page. You can evaluate the severity of the impact of those overload minutes by using the evidence page, where you can track how much impact an overload moment had, what Power BI items it impacted and how many users got affected. If based on your evaluation the impact is too high, you should turn on autoscale.

How to decide when to scale up to a higher SKU?

There are two different indicators that suggest you need to scale up your capacity:

- Using autoscale beyond a certain degree, is not economically viable. If your autoscaling patterns lead you to consume more than 25% of your capacity size on a regular basis, it may be less costly to upgrade your capacity to a higher SKU since your capacity CPU Power requirements are significantly higher than the capacity's original power. Here we consider over 25% as both how many cores got added and how long were they added for. For example, a P1 SKU with 8 v-cores that uses auto scale in a way that is equivalent to two additional cores consistently applied, will cost the same as a P2.
- The size of your Power BI items approach or exceed capacity limits. If the item size of any of the items reported in the metrics app approaches your capacity limit or exceeds it, operations against that item will fail. Therefore if a critical item approaches those limits (80% of the capacity size) it is advisable to consider upgrading the capacity in advance, to avoid interruption of service should that item exceed the capacity limit.

Next steps

[Using autoscale with Premium Gen2](#)

[Install the Gen2 metrics app](#)

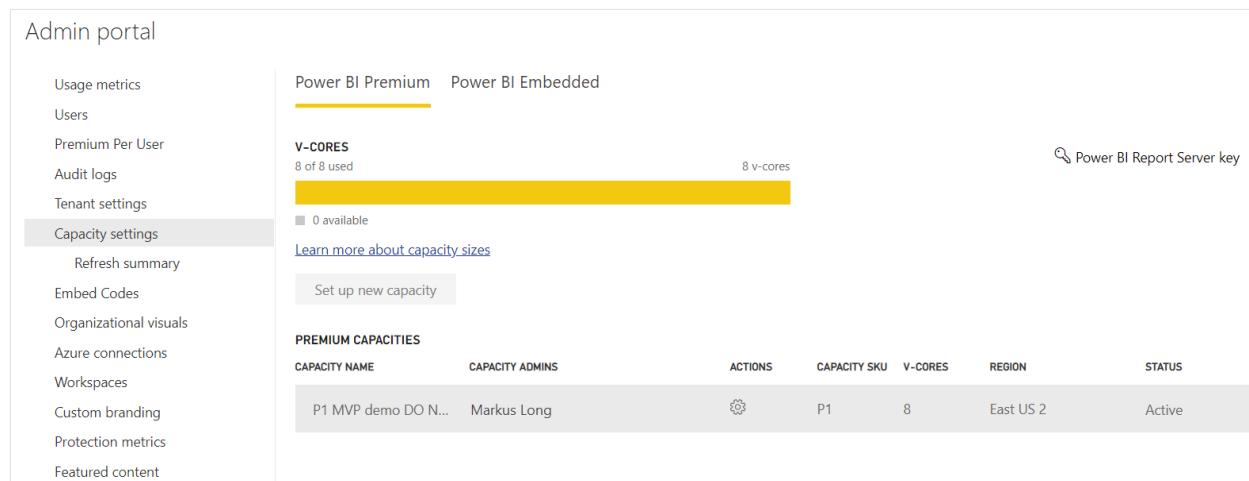
[Using the Premium Gen2 metrics app](#)

Configure and manage capacities in Power BI Premium

Article • 12/15/2022 • 6 minutes to read

Managing Power BI Premium involves creating, managing, and monitoring Premium capacities. This article provides step-by-step instructions; for an overview of capacities.

Learn how to manage Power BI Premium and Power BI Embedded capacities, which provide reserved resources for your content.



The screenshot shows the 'Admin portal' interface. On the left, a sidebar lists various administrative options: Usage metrics, Users, Premium Per User, Audit logs, Tenant settings, Capacity settings (which is selected), Refresh summary, Embed Codes, Organizational visuals, Azure connections, Workspaces, Custom branding, Protection metrics, and Featured content. The main area is divided into two tabs: 'Power BI Premium' (selected) and 'Power BI Embedded'. Under 'Power BI Premium', there's a 'V-CORES' section showing '8 of 8 used' with a progress bar and a link to 'Learn more about capacity sizes'. A 'Set up new capacity' button is also present. Below this is a table titled 'PREMIUM CAPACITIES' with columns: CAPACITY NAME, CAPACITY ADMINS, ACTIONS, CAPACITY SKU, V-CORES, REGION, and STATUS. It lists one capacity: 'P1 MVP demo DO N...' with 'Markus Long' as the admin, actions icon, P1 SKU, 8 v-cores, 'East US 2' region, and 'Active' status.

Capacity is at the heart of the Power BI Premium and [Power BI Embedded](#) offerings. It is a set of resources reserved for exclusive use by your organization. Having a capacity enables you to publish dashboards, reports, and datasets to users throughout your organization without having to purchase per-user licenses for them. It also offers dependable, consistent performance for the content hosted in capacity. For more information, see [What is Power BI Premium?](#).

ⓘ Note

- Premium Gen2 simplifies the management of Premium capacities, and reduces management overhead.
- You can get **Premium Per User (PPU)** licenses for individuals, which provide many of the features and capabilities of a Premium capacity, and incorporate all functionality included with a Power BI Pro license.

Manage capacity

After you have purchased capacity nodes in Microsoft 365, you set up the capacity in the Power BI admin portal. You manage Power BI Premium capacities in the **Capacity settings** section of the portal.

The screenshot shows the 'Admin portal' interface. On the left, there's a sidebar with links: Usage Metrics, Users, Audit logs, Tenant settings, and Capacity settings (which is highlighted with a red box). The main area is titled 'Power BI Premium' (with a yellow underline) and 'Power BI Embedded'. It displays 'V-CORES' usage: '3 of 20 used' (yellow bar) and '17 available' (grey bar). There's a link 'Learn more about capacity sizes' and a yellow button 'Set up new capacity'. Below this, under 'PREMIUM CAPACITIES', there are columns for 'CAPACITY NAME' and 'CAPACITY ADM'. A red box highlights the 'Contoso Sales' capacity name.

You manage a capacity by selecting the name of the capacity. This takes you to the capacity management screen.

The screenshot shows the 'PREMIUM CAPACITIES' screen. A red box highlights the 'Contoso Sales' capacity name, which is being clicked (indicated by a hand cursor icon). A large red arrow points from this click to a detailed view of the capacity. The detailed view includes sections for 'CAPACITY NAME' (Contoso Sales), 'CAPACITY ADMINS' (Michel AbdElmalik), 'CAPACITY SIZE' (This capacity is a P1, which is 8 v-cores), 'USER PERMISSIONS' (Capacity admins), and a 'Start using this capacity' section with a 'Assign workspace' button. An illustration of a laptop displaying charts is shown in the background.

If no workspaces have been assigned to the capacity, you will see a message about [assigning a workspace to the capacity](#).

Renew your capacity

Each capacity has a certain amount of v-cores allocated to it. When the v-cores expire, your capacity stops working. To renew your capacity, visit the [Microsoft 365 admin center](#).

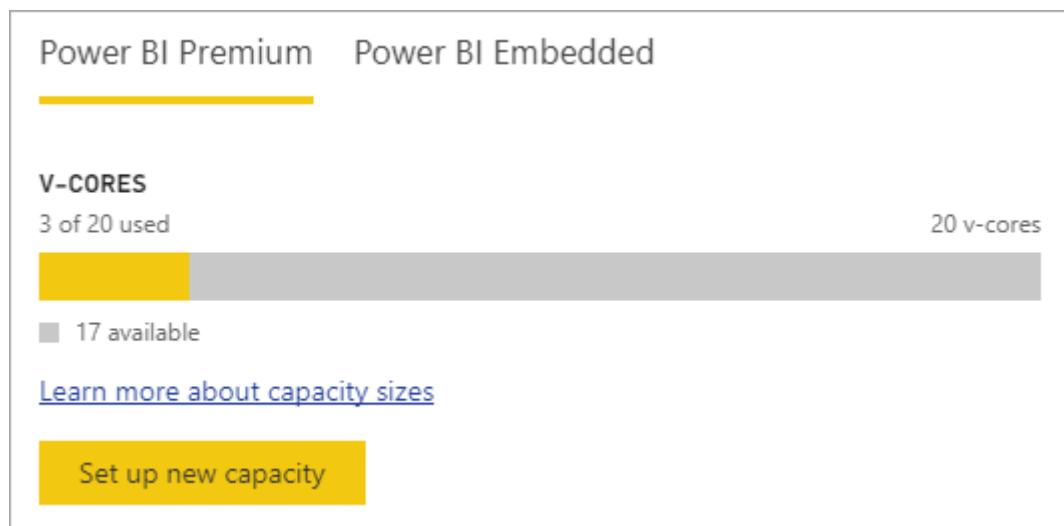
Note

If your v-cores expire, you may see this error in the Power BI admin portal:

One or more of your premium capacity v-cores have expired. Please contact your tenant administrator or Microsoft account representative to learn whether these v-cores will be renewed.

Setting up a new capacity (Power BI Premium)

The admin portal shows the number of *virtual cores* (v-cores) that you have used and that you still have available. The total number of v-cores is based on the Premium SKUs that you have purchased. For example, purchasing a P3 and a P2 results in 48 available cores – 32 from the P3 and 16 from the P2.



If you have available v-cores, set up your new capacity by following these steps.

1. Select **Set up new capacity**.
2. Give your capacity a name.

3. Define who the admin is for this capacity.
4. Select your capacity size. Available options are dependent on how many available v-cores you have. You can't select an option that is larger than what you have available.

CAPACITY SIZE

Available v-cores

8 of 17 used 17 v-cores

Capacity size *

P1 - 8 v-cores

Select capacity size

P1 - 8 v-cores

P2 - 16 v-cores

P3 - 32 v-cores

EM1 - 1 v-cores

EM2 - 2 v-cores

EM3 - 4 v-cores

5. Select Set up.

Power BI Premium > Set up new capacity

Please take a minute to set up your new Premium capacity.

* Required

Capacity name

Contoso Sales

Capacity admins *

Michel AbdElmalik Enter email addresses

CAPACITY SIZE

Available v-cores

8 of 17 used 17 v-cores

Capacity size *

P1 - 8 v-cores

[Learn more about capacity sizes](#)

Set up Cancel

Capacity admins, as well as Power BI admins and global administrators, then see the capacity listed in the admin portal.

Capacity settings

1. In the Premium capacity management screen, under Actions, select the gear icon to review and update settings.

ACTIONS	SKU	V-CORES
	P1	8

2. You can see who the service admins are, the SKU/size of the capacity, and what region the capacity is in.

Settings for Contoso Sales

Capacity name	Contoso Sales
SERVICE ADMIN	
Colin Murphy	colin@granularcontrols1.onmicrosoft.com
Michel AbdElmalik	admin@granularcontrols1.onmicrosoft.com
Nancy Leary	nancy@granularcontrols1.onmicrosoft.com
Tim Larson	tim@granularcontrols1.onmicrosoft.com
SKU/SIZE	P1
REGION	Central US

3. You can also rename or delete a capacity.

 Delete Capacity	Apply	Cancel
---	-------	--------

ⓘ Note

Power BI Embedded capacity settings are managed in the Microsoft Azure portal.

Change capacity size

Power BI admins and global administrators can change Power BI Premium capacity. Capacity admins who are not a Power BI admin or global administrator don't have this option.

1. Select the capacity name you want to change the size of.
2. Select **Change size**. You can see the

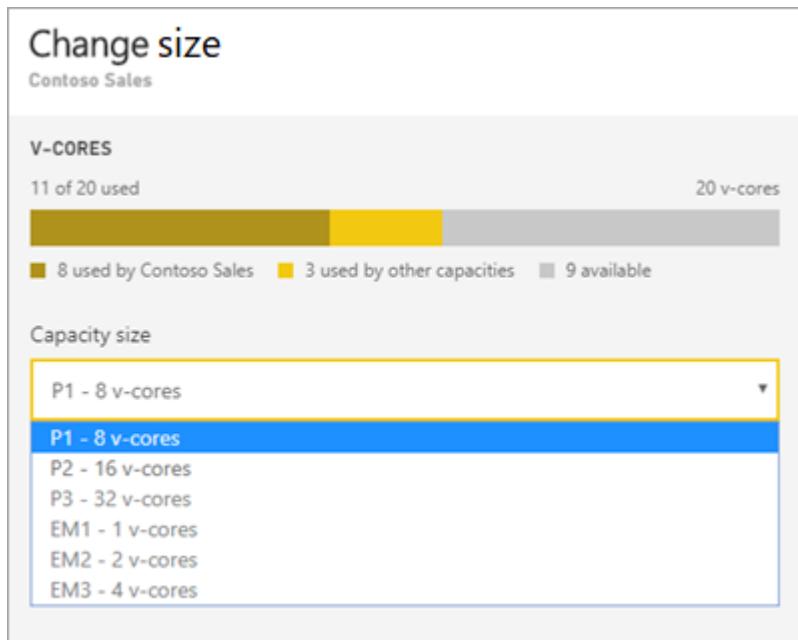
The Premium SKU size you purchased is a P1, which gives you access to 8 v-cores.

Change size

3. On the **Change size** screen, upgrade or downgrade your capacity as appropriate.

ⓘ Note

To upgrade to a P4 or a P5 capacity you need to **buy** a few smaller SKUs that will add up to the size of the capacity you want.



Administrators are free to create, resize and delete nodes, so long as they have the requisite number of v-cores.

P SKUs cannot be downgraded to EM SKUs. You can hover over any disabled options to see an explanation.

 **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. See [capacity and reliability notifications](#) for more information.

Manage user permissions

You can assign additional capacity admins, and assign users that have *contributor* permissions. Users that have contributor permissions can assign a workspace to a capacity if they are an admin of that workspace. They can also assign their personal *My Workspace* to the capacity. Users with contributor permissions do not have access to the admin portal.

 **Note**

For Power BI Embedded, capacity admins are defined in the Microsoft Azure portal.

Expand **Contributor permissions**, then add users or groups as appropriate.

- ▶ Capacity usage report
- ▶ Notifications
- ◀ Contributor permissions
Enabled for the entire organization

People who can add or remove workspaces in this capacity.

Apply to:

- The entire organization
- Specific users or groups

Apply

Discard

Assign a workspace to a capacity

There are two ways to assign a workspace to a capacity: in the admin portal; and from a workspace.

Assign from the admin portal

Capacity admins, along with Power BI admins and global administrators, can bulk assign workspaces in the premium capacity management section of the admin portal. When you manage a capacity, you see a **Workspaces assigned to this capacity** section that allows you to assign workspaces.

◀ Workspaces assigned to this capacity

Search for, add, or remove workspaces assigned to this capacity

Search workspaces X Remove all **+ Assign workspaces**

Workspace name ↑	Workspace admins	Actions ⓘ	Status ↑↓
 !CapacityChecker	View admins	X	Assigned
 !CapacityChecker	View admins	X	Assigned

1. Select **Assign workspaces**.
2. Select an option for **Apply to**.

Assign workspaces

Apply to:

- Workspaces by users
- Specific workspaces
- The entire organization's workspaces

(i) Assigning the entire organization's workspaces to dedicated capacity gives all current and future users the permission to reassign individual workspaces to this capacity. This dedicated capacity will become the organization's default capacity. [Learn more](#)

Apply

Cancel

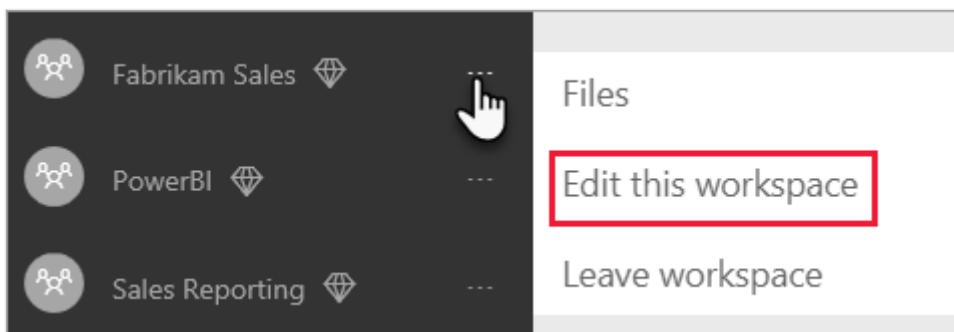
Selection	Description
Workspaces by users	When you assign workspaces by user, or group, all the workspaces that the user or group is admin of become part of the Premium capacity, including the user's personal workspace. The users automatically get workspace assignment permissions. This includes workspaces already assigned to a different capacity.
Specific workspaces	Enter the name of a specific workspace to assign to the selected capacity.
The entire organization's workspaces	Assigning the entire organization's workspaces to Premium capacity assigns all workspaces and My Workspaces, in your organization, to this Premium capacity. In addition, all current and future users will have the permission to reassign individual workspaces to this capacity.

3. Select **Apply**.

Assign from workspace settings

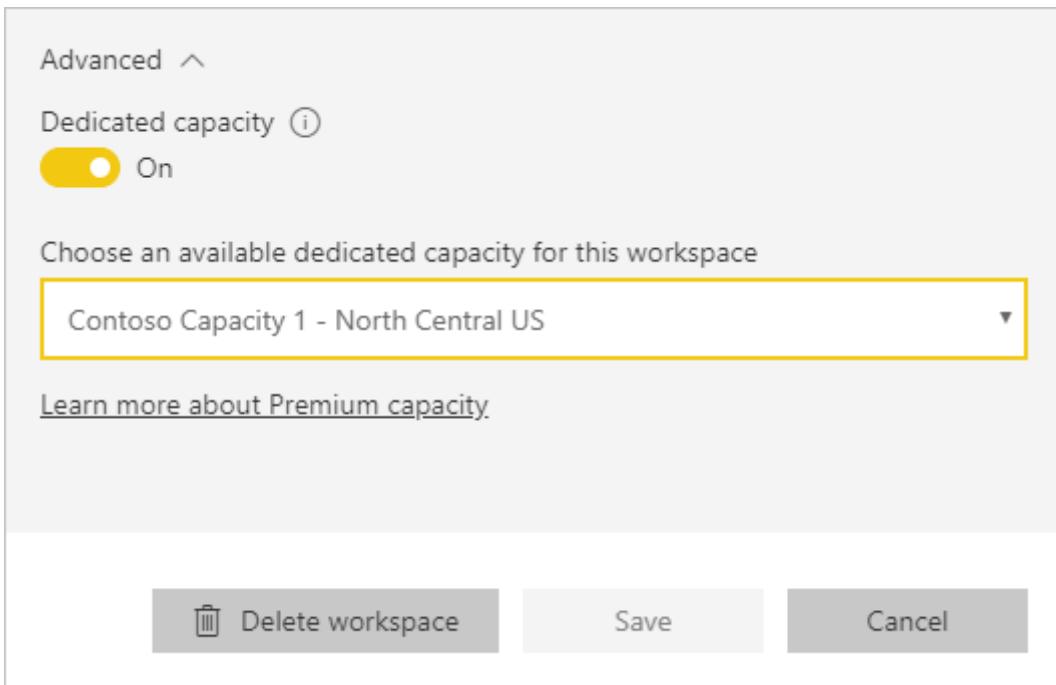
You can also assign a workspace to a Premium capacity from the settings of that workspace. To move a workspace into a capacity, you must have admin permissions to that workspace, and also capacity assignment permissions to that capacity. Note that workspace admins can always remove a workspace from Premium capacity.

1. Edit a workspace by selecting the ellipsis (...) then selecting **Edit this workspace**.



2. Under **Edit this workspace**, expand **Advanced**.

3. Select the capacity that you want to assign this workspace to.



4. Select **Save**.

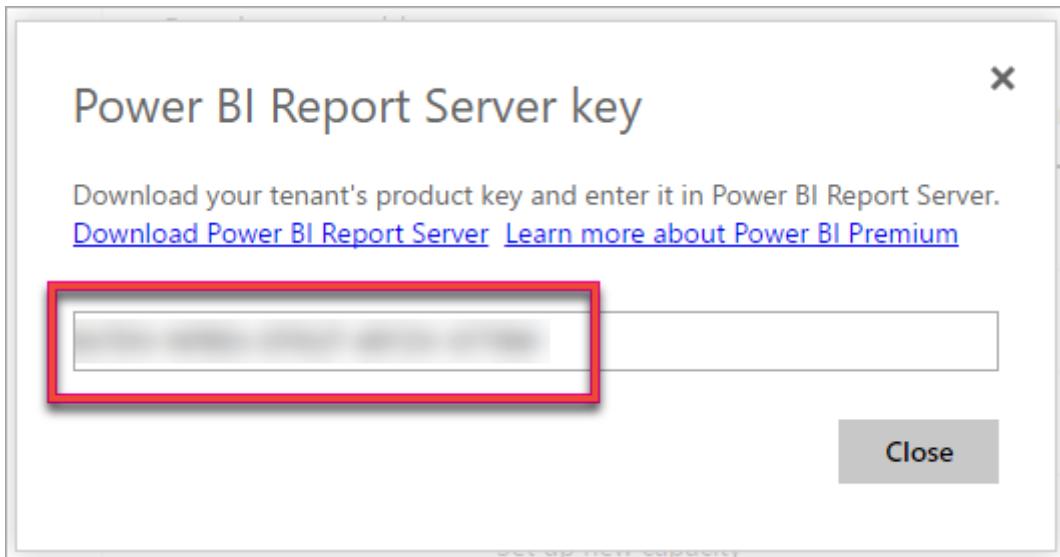
Once saved, the workspace and all its contents are moved into Premium capacity without any experience interruption for end users.

Power BI Report Server product key

On the **Capacity settings** tab of the Power BI admin portal, you will have access to your Power BI Report Server product key. This will only be available for Global Admins or users assigned the Power BI service administrator role and if you have purchase a Power BI Premium SKU.

The screenshot shows the 'Power BI Premium' section of the Azure portal. It displays the current usage of v-cores (11 of 20 used) and a progress bar indicating 20 v-cores. A red box highlights the search bar labeled 'Power BI Report Server key'. Below this, there's a link to learn more about capacity sizes and a button to 'Set up new capacity'. A table titled 'PREMIUM CAPACITIES' lists one entry: 'Contoso Sales' with 'Michel AbdElmalik' as the capacity admin, SKU P1, 8 v-cores, and an 'Active' status.

Selecting **Power BI Report Server key** will display a dialog contain your product key. You can copy it and use it with the installation.



For more information, see [Install Power BI Report Server](#).

Next steps

[Managing Premium capacities](#)

More questions? [Try asking the Power BI Community](#) ↗

Power BI has released Power BI Premium Gen2, which improves the Power BI Premium experience with improvements in the following:

- Performance
- Per-user licensing
- Greater scale
- Improved metrics
- Autoscaling
- Reduced management overhead

For more information about Power BI Premium Gen2, see [Power BI Premium Generation 2](#).

Premium Gen2 capacity load evaluation

Article • 12/12/2022 • 4 minutes to read

Tip

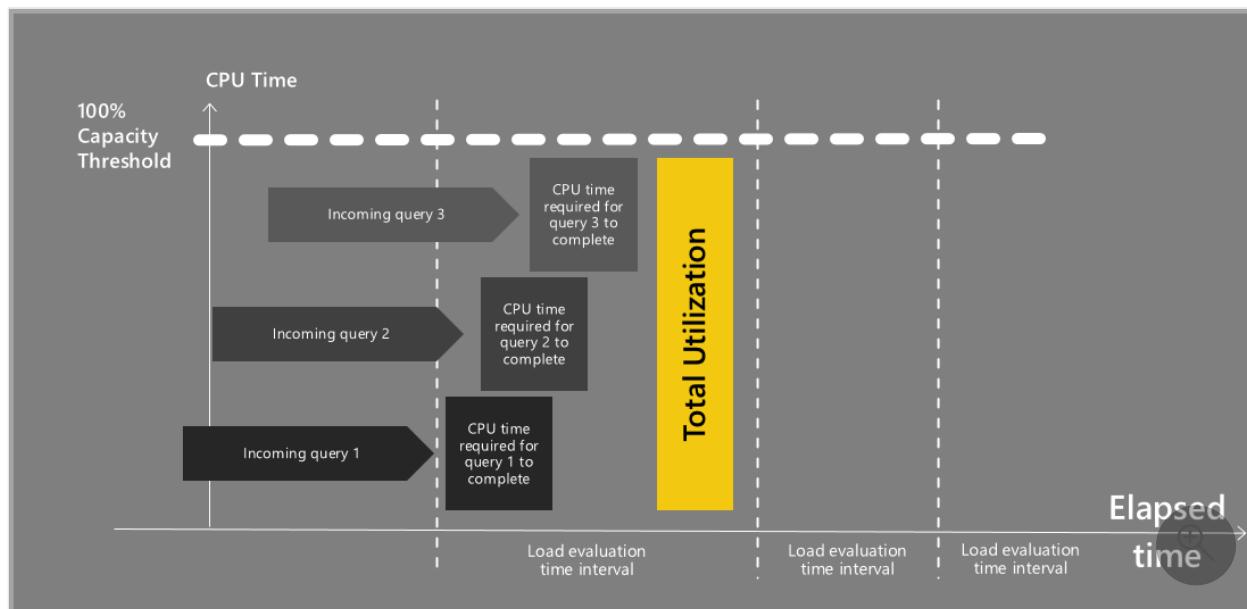
This article explains how to evaluate your Gen2 capacity load. It covers concepts such as *overload* and *autoscale*. You can also watch these videos which illustrate some of the Gen2 features described in this article.

- [Gen2 fundamentals and capacity analytics deep dive ↗](#)
- [Gen2 features breakdown ↗](#)

To enforce CPU throughput limitations, Power BI evaluates the throughput from your Premium Gen2 capacity on an ongoing basis.

Power BI evaluates throughput every **30 seconds**. It allows operations to complete, collects execution time on the shared pool physical node's CPUs, and then for all operations on your capacity, aggregates them into **30-second CPU intervals** and compares the results to what your purchased capacity is able to support.

The following image illustrates how Premium Gen2 evaluates and completes queries.



Let's look at an example: A P1 with eight v-cores can support $8 \times 30 = 240$ seconds of v-core execution time, also known as *CPU time*.

The aggregation is complex. It uses specialized algorithms for different workloads, and for different types of operations, as described in the following points:

- **Slow-running operations**, such as dataset and dataflow refresh, are considered *background operations* since they typically run in the background and users don't actively monitor them or look at them visually. Background operations are lengthy and require significant CPU power to complete during the long process. Power BI spreads CPU costs of background operations over 24 hours, so that capacities don't hit maximum resource usage due to too many refreshes running simultaneously. This allows Power BI Premium Gen2 subscribers to run as many background operations as allowed by their purchased capacity SKU, and doesn't limit them like the original Premium generation.
- **Fast operations** like queries, report loads, and others are considered *interactive operations*. The CPU time required to complete those operations is aggregated, to minimize the number of 30-seconds windows that are impacted following that operation's completion.

Premium Gen2 background operation scheduling

Refreshes are run on Premium Gen2 capacities at the time they are scheduled, or close to it, regardless of how many other background operations were scheduled for the same time. Datasets and dataflows being refreshed are placed on a physical processing node that has enough memory available to load them, and then begin the refresh process.

While processing the refresh, datasets may consume more memory to complete the refresh process. The refresh engine makes sure no item can exceed the amount of memory that their base SKU allows them to consume (for example, 25 GB on a P1 subscription, 50 GB on a P2 subscription, and so on).

How capacity size limits are enforced when viewing reports

Premium Gen2 evaluates utilization by aggregating utilization records every 30 seconds. Each evaluation consists of 2 different aggregations:

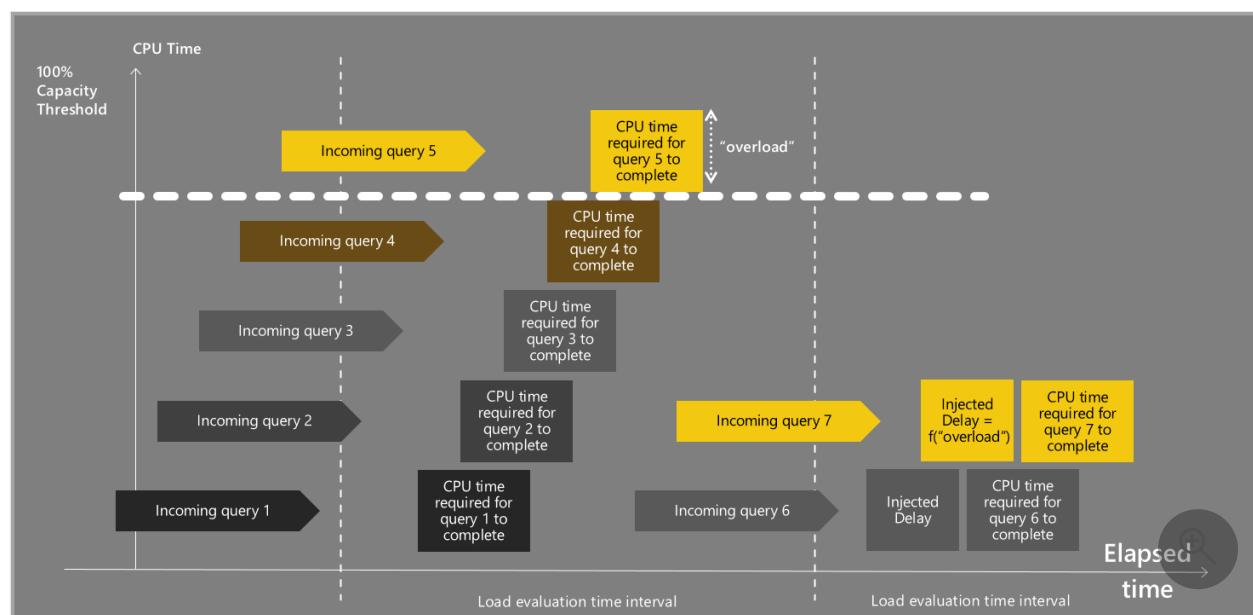
- Interactive utilization
- Background utilization

Interactive utilization is evaluated by considering all interactive operations that completed on or near the current 30-second evaluation cycle.

Background utilization is evaluated by considering all the background operations that completed during the past 24 hours. Each background operation contributes only 1/2880 of its total CPU cost (2880 is the number of evaluation cycles in a 24-hour period).

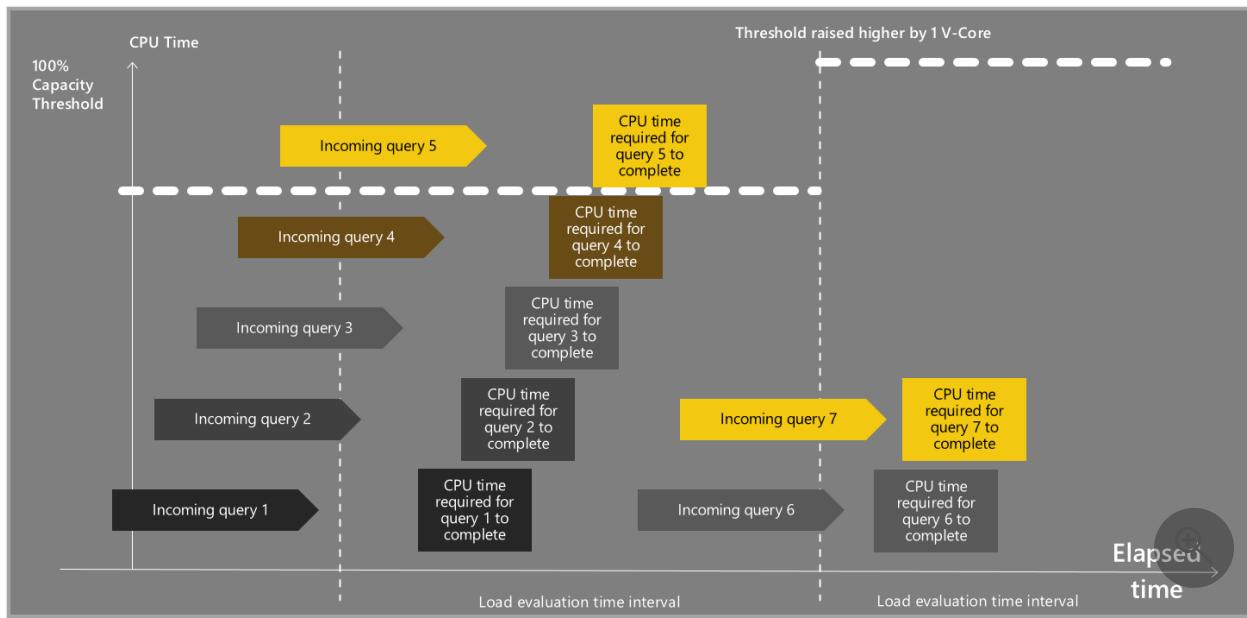
Each capacity consists of an defined number of v-cores. The CPU time measured in utilization records reflects the v-cores' utilization, and that utilization drives the need to autoscale.

If you have a P1 subscription with eight v-cores, each evaluation cycle quota equates to $8 \times 30 = 240$ seconds of CPU utilization. If the sum of both interactive and background utilizations *exceeds* the total v-core quote in your capacity, and you have *not* optionally enabled autoscale, the workload for your Gen2 capacity will exceed your available resources, also called your *capacity threshold*. The following image illustrates this condition, called *overload*, when autoscale is *not* enabled.



In contrast, if autoscale is optionally enabled, if your CPU utilizations exceeds the total v-core quota in your capacity, your capacity is automatically autoscaled (raised) by one v-core for the next 24 hours.

The following image shows how autoscale works.



Autoscale always considers your current capacity size to evaluate how much you use. When you autoscale, one v-core is added to your capacity. This means that if you're using a P1 SKU with eight v-cores, your maximum capacity is now at 270 seconds ($8 \times 30 + 1 \times 30$) of CPU time in an evaluation cycle.

Autoscale always ensures that no single interactive operation can account for all of your capacity, and you must have two or more operations occurring in a single evaluation cycle to initiate autoscale.

Using Premium Gen2 without autoscale

If a capacity's utilization exceeded 100% of its resources, and it cannot initiate autoscale due to autoscale being turned off, or already being at its maximum v-core value, the capacity enters a temporary *interactive request delay* mode. During the *interactive request delay* mode, each interactive request (such as a report load, visual interaction, and others) is delayed before it is sent to the engine for execution.

The capacity stays in *interactive request delay* mode if the previous evaluation is evaluated at greater than 100% resource utilization.

Configure autoscale

To configure autoscale on a Power BI Premium Gen2 capacity, follow the instructions in [Using Autoscale with Power BI Premium](#).

Next steps

[What is Power BI Premium Gen2?](#)

[Power BI Premium Gen2 architecture](#)

[Using Autoscale with Power BI Premium](#)

[Power BI Premium Gen2 FAQ](#)

[Power BI Premium Per User FAQ \(preview\)](#)

[Add or change Azure subscription administrators](#)

More questions? [Try asking the Power BI Community ↗](#)

Install the Gen2 metrics app

Article • 03/09/2022 • 4 minutes to read

The *Power BI Premium Utilization and Metrics* app is designed to provide monitoring capabilities for Power BI Gen2 Premium capacities. Use this guide to install the app. Once the app is installed, you can [learn how to use it](#).

ⓘ Note

The app is updated regularly with new features and functionalities. If you see there's a pending update in the notifications center, we recommend that you update the app.

Prerequisites

Before you install the Gen2 metrics app, review these requirements:

- You need to be a capacity admin
- The app only works with Gen2 capacities

Install the app

Follow the steps below according to the type of installation you need.

ⓘ Note

If you're installing the app in a government cloud environment, use one of the links below. You can also use these links to upgrade the app. When upgrading, you don't need to delete the old app.

- Microsoft 365 Government Community Cloud (GCC) ↗
- Microsoft 365 Government Community Cloud High (GCC High) ↗
- Microsoft 365 Department of Defense (DoD) ↗
- Power BI for China cloud ↗

First time installation

To install the *Power BI Premium Capacity Utilization and Metrics* app for the first time, follow these steps:

1. Select one of these options to get the app from AppSource:
 - Go to [AppSource > Power BI Premium Capacity Utilization and Metrics](#) and select **Get it now**.
 - In Power BI service, do the following:
 - a. Select **Apps**.
 - b. Select **Get apps**.
 - c. Search for **Power BI Premium**.
 - d. Select the **Power BI Premium Capacity Utilization and Metrics** app.
 - e. Select **Get it now**.
2. When prompted, sign in to AppSource using your Microsoft account and complete the registration screen. The app will take you to the Power BI service to complete the process. Select **Install** to continue.

One more thing ...



Power BI Premium Capacity Utilization and Metrics

By Microsoft

This app requires some basic profile information. We have pulled your Microsoft Account data to help you get started. AppSource will save your information for next time.

Name *

Work email *

Job title

Company

Country / region *



Phone number *

I give Microsoft permission to use or share my account information so that the provider or Microsoft can contact me regarding this product and related products. I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of AppSource is governed by separate [terms](#) and [privacy](#).

Continue

3. In the *Install this Power BI app* window, select **Install**.

Install this Power BI app?



Power BI Premium Capacity Utilization and Metrics

by Microsoft

[View in AppSource](#)

Apps may contain security or privacy risks. Only install apps from trusted authors and sources.

[Learn more](#)

By installing this app I agree to the publisher's [privacy policy](#) and [terms of service](#)

Install

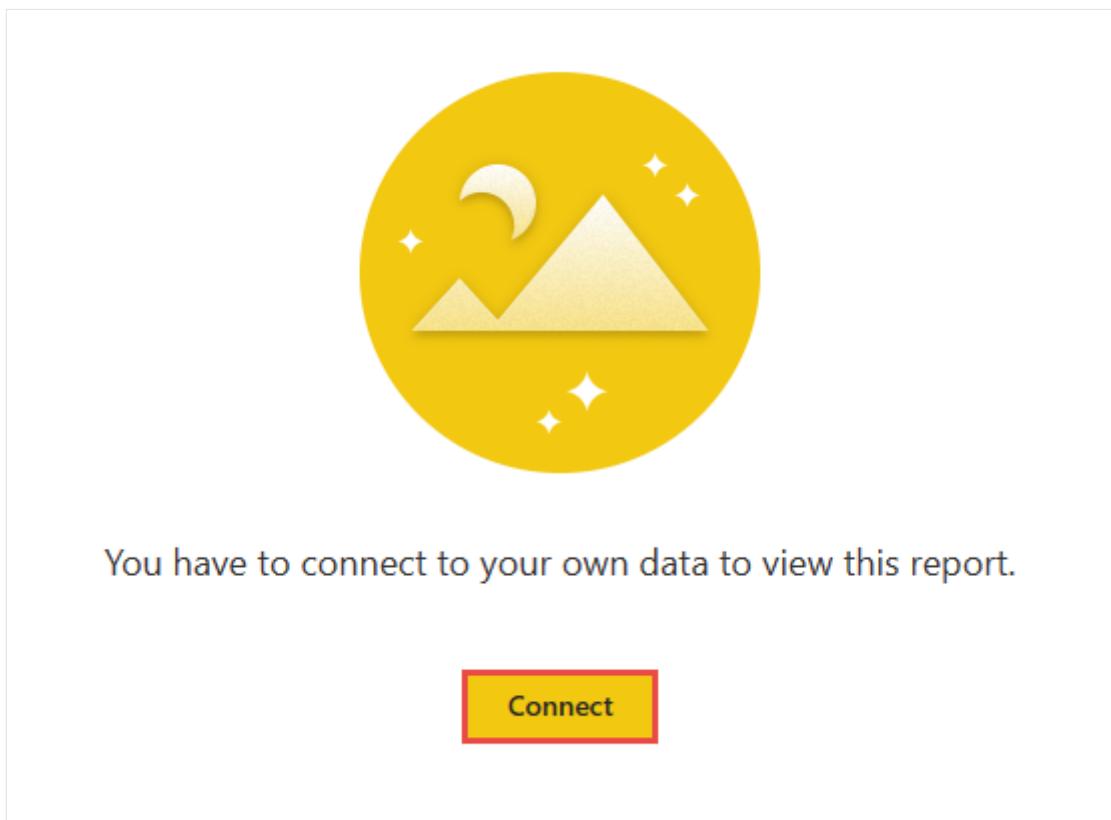
Cancel

4. Wait a few seconds for the app to install.

Run the app for the first time

To complete the installation, you need to configure the Power BI Premium utilization and metrics app by running it for the first time.

1. In Power BI service, select **Apps**.
2. Select the **Premium Capacity Utilization And Metrics** app.
3. when you see the message *You have to connect to your own data to view this report*, select **Connect**.



4. In the **Connect to Premium Capacity Utilization And Metrics** first window, fill in the fields according to the table below:

Field	Required	Value	Notes

Field	Required	Value	Notes
CapacityID	Yes	An ID of a capacity you're an admin of	<p>You can find the capacity ID in the URL of the capacity management page. In the Power BI service, go to Settings > Admin portal > Capacity settings, then select a Gen2 capacity. The capacity ID is shown in the URL after <code>/capacities/</code>. For example, <code>9B77CC50-E537-40E4-99B9-2B356347E584</code> is the capacity ID in this URL: https://app.powerbi.com/admin-portal/capacities/9B77CC50-E537-40E4-99B9-2B356347E584.</p> <p>Once installed, the app will let you see all the capacities you can access.</p>
UTC_offset	Yes	Numerical values ranging from <code>14</code> to <code>-12</code> . To signify a Half hour timezone, use <code>.5</code> . For example, for Iran's standard time enter <code>3.5</code> .	Enter your organization's standard time in Coordinated Universal Time (UTC).
Timepoint	Automatically populated		This field is automatically populated and is used for internal purposes. The value in this field will be overwritten when you use the app.
Timepoint2	Automatically populated		This field is automatically populated and is used for internal purposes. The value in this field will be overwritten when you use the app.
Advanced	Optional	On or Off	The app automatically refreshes your data at midnight. This option can be disabled by expanding the <i>advanced</i> option and selecting Off.

5. Select **Next**.

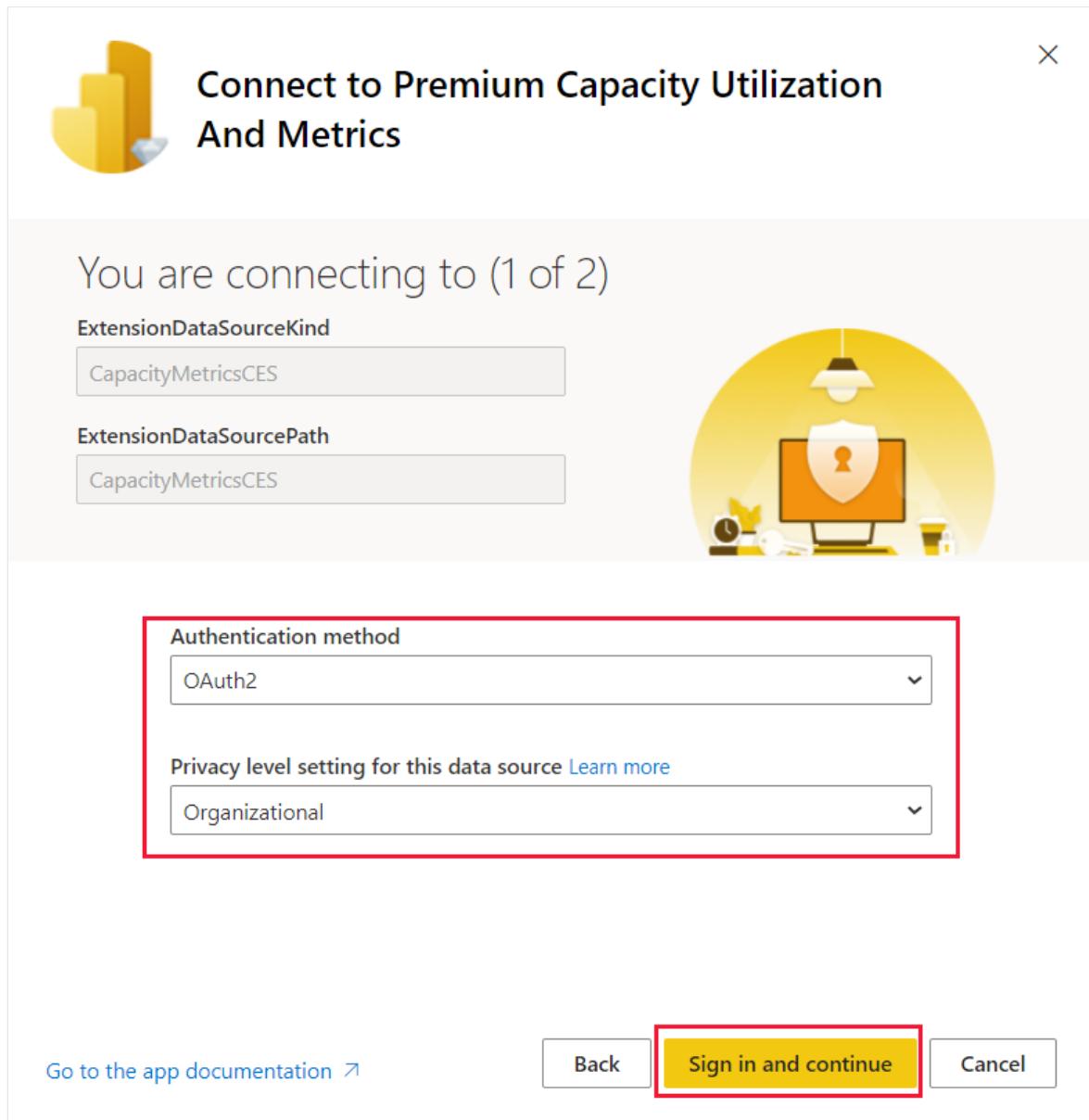
6. In the Connect to Premium Capacity Utilization And Metrics second window, fill in the following fields:

- **Authentication method** - Select your authentication method. The default authentication method is *OAuth2*.
- **Privacy level setting for this data source** - Select *Organizational* to enable app access to all the data sources in your organization.

 **Note**

ExtensionDataSourceKind and *ExtensionDataSourcePath* are internal fields related to the app's connector. Do not change the values of these fields.

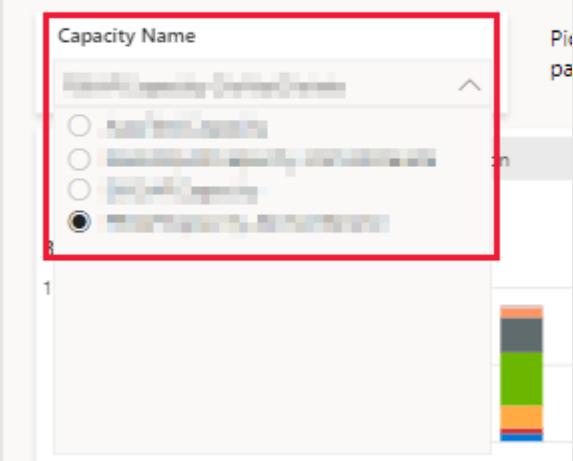
7. Select **Sign in and continue**.



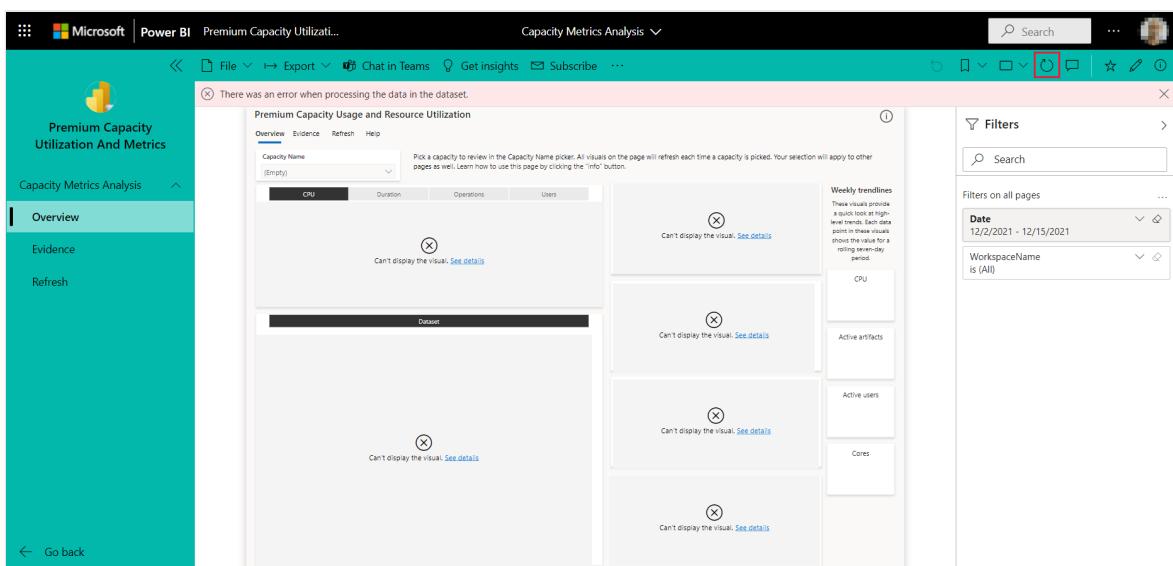
8. Select a capacity from the **capacity name** dropdown.

Premium Capacity Usage and Resource Utilization

Overview Evidence Refresh Help



9. After configuring the app, it may take a few minutes for the app to get your data. If you run the app and it's not displaying any data, refresh the app. This behavior happens only when you open the app for the first time.



Next steps

Use the gen2 metrics app

Use the Gen2 metrics app

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

The Power BI Premium utilization and metrics app is designed to provide monitoring capabilities for Power BI Gen2 Premium capacities. Monitoring your capacities is essential for making informed decisions on how to best use your Premium capacity resources. For example, the app can help identify when to scale up your capacity or when to turn on [autoscale](#).

ⓘ Note

When turning on autoscale, make sure there are no [Azure policies](#) preventing autoscale from working.

The app is updated often with new features and functionalities and provides the most in-depth information into how your capacities are performing.

To [install the Gen2 metrics app](#), you must be a capacity admin. Once installed, anyone in the organization with the right permissions can view the app.

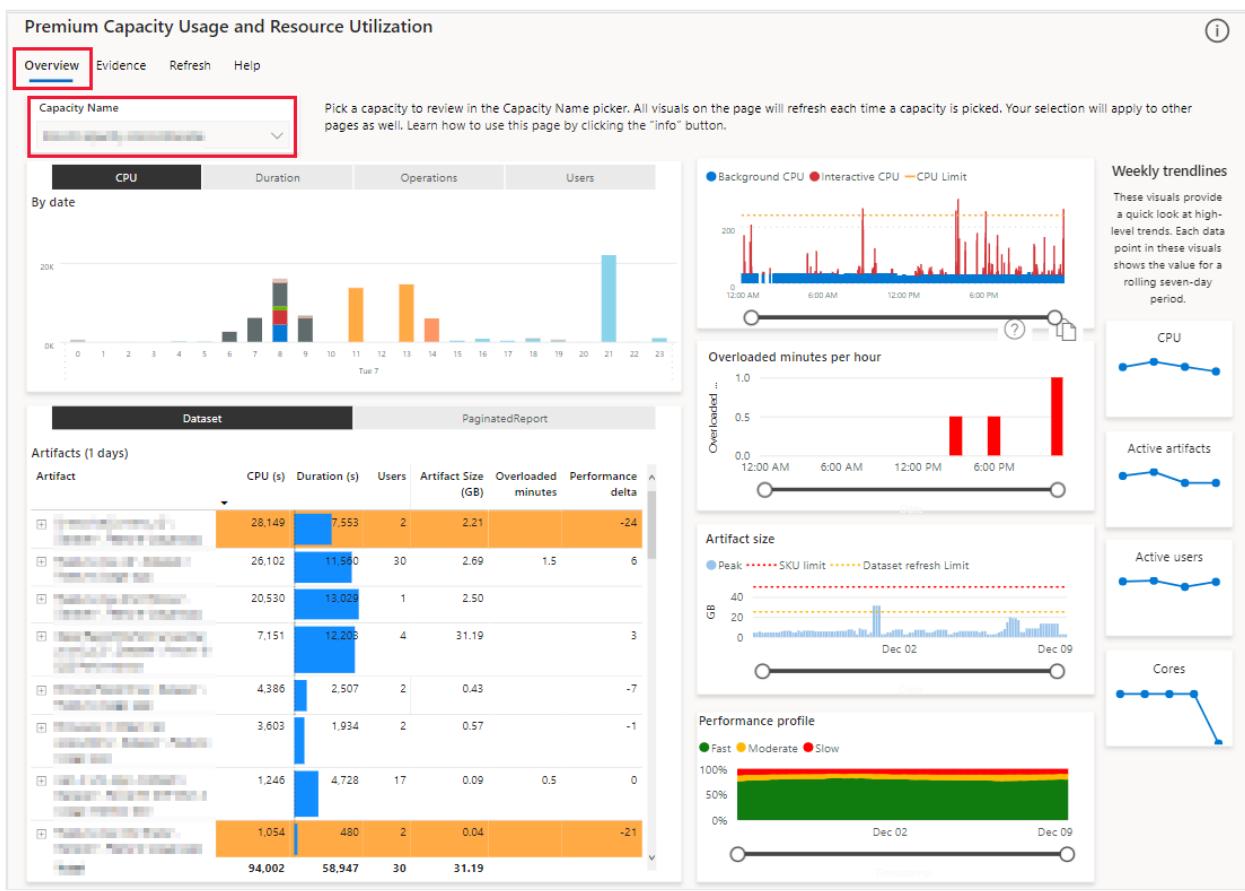
The Gen2 metrics app has six pages:

- [Overview](#)
- [Evidence](#)
- [Refresh](#)
- [Timepoint](#)
- [Artifact Detail](#)

Overview

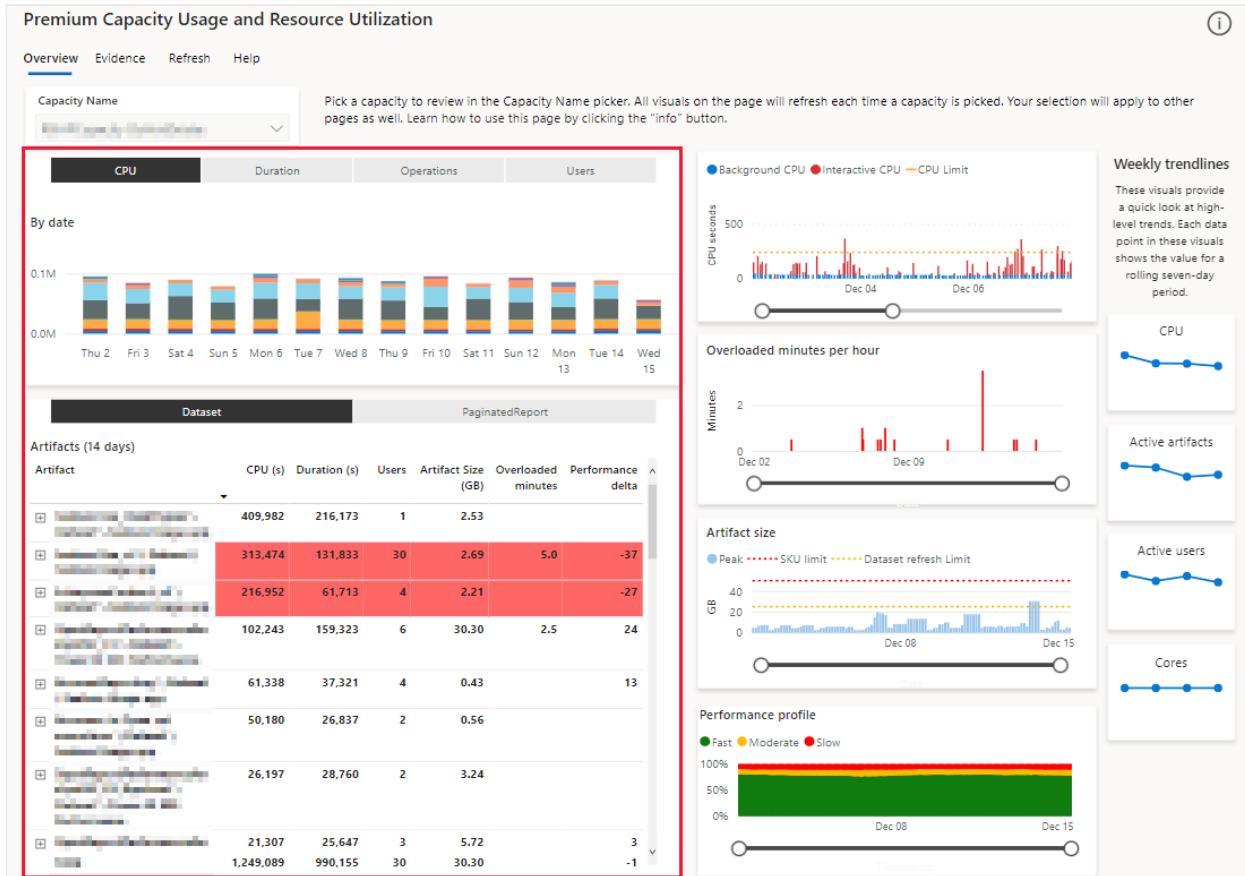
This page provides an overview of the capacity performance. It's divided into the three sections listed below.

At the top of each page, the **CapacityID** field allows you to select the capacity the app shows results for.



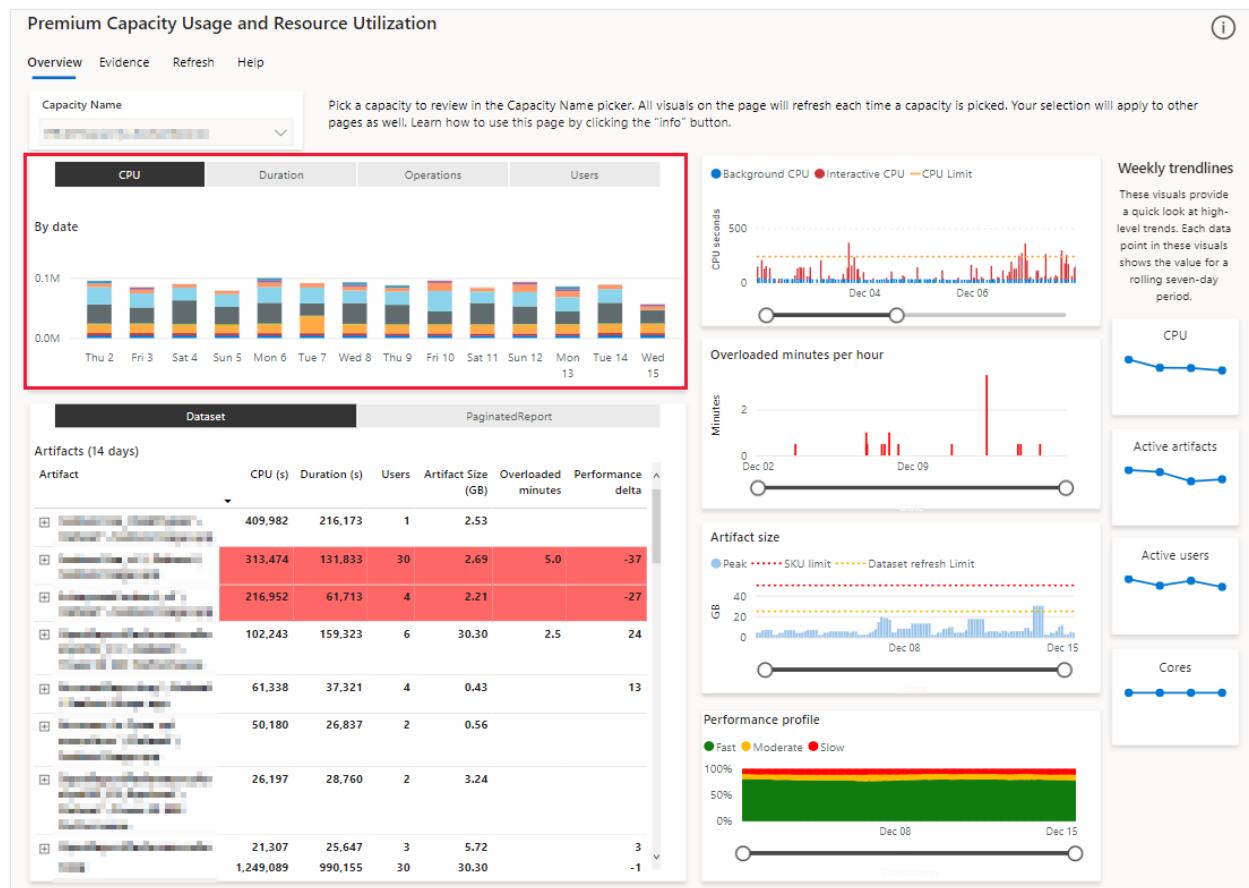
Artifacts

The artifacts section is made up of two visuals, one on top of the other, in the left side of the page. The top visual is a stacked column table, and below it is a matrix table.

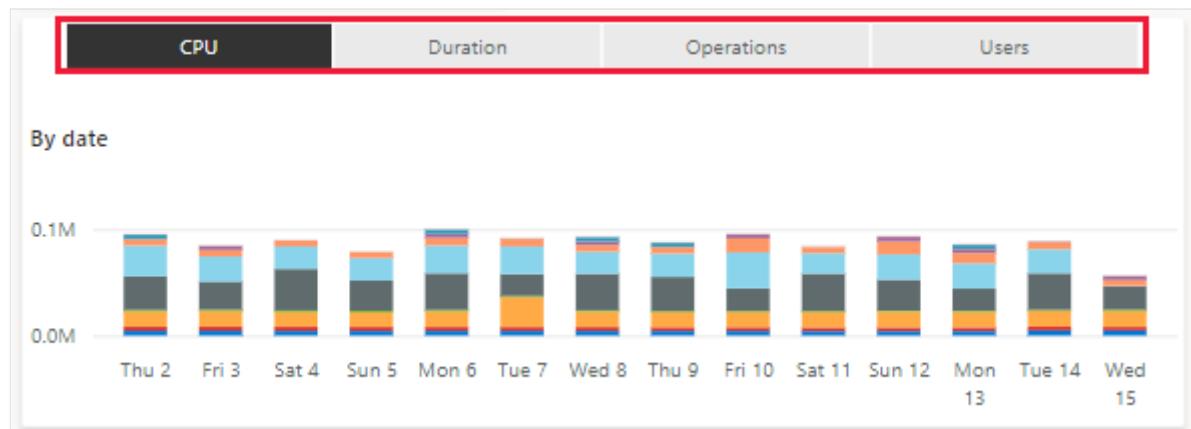


Multi metric column chart

A stacked column table that provides an hourly view of your capacity's usage. Drill down to a specific day to identify daily patterns. Selecting each stacked column will filter the main matrix and the other visuals according to your selection.



The Multi metric column chart displays the four values listed below. It shows the top results for these values per Power BI item during the past two weeks.

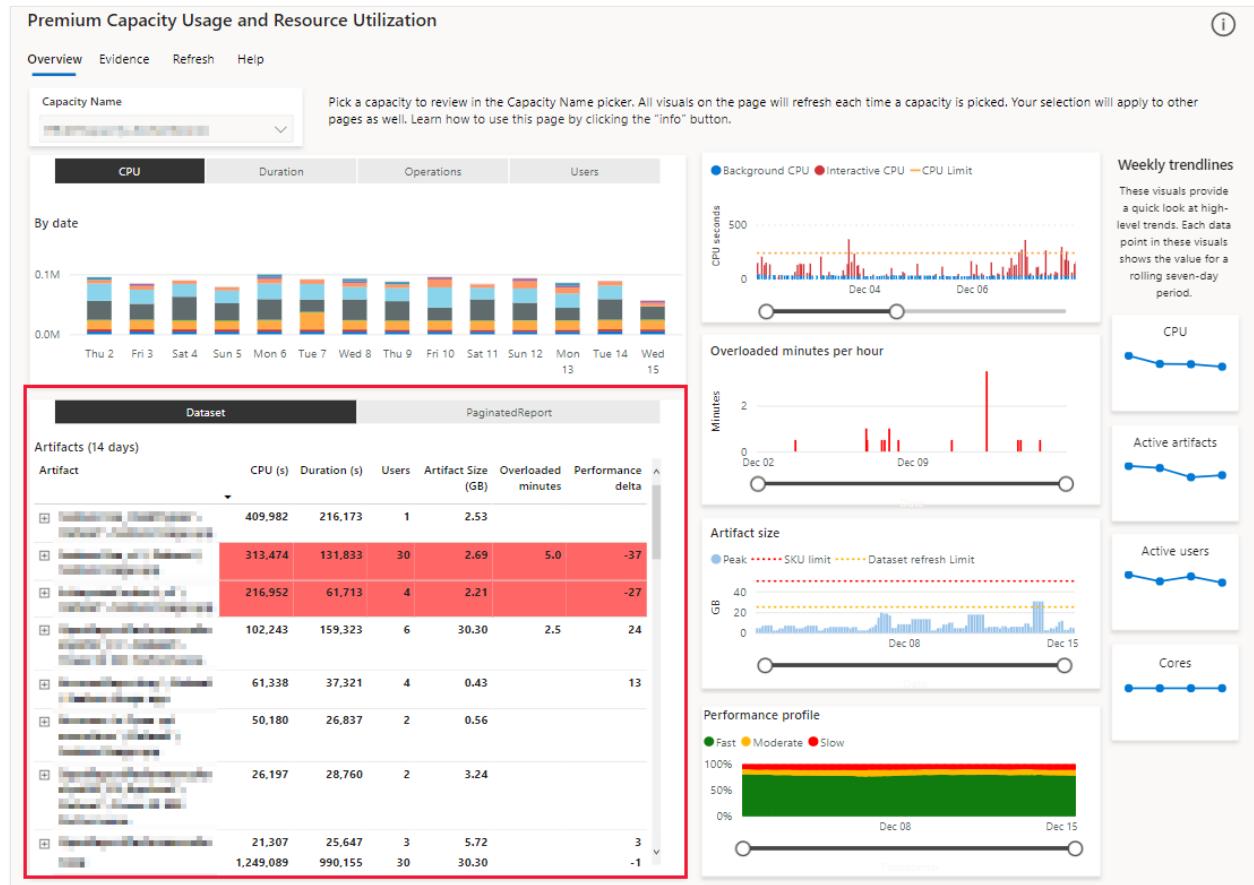


- **CPU** - CPU processing time in seconds.
- **Duration** - Processing time in seconds.
- **Operations** - The number of Power BI operations that took place.

- **Users** - The number of users that performed operations.

Matrix by artifact and operation

A matrix table that displays metrics for each Power BI item on the capacity.



To gain a better understanding of your capacity's performance, you can sort this table according to the parameters listed below. The colors in the table represent your *performance delta*.

The screenshot shows a table titled "Artifacts (14 days)" with the following columns: Artifact, CPU (s), Duration (s), Users, Artifact Size (GB), Overloaded minutes, and Performance delta. The table lists eight items, each with a small thumbnail icon and a detailed view button. The last two rows show expanded details for the first item.

Artifact	CPU (s)	Duration (s)	Users	Artifact Size (GB)	Overloaded minutes	Performance delta
[Thumbnail]	409,982	216,173	1	2.53		
[Thumbnail]	313,474	131,833	30	2.69	5.0	-37
[Thumbnail]	216,952	61,713	4	2.21		-27
[Thumbnail]	102,243	159,323	6	30.30	2.5	24
[Thumbnail]	61,338	37,321	4	0.43		13
[Thumbnail]	50,180	26,837	2	0.56		
[Thumbnail]	26,197	28,760	2	3.24		
[Thumbnail]	21,307	25,647	3	5.72		3
[Thumbnail]	1,249,089	990,155	30	30.30		-1

- **Artifacts** - A list of Power BI items active during the selected period of time. The item name is a string with the syntax: `item name \ item type \ workspace name`. You can expand each entry to show the various operations (such as queries and refreshes) the item performed.
- **CPU (s)** - CPU processing time in seconds. Sort to view the top CPUs that consumed Power BI items over the past two weeks.
- **Duration (s)** - Processing time in seconds. Sort to view the Power BI items that needed the longest processing time during the past two weeks.
- **Users** - The number of users that used the Power BI item.
- **Artifact Size** - The amount of memory a Power BI item needs. Sort to view the Power BI items that have the largest memory footprint.
- **Overloaded minutes** - Displays a sum of 30 seconds increments where overloading occurred at least once. Sort to view the Power BI items that were affected the most due to overload penalty.
- **Performance delta** - Displays the performance effect on Power BI items. The number represents the percent of change from seven days ago. For example, 20 suggests that there's a 20% improvement today, compared with the same metric taken a week ago.

The colors in the matrix represent your *performance delta*:

- *No color* - A value higher than -10
- *Orange* - A value between -10 and -25
- *Red* - A value lower than -25

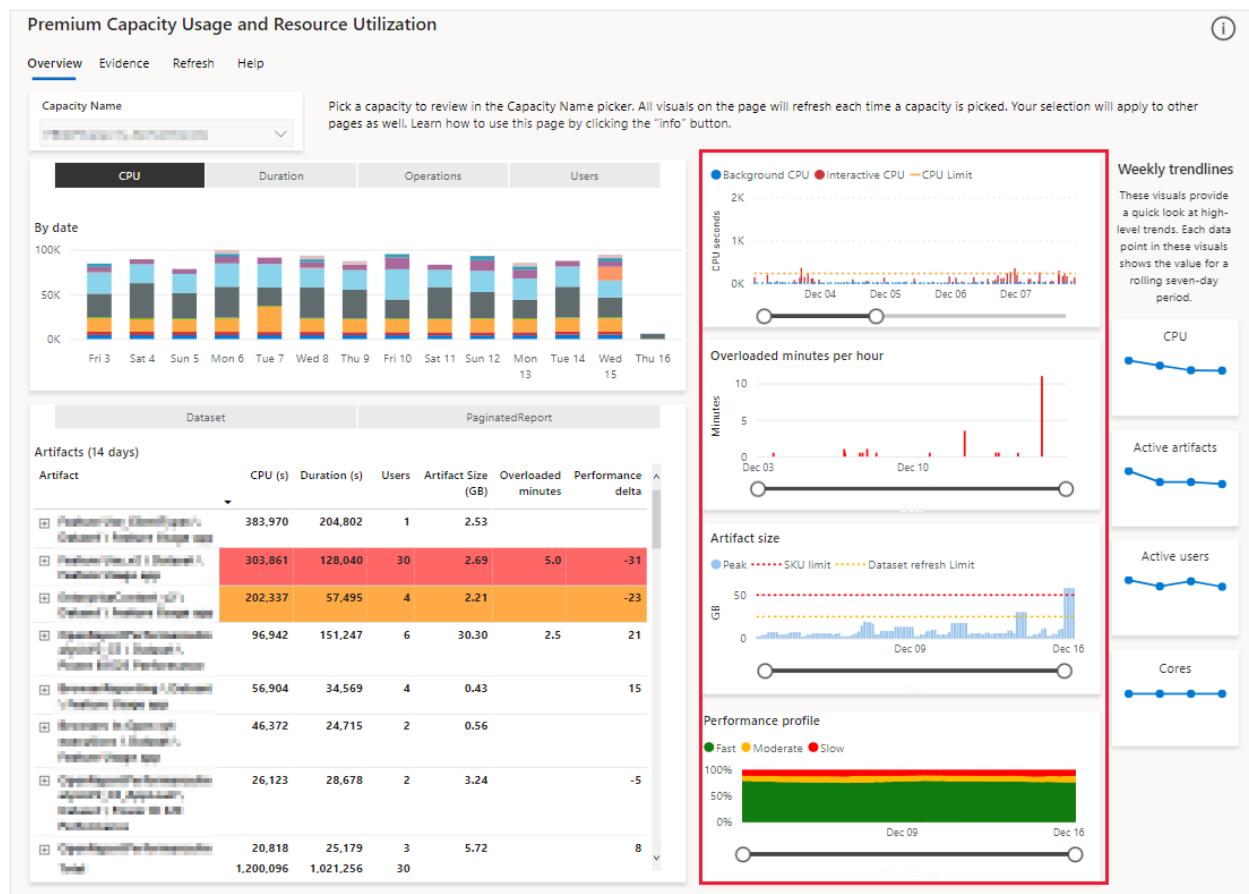
To create the *performance delta* Power BI calculates an hourly average for all the fast operations that take under 200 milliseconds to complete. The hourly value is used as a slow moving average over the last seven days (168 hours). The slow moving average is then compared to the average between the most recent data point, and a data point from seven days ago. The *performance delta* indicates the difference between these two averages.

You can use the *performance delta* value to assess whether the average performance of your Power BI items improved or worsened over the past week. The higher the value is, the better the performance is likely to be. A value close to zero indicates that not much has changed, and a negative value suggests that the average performance of your Power BI items got worse over the past week.

Sorting the matrix by the *performance delta* column helps identify datasets that have had the biggest change in their performance. During your investigation, don't forget to consider the *CPU (s)* and number of *Users*. The *performance delta* value is a good indicator when it comes to Power BI items that have a high CPU utilization because they're heavily used or run many operations. However, small datasets with little CPU activity may not reflect a true picture, as they can easily show large positive or negative values.

Performance

The performance section is made up of four visuals, one on top of the other, in the middle of the page.



CPU over time

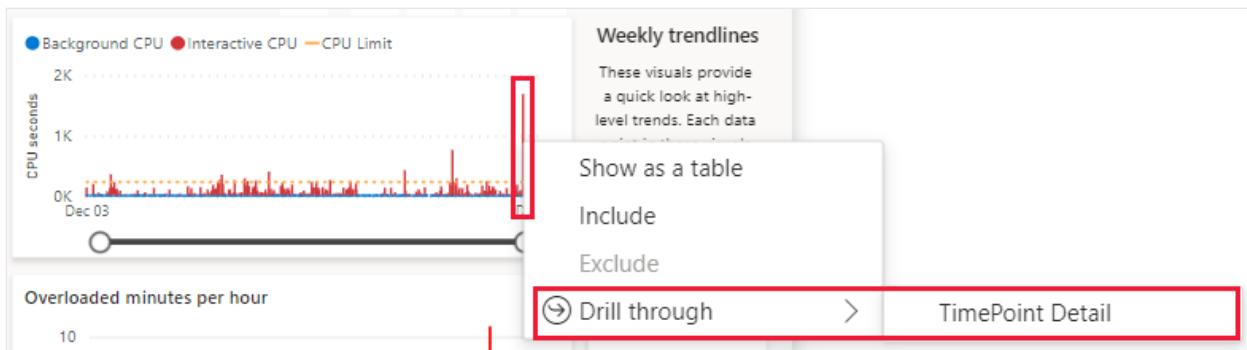
Displays the CPU usage of the selected capacity over time. Filters applied to the page in the [Multi metric column chart](#), affect this chart's display as follows:

- *No filters applied* - Columns display the peak timepoint per hour.
- *Filters are applied* - The visual displays every 30 second timepoint.

Note

Peak is calculated as the highest number of seconds from both *interactive* and *background* operations.

To access the [Timepoint](#) page from this visual, right-click an overloaded timepoint, select **Drill through** and then select **TimePoint Detail**.



The CPU over time chart displays the following elements:

- **Interactive CPU** - Red columns represent the number of CPU seconds used during interactive operations in a 30 second period.

Interactive operations cover a wide range of resources triggered by Power BI users. These operations are associated with interactive page loads.
- **Background** - Blue columns represent the number of CPU seconds used during background operations in a 30 second period.

Background operations cover Power BI backend processes that are not directly triggered by users, such as data refreshes.
- **CPU Limit** - A yellow dotted line that shows the threshold of the allowed number of CPU seconds for the selected capacity. Columns that stretch above this line, represent timepoints where the capacity is overloaded.

Overloaded minutes per hour

Displays a score that represents the severity that overload had on the performance of a Power BI item. If no item is filtered, this chart shows the maximum value seen from all items at each load evaluation interval (30 seconds) in the past two weeks.

Artifact size

Displays the memory footprint recorded for Power BI items over time. If no item is filtered this chart shows the maximum value seen from all items at each ten minute time sample in the past two weeks.

Performance profile

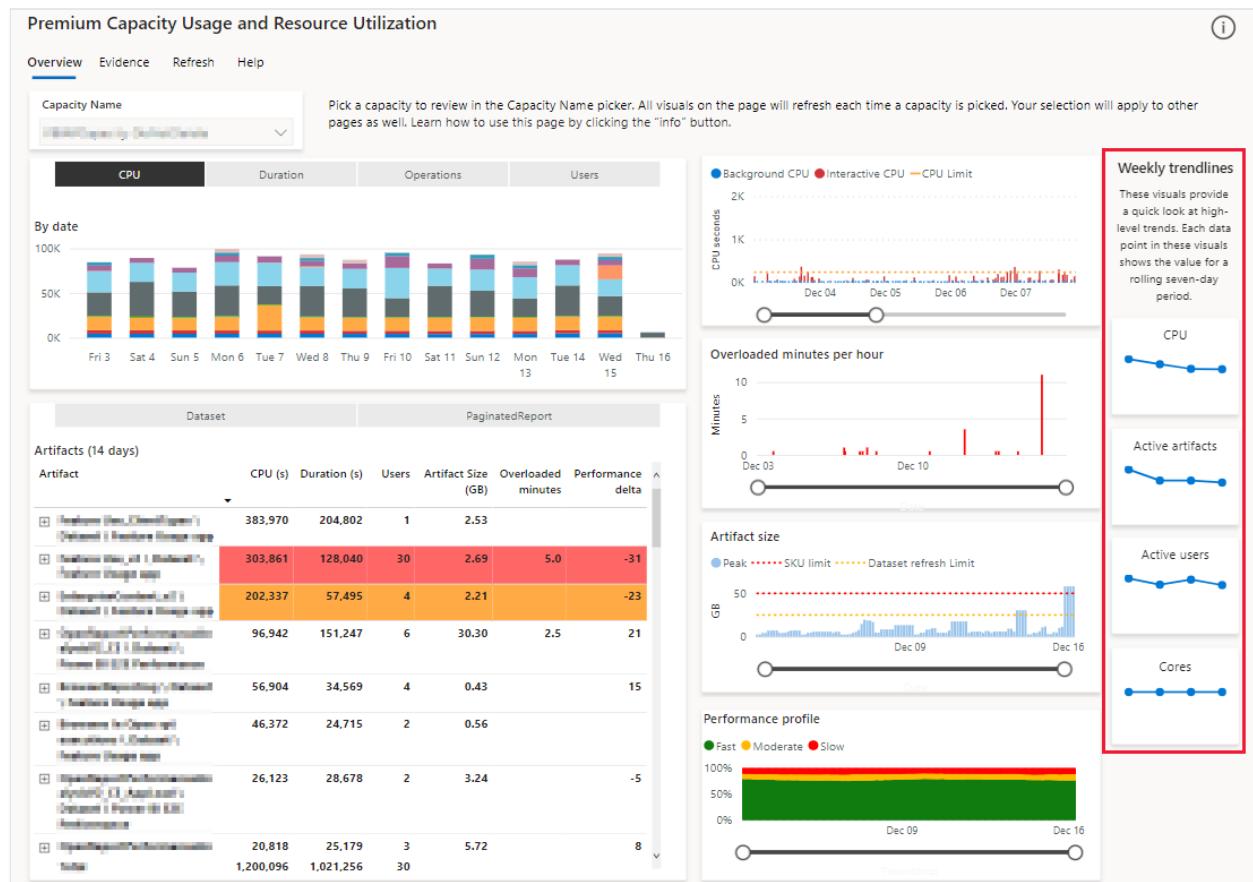
Displays an aggregate of report performance across three operation categories:

- **Fast** - The moving average of fast operations as a percentage of all the operations over time. A fast operation takes less than 100 milliseconds.
- **Moderate** - The moving average of moderate operations as a percentage of all the operations over time. A moderate operation takes between 100 milliseconds to two seconds.
- **Slow** - The moving average of slow operations as a percentage of all the operations over time. A slow operation takes over two seconds.

The aggregate is taken from the total number of operations performed on a Power BI item, over the past two weeks. If no item is filtered, this chart shows the performance profile for datasets on the entire capacity.

Weekly trendlines

The weekly trendlines section is made up of four visuals, one on top of the other, in the right side of the report. These visuals summarize the capacity's behavior over the past four weeks. This section is designed to provide a snapshot of your capacity, highlighting trends for the past four weeks.



CPU

Displays the total CPU power your capacity consumed over the past four weeks. Each data point is the aggregated sum of CPU used for the past seven days.

Active Artifacts

Displays the number of Power BI items (such as reports, dashboards, and datasets) that used CPU during the past four weeks.

Active Users

Displays the number of users that used the capacity during the past four weeks.

Cores

Displays the number of cores used by the capacity in the past four weeks. Each data point is the maximum capacity size reported during that week. If your capacity used autoscaling or scaled up to a bigger size, the visual will show the increase.

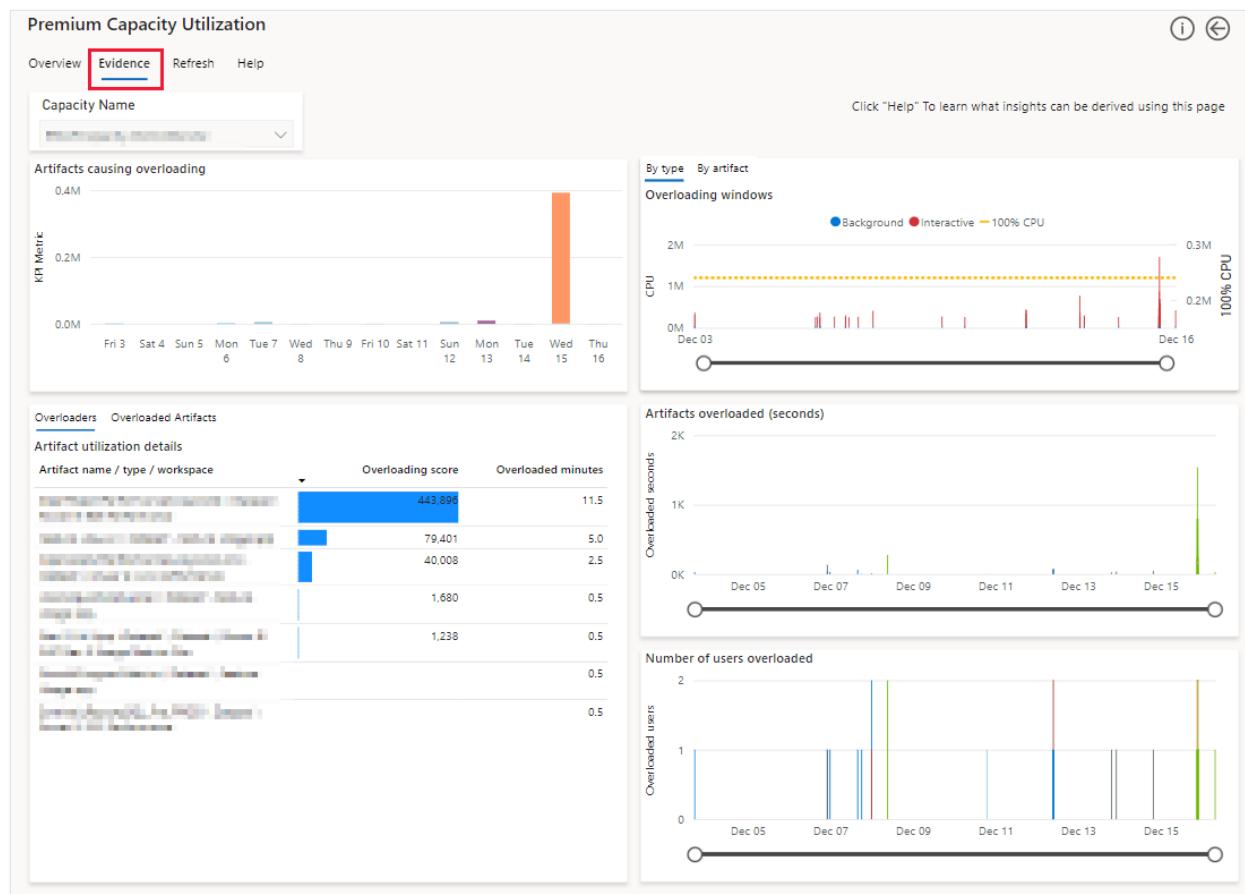
Evidence

This page provides information about overloads in your capacity. You can use it to establish which Power BI items (such as reports, dashboards, and datasets) cause overload, and which items are affected by this overload.

Note

This page only displays data when the capacity is overloaded.

When you detect a Power BI item that causes overload, you can either optimize that item to reduce its impact on the capacity, or you can scale up the capacity.

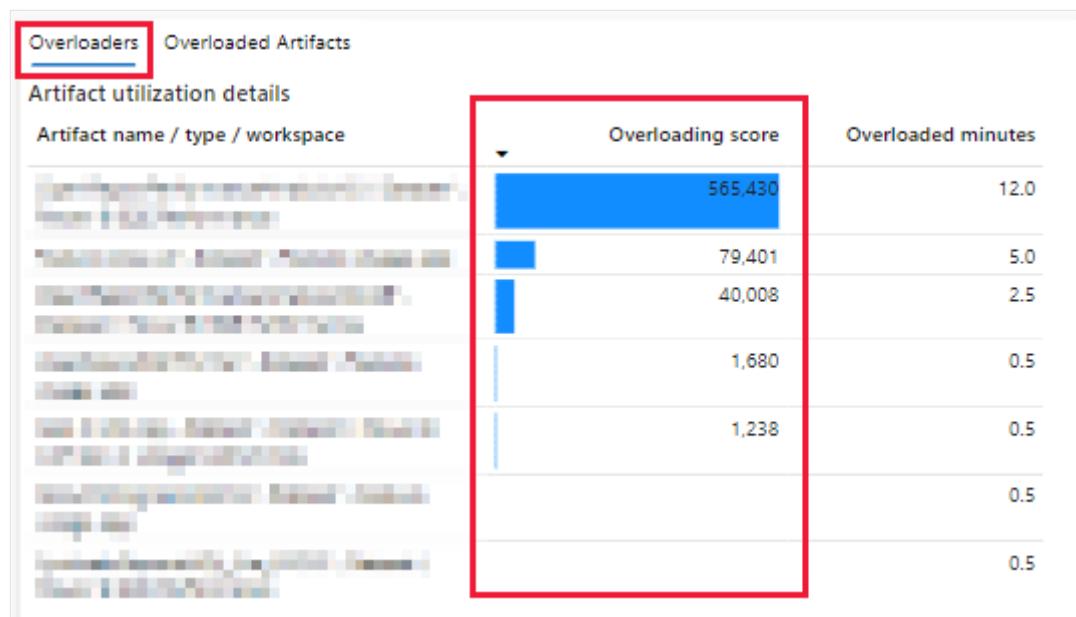


Artifacts causing overloading

You can visually identify the different Power BI items that cause overload, by using the timeline. Each day in the timeline displays items causing overload. Drill down to see an hourly timeline. The value shown is an aggregate of the CPU power consumed by artifacts when they overloaded the capacity.

Overloaders

Use this visual to identify the Power BI items that generate impactful overload events. This is shown as an [Overloading score](#) when you select the *Overloaders* pivot. The overloading score for an artifact is derived from the severity of an overload event, and how frequently the overload event occurred over the past 14 days. This score has no physical property.



Switch to the *Overloaded artifacts* pivot to identify the items most affected by overload over the past 14 days. The overloading impact can affect either the item that's causing the overload, or other items that are hosted in the same capacity.

The *Overloaded time (s)* value is the amount of processing time that was impacted by an overload penalty. This value is shown for each affected item, over the past 14 days.



Overloading windows

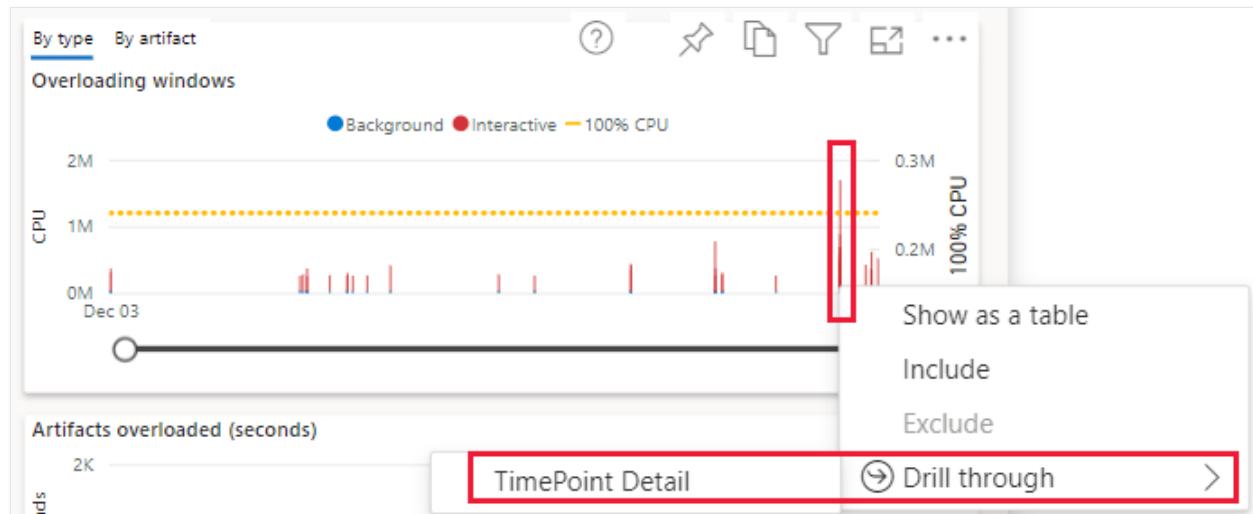
Use this visual to understand whether overload or autoscale events happen due to a single Power BI item, or many items. Each Power BI item is given a different color.

Each column represents a 30 second window where CPU usage for the capacity exceeded allowance. The height of the column represents the amount of CPU used.

The 30 second CPU allowance is determined by the number of v-cores your capacity has. When autoscale is turned on, each added autoscale CPU adds 15 seconds to the

allowance. When autoscale isn't turned on, or if autoscale is fully utilized, penalties are applied to interactive operations in the next 30 second window. You can see a visualization of these penalties in the [Artifacts overloaded \(seconds\)](#) chart.

To access the [Timepoint](#) page from this visual, right-click an overloaded timepoint, select **Drill through** and then select **TimePoint Detail**.



Artifacts overloaded (seconds)

Use this visual to understand whether overloading Power BI items impacts their own performance, or whether they produce a noisy neighbor problem by impacting the performance of other items. Each item is given a different color.

The column height represents the duration of operations subject to overload penalties, which occur when autoscale isn't turned on or used to its maximum.

Number of users overloaded

Use this visual to understand how widespread the impact of overload is. The visual will help you determine whether a single user is impacted by an overload event, or whether the overload event impacts multiple users.

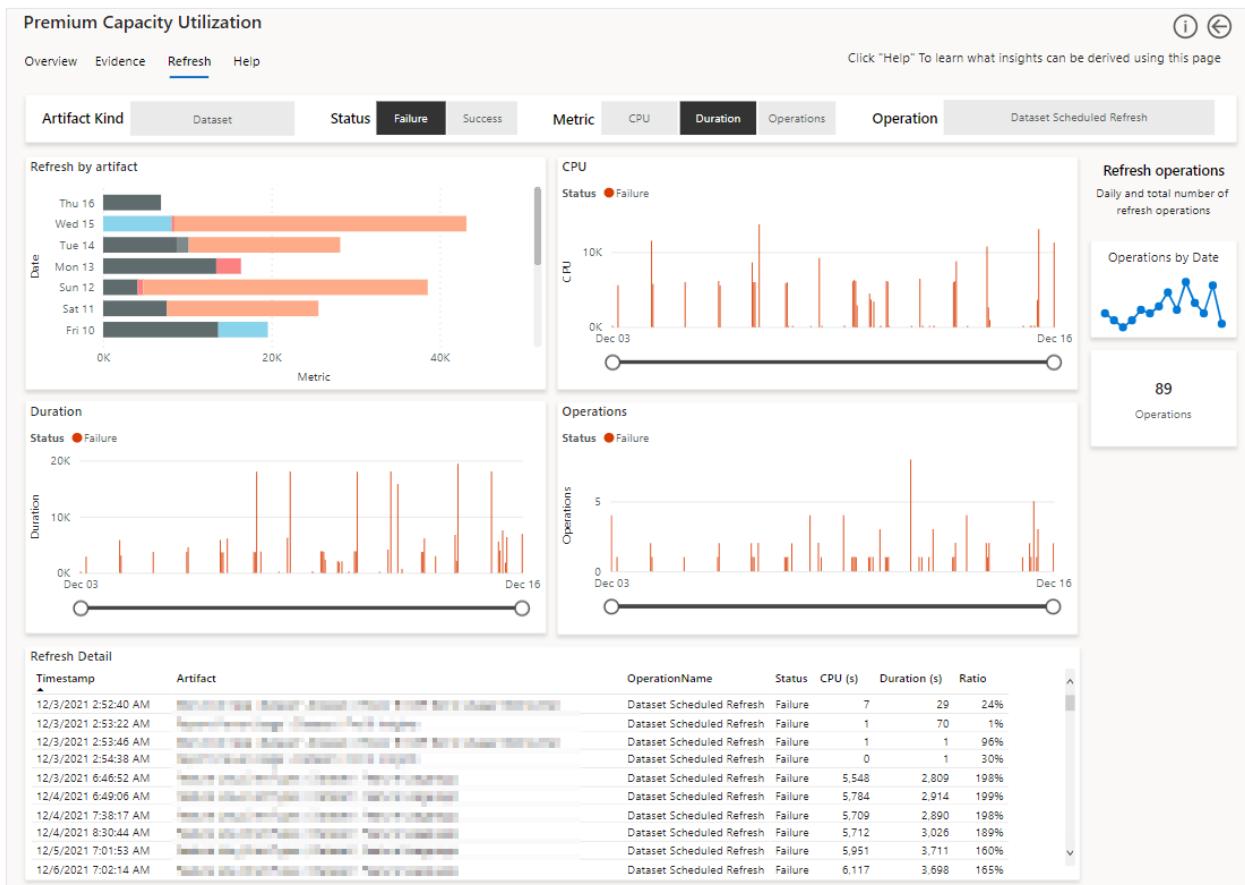
The column height represents the number of distinct users affected when overload occurs.

Refresh

This page is designed to help you identify aspects concerning refresh performance such as refresh CPU consumption power.

(!) Note

You can get to a version of this page, dedicated to a specific Power BI item, using the drill through feature in one of the visuals that displays individual items. The visuals in the drill through version of the page are identical to the ones listed below. However, they only display information for the item you're drilling into.



At the top of the page there's a multi-selection pivot allowing you to focus on refreshing the page according to the filters listed below. Each of these pivots filters all the visuals in the refresh page.



- **Artifact Kind** - Filter the page by Power BI item type, such as report, dataset and dashboard.
- **Status** - Filter the page by failed or successful operations.
- **Metric** - Filter the page by one of the following:
 - **CPU** - CPU consumption
 - **Duration** - Operation processing time

- *Operations* - Number of operations
- **Operation** - Filter according to the type of operation selected.

Refresh by artifact

Displays the breakdown of the metric selected in the pivot at the top, in the past 14 days. These breakdowns can indicate which refresh optimization is more likely to reduce the capacity footprint or the data source load.

- When you select *CPU*, you can identify whether to reduce the capacity footprint.
- When you select *Duration*, you can identify which data source load to reduce.

Duration

Each column represents the number of seconds it took to compete a single operation per hour, over a 14 day period.

CPU

Each column represents the number of CPU seconds used to compete a single operation per hour, over a 14 day period.

Operations

Each column represents the number of seconds it took to compete a single operation per hour, over a 14 day period.

Refresh detail

A matrix table that describes all the metadata for each individual refresh operation that took place. Selecting a cell in the visual will filter the matrix to show specific events.

Scheduled and manual refresh workflows can trigger multiple internal operations in the backend service. For example, refreshes sometimes perform automatic retries if a temporary error occurred. These operations might be recorded in the app using different activity IDs. Each activity ID is represented as a row in the table. When reviewing the table, take into consideration that several rows may indicate an operation of a single activity.

The table has a *Ratio* column describing the ratio between CPU time and processing time. A low ratio suggests data source inefficiencies, where Power BI service is spending more time waiting for the data source, and less time processing the refresh.

Refresh operations

On the right side of the refresh page, there are two visuals designed to help you identify patterns.

- **Timeline** - Displays the number of operations per day, for the past 14 days.
- **Score card** - Displays the total number of performed operations.

Timepoint

All the activities in the capacity are ranked according to their compute impact. The timepoint page shows the top 100,000 impactful activities in the capacity. Use this page to understand which *interactive* and *background* operations contributed the most to CPU usage.

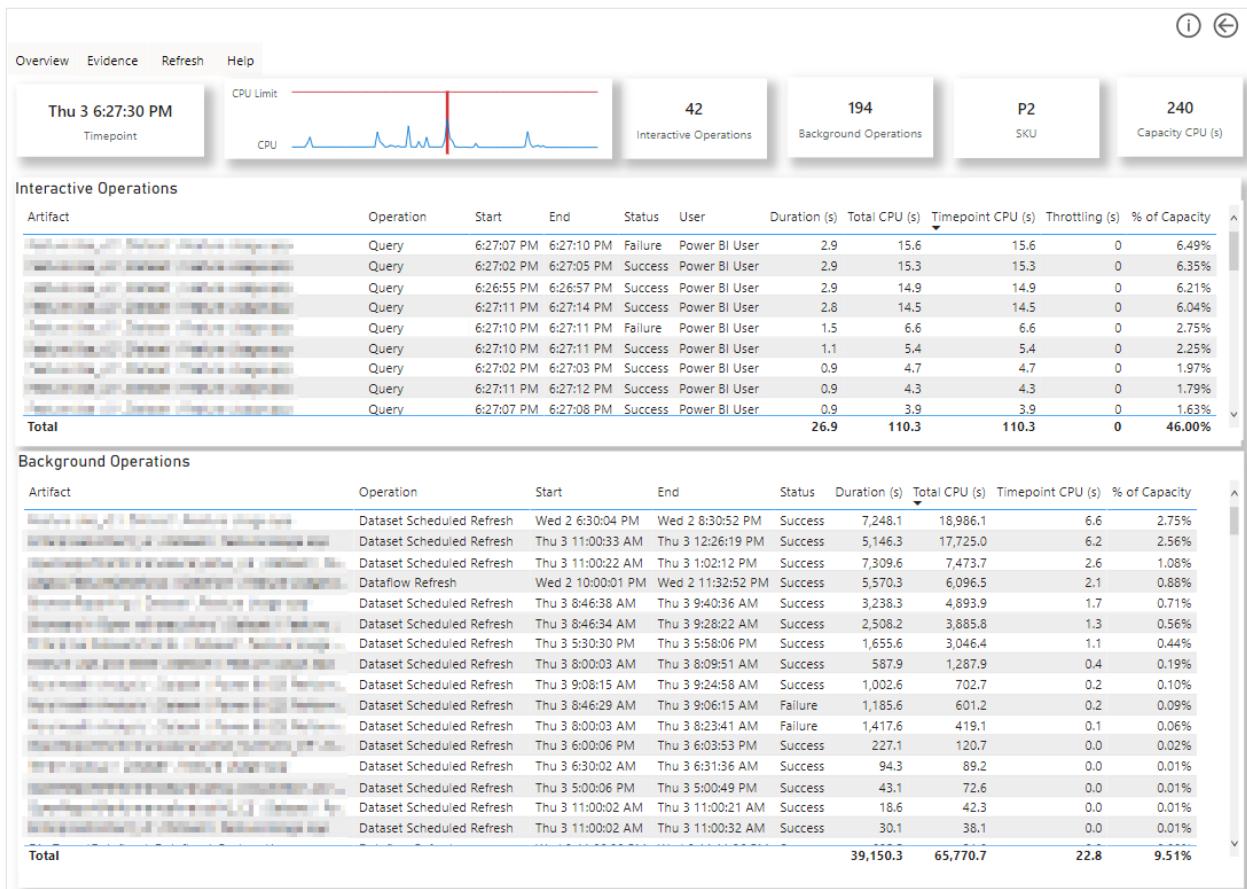
Note

Start and end times may occur before or after the displayed time period, due to **background smoothing** operations.

Important

You can only get to this page by using the drill through feature in an overloaded timepoint in one of these visuals:

- **CPU over time** in the *Overview* page
- **Overloading windows** in the *Evidence* page



When the total combined CPU for *interactive* and *background* operations exceeds the 30 second timepoint allowance, the capacity is overloaded and depending on whether autoscale is enabled or not, throttling is applied.

- **Autoscale is enabled** - If the capacity has autoscale enabled, a new v-core will get added for the next 24 hours and will be shown as an increased value in the *CPU Limit* line in the *CPU over time* chart.

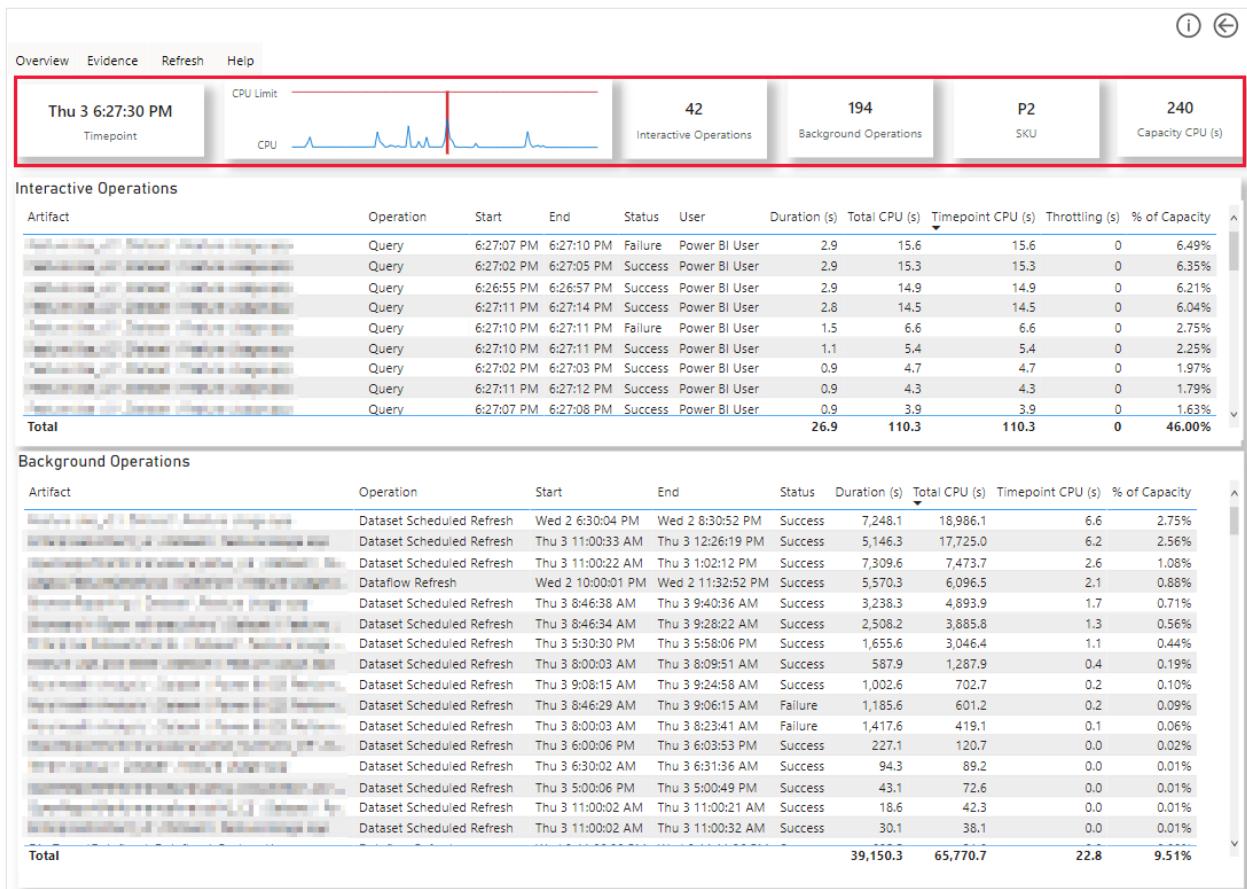
! Note

When autoscale is enabled, if the capacity reaches the maximum number of v-cores allowed by the autoscale operation, throttling is applied.

- **Autoscale isn't enabled** - If autoscale isn't enabled, throttling gets applied to every interactive operation in the subsequent timepoint.

Top row visuals

This section describes the operations of the visuals in the top row of the timepoint page.



- **Top left card** - Displays the timepoint used to drill through to this page.
- **Heartbeat line chart** - Shows a 60 minute window of CPU activity. Use this visual to establish the duration of peaks and troughs.
 - *Vertical red line* - The timepoint you currently drilled to view. The visual shows the 30 minutes of CPU activity leading to the selected timepoint, as well as the 30 minutes of CPU activity after the selected timepoint.
 - *Blue line* - Total CPUs.
 - *Yellow line* - The capacity allowance.

ⓘ Note

If the blue line is above the yellow line the capacity is overloaded.

- **Interactive operations card** - Displays the total number of interactive operations that contributed to the CPU's activity during this timepoint.
- **Background operations card** - Displays the total number of background operations that contributed to the CPU's activity during this timepoint.
- **SKU card** - Displays the current SKU.

- **Capacity CPU card** - Displays the total number of CPU seconds allowed for this capacity, for a given 30 second timepoint window.

Interactive Operations

A table showing every [interactive operation](#) that contributed CPU usage in the timepoint used to drill through to this page. Once an interactive operation completes, all of the CPU seconds used by it get attributed to the timepoint window.

- **Artifact** - The name of the Power BI item, its type, and its workspace details.
- **Operation** - The type of interactive operation.
- **Start** - The time the interactive operation began.
- **End** - The time the interactive operation finished.
- **Status** - An indication showing if the operation succeeded or failed.

ⓘ Note

CPU usage for failed operations is counted when determining if the capacity is in overload.

- **User** - The name of the user that triggered the interactive operation.
- **Duration** - The number of seconds the interactive operation took to complete.
- **Total CPU** - The number of CPU seconds used by the interactive operation. This metric contributes to determine if the capacity exceeds the total number of CPU seconds allowed for the capacity.
- **Timepoint CPU** - The number of CPU seconds assigned to the interactive operation in the current timepoint.
- **Throttling** - The number of seconds of throttling applied to this interactive operation because of the capacity being overloaded in the previous timepoint.
- **% Of Capacity** - Interactive CPU operations as a proportion of the overall capacity allowance.

Background Operations

A table showing every background operation that contributed CPU usage to the timepoint window used to drill through to this page. Every background operation that completed in the prior 24 hours (defined as a 2,880 x 30 second timepoint window), contributes a small portion of its total usage to the CPU value. This means that a background operation that completed the previous day can contribute some CPU activity to determine if the capacity is in overload. For more information see [performance smoothing](#).

All the columns in the background operations table are similar to the ones in the [interactive operations](#) table. However, the background operations table doesn't have a *users* column.

Artifact Detail

This page provides useful information about a specific Power BI item.

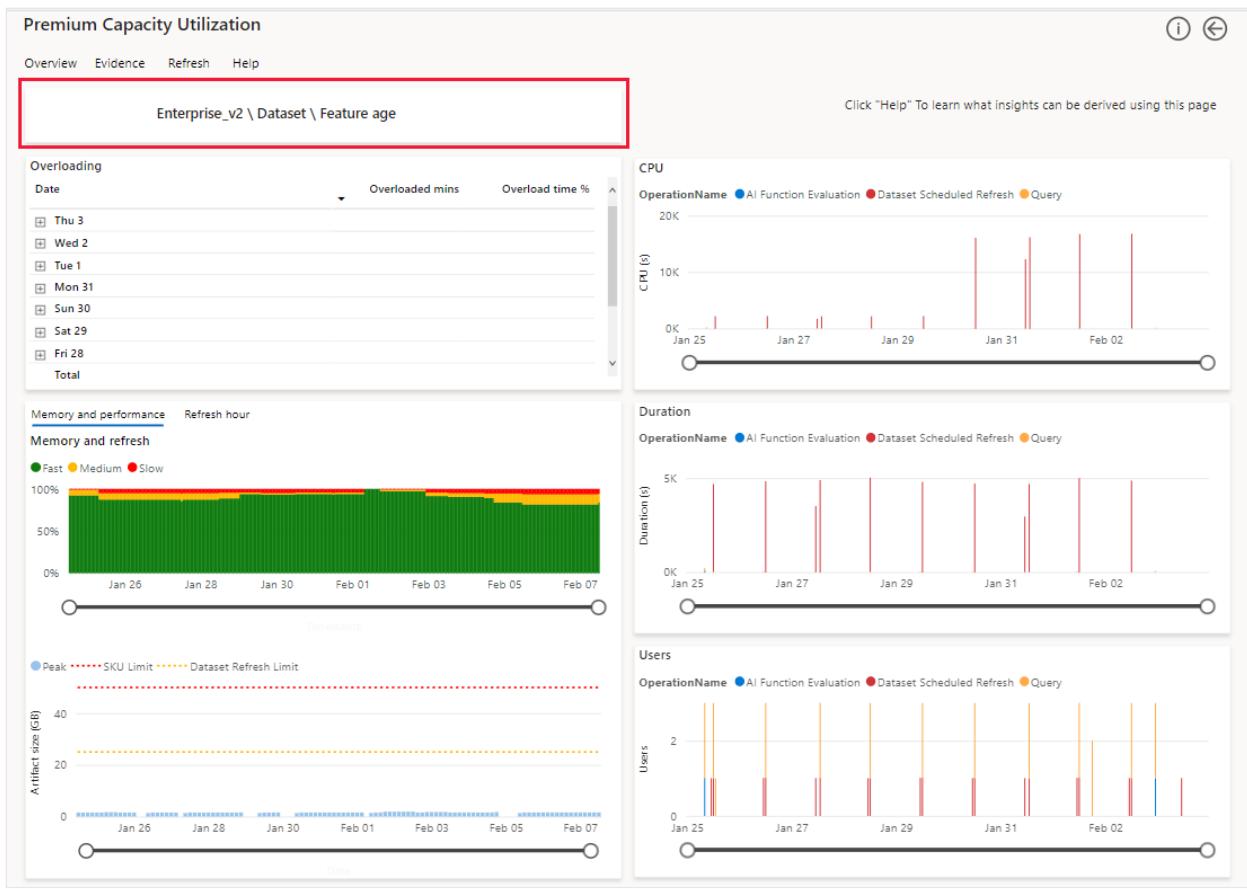
Important

You can only get to this page by using the drill through feature in one of the visuals that displays individual Power BI items.

Note

Some of the visuals in the *Artifact Detail* page may not display information. A visual will not show anything when it's designed to display an event that hasn't occurred.

You can tell which Power BI item you're reviewing, by looking at the card at the top left side of the report, highlighted below. This syntax of this card is `workspace \ Power BI item type \ Power BI item name`.



Overloading

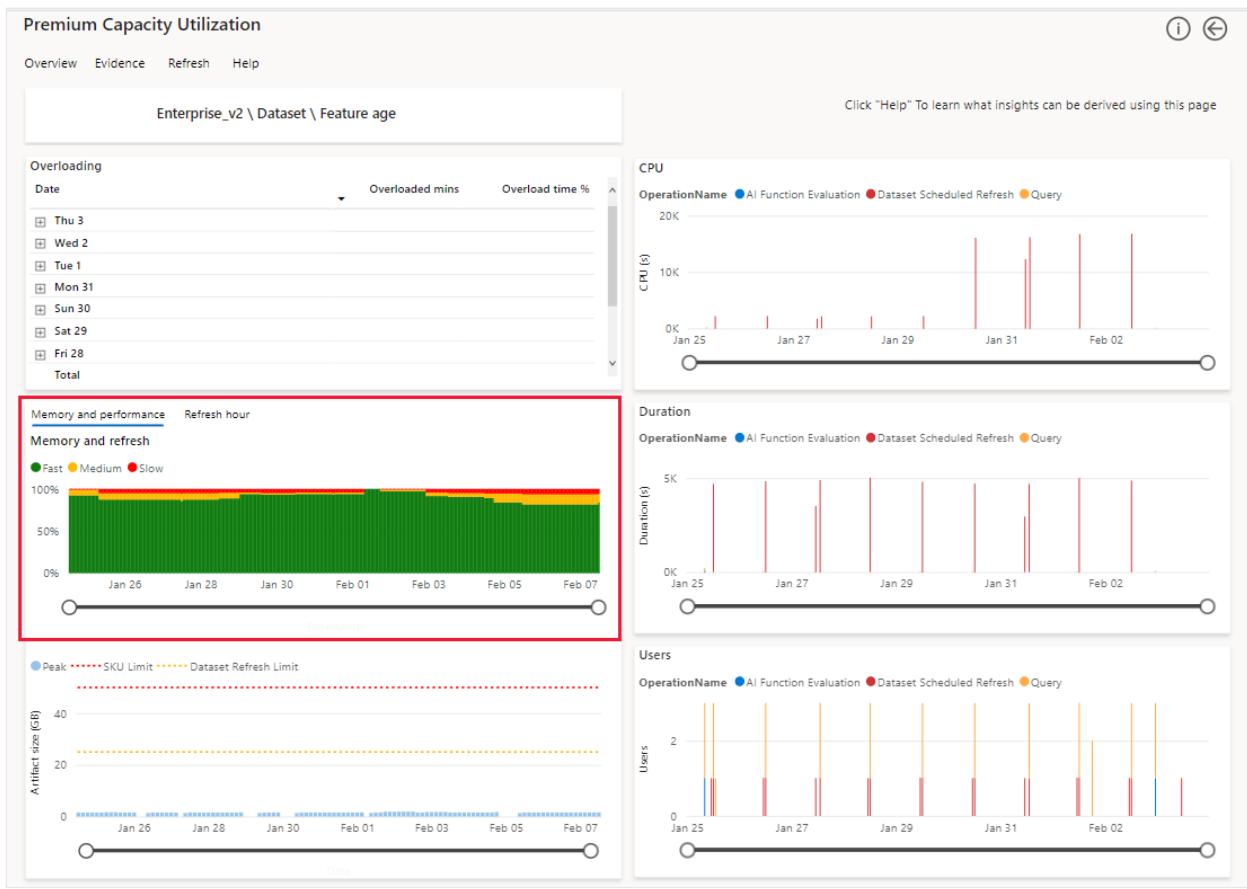
The overloading visual displays time slots where overloading occurred involving the Power BI item you're drilling into.

The overloading visual has the following columns:

- **Date** - The date the item was in overload.
- **Overloaded mins** - Summed 30 second windows where at least one overload event took place.
- **Overload time %** - The proportion of the total operation run time spent in a throttled state. The smaller this value, the better.

Performance

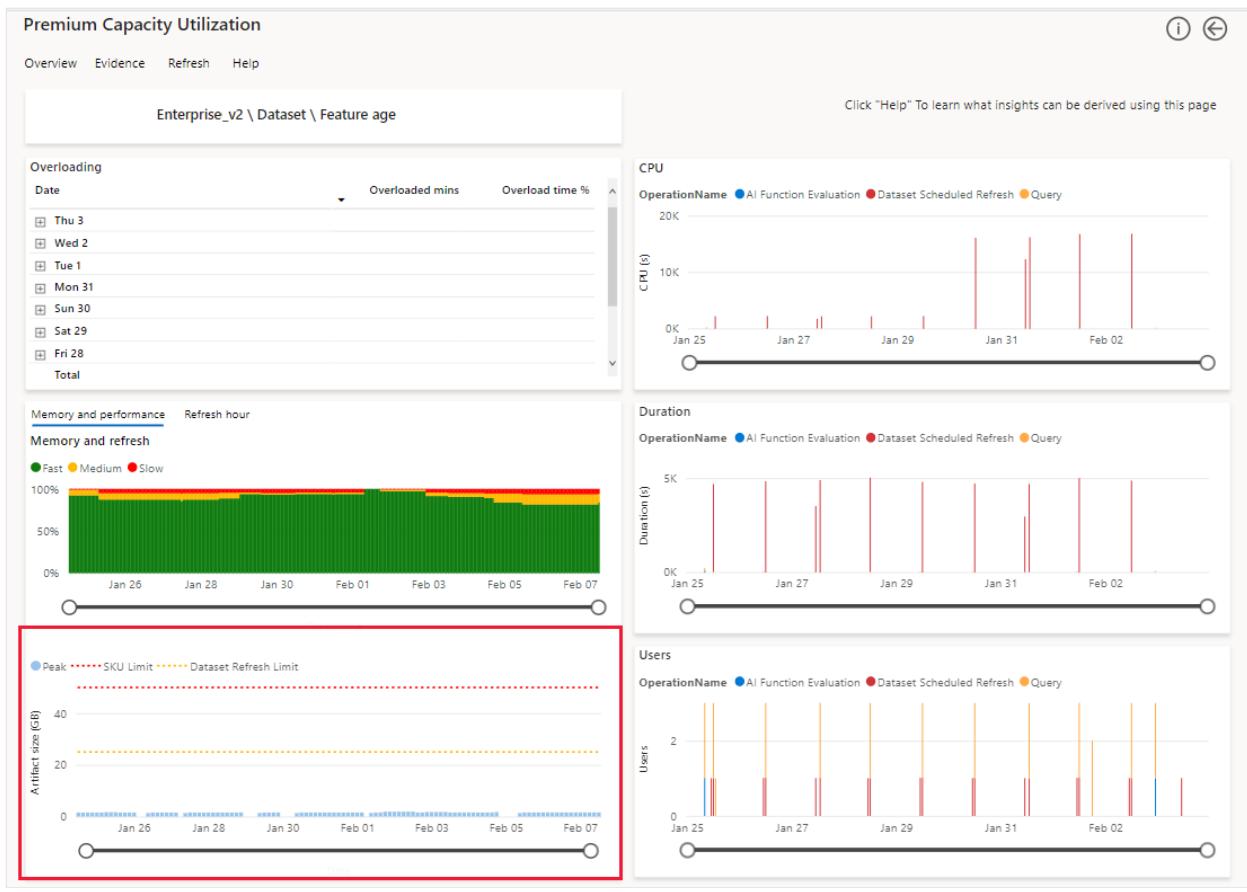
Displays the percentage of fast, moderate, and slow operations from the total number of operations performed by the Power BI item you're drilling into, over the past two weeks.



- **Fast** - The moving average of fast operations as a percentage of all the operations over time. A fast operation takes less than 100 milliseconds.
- **Moderate** - The moving average of moderate operations as a percentage of all the operations over time. A moderate operation takes between 100 milliseconds to two seconds.
- **Slow** - The moving average of slow operations as a percentage of all the operations over time. A slow operation takes over two seconds.

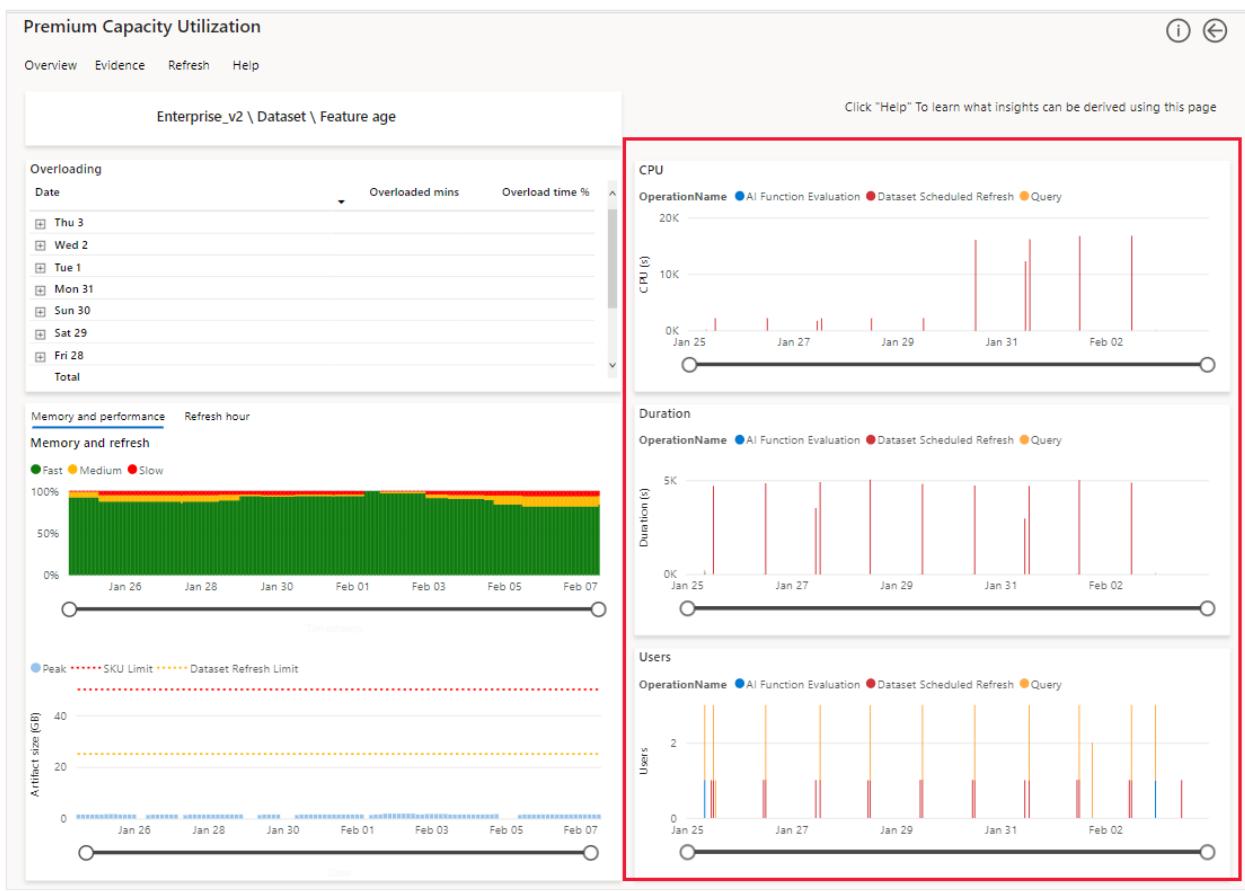
Artifact size

This visual displays the peak amount of memory detected in any three hour window, over a 14 day period, for the item you're drilling into. You can cross filter this visual from the [matrix by artifact](#) and [operation](#) visual, to show a peak memory profile for an individual day.



CPU duration and users

Use these visuals to review CPU consumption, operation duration and number of users for the item you're drilling into. In these visuals, each column represents a single hour over a 14 day period.



- **CPU** - Each column displays the number of CPU seconds used to complete each operation per hour.
- **Duration** - Each column displays the number of seconds used to complete each operation per hour.
- **Users** - Each column displays the number of active users per hour.

Considerations and limitations

- The app displays results for the last 14 or 28 days, depending on the visual.
- The app only displays memory measurements and performance breakdown for datasets.
- The app only supports monitoring datasets that use [import mode](#). To monitor [Power BI service live connections](#) use [Azure Analysis Services](#).
- The *Users* column in the visuals displays the number of distinct users that performed operations against the dataset. These operations may be performed by the users themselves, or by Power BI on behalf of the users. When reviewing the visuals in the app, take into consideration that background operations performed by Power BI, may inflate the count of unique users.

- *Operations triggered by users* - [Interactive operations](#) that include opening a report or clicking a slicer.
 - *Operations triggered by Power BI* - [Background operations](#) that include system operations such as dataset or dataflow refreshes. Sometimes these operations are performed by Power BI on behalf of a user. For example, a refresh operation may execute background queries to cache tile results for users who viewed these tiles recently. The tile refresh cache queries provide a much faster performance for users, when they next view the dashboard.
- [Email subscriptions](#) will be sent with the app's default filter and slicer states.

Next steps

[Install the Gen2 metrics app](#)

Performance smoothing

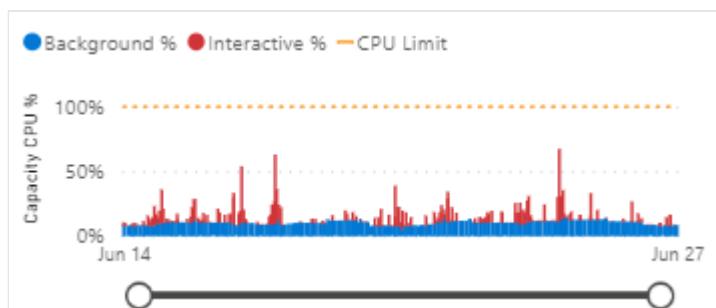
Article • 12/15/2022 • 3 minutes to read

Power BI runs performance smoothing on all Premium Gen2 capacities. Smoothing is used to calculate the impact of your operations on your capacity. Knowing what impact your operations have on your capacity affects many Power BI functions such as billing, [autoscale](#) and the metrics you see in the [Gen2 app](#).

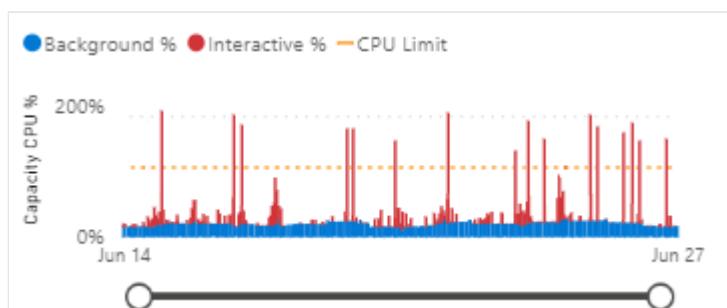
In a Premium Gen2 capacity, CPU usage is the most important measure, because it determines how much of your capacity is in use. By flattening your CPU usage over time, smoothing helps you avoid being penalized due to bursts of intensive CPU usage. When your CPU usage is flatter, you can avoid being throttled when small bursts occur.

The figures below show the way CPU usage is currently reported in the [CPU over time](#) chart, as opposed to the way it used to be reported.

Currently



Prior to May 2022



By smoothing the spikes in your Power BI operations, your capacity becomes easier to manage. Throttling is no longer implemented every time a short lived operation exceeds the capacity's computation power.

How is CPU usage calculated?

To calculate CPU usage, Power BI separates operations into two categories, *interactive* and *background operations*. *Interactive operations* are shorter running operations, usually triggered by user interactions with the UI. *Background operations* are operations that run for a long period of time. Power BI calculates CPU usage for these operations differently, depending on their type.

Interactive operations average your capacity usage over a short time frame, such as five minute intervals. *Background operations* on the other hand, average your capacity usage over a much larger 24 hour time frame. The benefit of this method is that operations that require many resources, such as refreshes, get smoothed because they're averaged over a long period of time.

During each timepoint, Power BI adds up the average CPU usage from both the interactive and background operations. If the CPU usage for a specific timepoint exceeds the SKU limit, [autoscale](#) kicks in if enabled. If autoscale isn't enabled, or if the CPU usage is higher than what autoscale can handle, throttling is applied.

How to detect overload?

You can see if your capacity is overloading, by reviewing the [CPU over time](#) chart in the Gen2 app. A spike that goes over the yellow 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.

How to resolve overload?

When your capacity overloads, you can choose to either turn on [autoscale](#), update your capacity to a higher SKU, or do nothing. The following table gives three examples of the type of action you might want to take, when your capacity is overloading.

Scenario	Solution	Details
A few overload incidents during the night	Do nothing	It's likely that a small number of overloading incidents that don't last for long periods, will have a small impact on the performance of your capacity. If they occur during the night, and you evaluate that during this time the capacity isn't heavily used, you can decide not to take any action. However, when your capacity is experiencing overload, throttling will be applied. You should consider the implications of slower performance during these times when your capacity overloads.

Scenario	Solution	Details
A few overload incidents during the day	Turn on autoscale	When you encounter a fairly low number of overload incidents, it's important to note when they happen. If these incidents happen during peak time, when your capacity is heavily used, throttling will be applied and slow down operations on your capacity. As a result, your capacity will provide a below average experience to the people who use it. In these situations, it's worth turning on autoscale , to avoid throttling.
Many overload incidents	Upgrade to a higher SKU	When your investigation indicates that there are many overload incidents on your capacity, it's worth considering an upgrade to a higher SKU. In such cases, consider the cost of constant autoscale versus the cost of upgrading to a higher SKU.

Next steps

[What is Power BI Premium Gen2?](#)

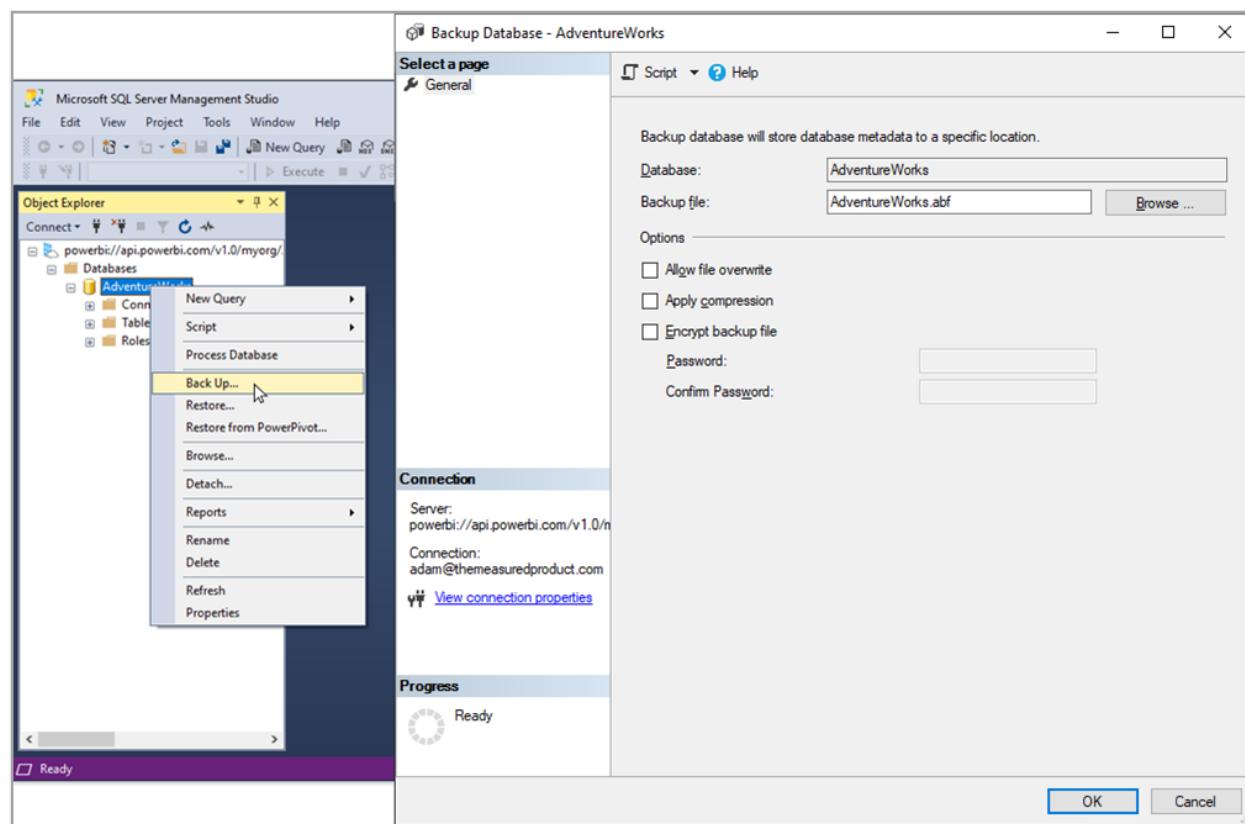
[What is Power BI Premium?](#)

Backup and restore datasets with Power BI Premium

Article • 12/15/2022 • 5 minutes to read

You can use the **Backup and Restore** feature with Power BI datasets 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 datasets, requirements, and considerations.



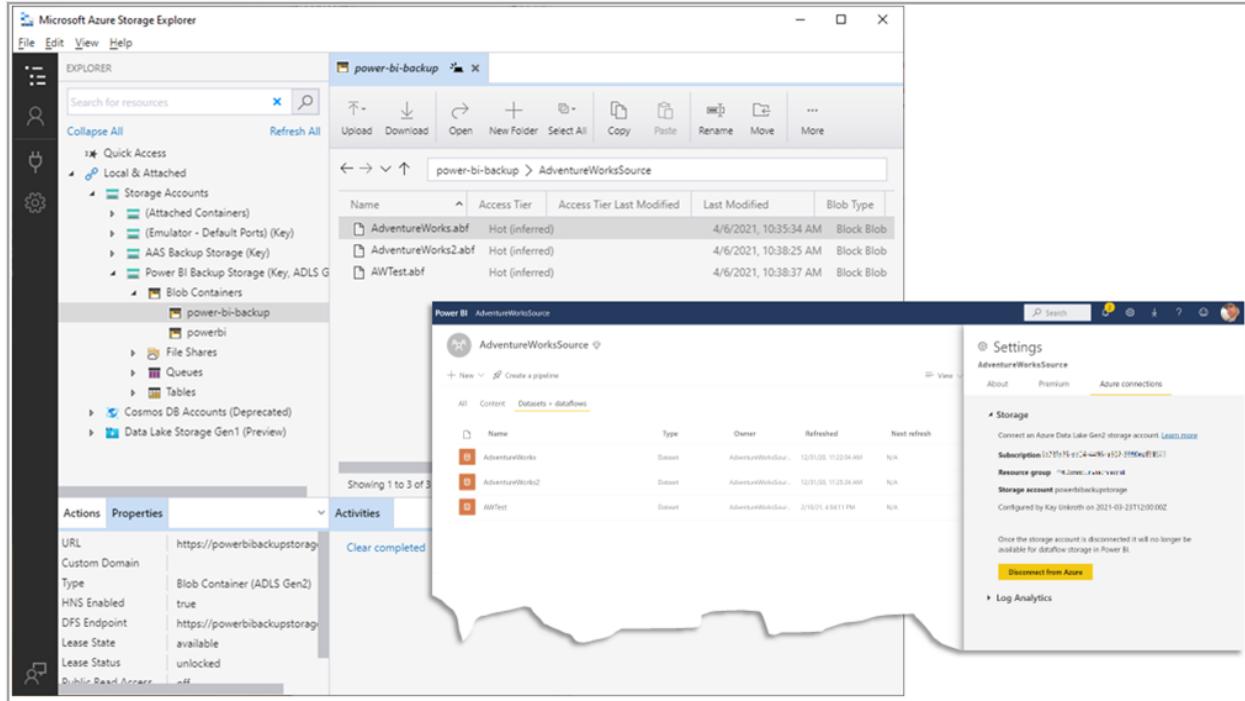
The ability to backup and restore Power BI datasets provides a migration path from Azure Analysis Services workloads to Power BI Premium. It also enables dataset backups for multiple reasons, including corruption or loss, data retention requirements, and tenant movement, among others.

Using dataset 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 datasets 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 dataset.

To *restore* an existing dataset, users who have write or admin permission to the dataset can conduct a *restore* operation. To *restore* a new dataset, the user must be an admin, member, or contributor 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 datasets 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 will fail.

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.
- 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.
- **Password** encryption in the backup command isn't supported
- There's a new property, `ignoreIncompatibilities`, for the `restore` command that 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 dataset backup right now because there is not enough memory to complete this operation. Please use the /forceRestore option to restore the dataset with the existing dataset 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
  }
}
```

Next steps

- [What is Power BI Premium?](#)
- [SQL Server Management Studio \(SSMS\)](#)
- [Analysis Services cmdlets for PowerShell ↗](#)
- [Dataset connectivity with the XMLA endpoint](#)
- [Using Autoscale with Power BI Premium](#)
- [Power BI Premium FAQ](#)
- [Power BI Premium Per User FAQ](#)
- [Add or change Azure subscription administrators](#)

- Configuring tenant and workspace storage

More questions? [Ask the Power BI Community](#).

Using Autoscale with Power BI Premium

Article • 12/19/2022 • 3 minutes to read

Power BI Premium offers scale and performance for Power BI content in your organization. With Power BI Premium Gen2, many improvements are introduced including enhanced performance, greater scale, improved metrics. In addition, Premium Gen2 enables customers to automatically add compute capacity to avoid slowdowns under heavy use, using **Autoscale**.

The screenshot shows the Power BI Admin portal interface. On the left, there's a sidebar with various icons and links. The 'Capacity settings' link is highlighted. The main area is titled 'Power BI Premium > AutoScale test'. It contains two boxes: one for 'Size | P1' showing '8 Base v-cores', and another for 'Auto scale | On' showing '0 Additional v-cores in use Max = 2'. Below these boxes, descriptive text and 'Change size' and 'Manage auto-scale' buttons are visible.

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. Autoscale only works with Power BI Premium Gen2.

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

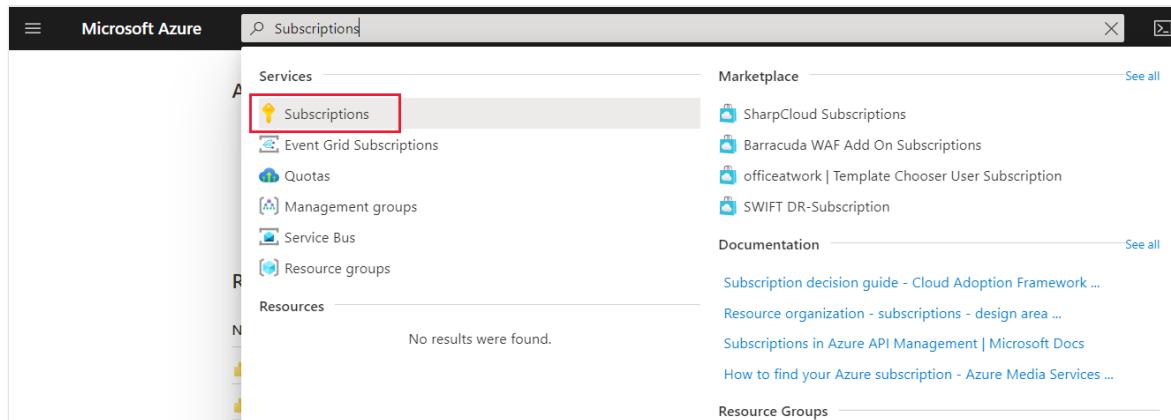
- Autoscale isn't available for Microsoft 365 Government Community Cloud (GCC), due to the use of the commercial Azure cloud.
- **Embedded Gen 2** does not provide an out-of-the-box vertical autoscale feature. To learn about alternative autoscale options for Embedded Gen2, see [Autoscaling in Embedded Gen2](#)

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. Log into 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.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Subscriptions

Test_PBIE

+ Add Manage Policies View Requests

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. Showing subscriptions in Test_PBIE directory. Don't see a subscription? [Switch directories](#)

My role ⓘ

8 selected

Apply

Showing 1 of 1 subscriptions Show only subscriptions selected in the [global subscriptions filter](#) ⓘ

Search for any field...

Subscription name ↑↓	Subscription ID ↑↓
 Test_PBIE	ms-azr-0003

3. From the *Settings* selections for your selected subscription, select **Resource groups**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Subscriptions > Subscriptions

Test_PBIE

+ Add Manage Policies ...

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, [click here](#). Showing subscriptions in Test_PBIE directory. Don't see a subscription? [Switch directories](#)

My role ⓘ Status ⓘ

8 selected 3 selected

Show 1 of 1 subscriptions global
Show only subscriptions selected in the [subscriptions filter](#) ⓘ

Search for any field...

Subscription name ↑↓

Test_PBIE

Test_PBIE Subscription

Cost Management

-  Cost analysis
-  Cost alerts
-  Budgets
-  Advisor recommendations

Billing

-  Invoices
-  External services
-  Payment methods
-  Partner information

Settings

-  Programmatic deployment
-  Resource groups
-  Resources

Cancel subscription

Essentials

- Subscription ID: ms-azr-0003
- Directory: Test_PBIE
- My role: Account admin
- Offer: Pay-As-You-Go
- Offer ID: MS-AZR-0003P
- Parent management group: ...

Latest billed amount

4. Select **Create** to create a resource group to use with Autoscale.

The screenshot shows the Microsoft Azure portal's 'Resource groups' blade. At the top, there is a search bar labeled 'Search (Ctrl+ /)' and several navigation buttons: '+ Create' (highlighted with a red box), 'Edit columns', 'Refresh', and a location dropdown set to 'all'. Below these are filter and search fields: 'Filter for any field...' and 'Location == all'. A message indicates 'Showing 1 to 2 of 2 records.' The main area lists resource groups under three categories: 'Cost Management', 'Billing', and 'Settings'. Under 'Cost Management', there are four items: 'Cost analysis', 'Cost alerts', 'Budgets', and 'Advisor recommendations'. Under 'Billing', there are four items: 'Invoices', 'External services', 'Payment methods', and 'Partner information'. Under 'Settings', there are two items: 'Programmatic deployment' and 'Resource groups'. The 'Resource groups' item is highlighted with a grey background.

5. Name your resource group and select **Review + create**. In the following image, the resource group is called *powerBIPremiumAutoscaleCores*. You can name your resource group whatever you prefer. Just remember the name of the subscription, and the name of your resource group, since you'll need to select it again when you configure Autoscale in the Power BI Admin Portal.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Subscriptions > Test_PBIE >

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more ↗](#)

Project details

Subscription * ⓘ Test_PBIE

Resource group * ⓘ powerBIPremiumAutoscaleCores

Resource details

Region * ⓘ (US) East US

Review + create < Previous Next : Tags >



6. Azure validates the information. After the validation process completes successfully, select **Create**. Once created, you receive a notification in the upper-right corner of the Azure portal.

[Home](#) > [Subscriptions](#) > [Test_PBIE](#) >

Create a resource group

Validation passed.

Basics Tags [Review + create](#)

Basics

Subscription	Test_PBIE
Resource group	powerBIPremiumAutoscaleCores
Region	East US

Tags

None

[Create](#)

< Previous

Next >

[Download a template for automation](#)

Enable Autoscale in the Power BI Admin portal

Once 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 is displayed.

The screenshot shows the Power BI Admin portal interface. The left sidebar has a 'Capacity settings' section highlighted. The main content area displays 'Power BI Premium > AutoScale test' with the following details:

- Premium Generation 2 (preview)**: A note about enabling Premium Generation 2, stating it improves performance and tracks usage. It mentions that once enabled, the capacity stops emitting metrics to the metrics app. A toggle switch is set to **Enabled**.
- Size | P1**: Shows a large number **8** and the text "Base v-cores".
- Auto scale | Off**: Shows a large number **0** and the text "Additional v-cores in use Max = 0".
- A note below the size box states: "The Premium SKU size you purchased is a P1, which gives you access to 8 v-cores."
- Buttons at the bottom: "Change size" and "Manage auto-scale".

2. Autoscale only works with Power BI Premium Gen2. Enabling Gen2 is easy: just move the slider to **Enabled** in the **Premium Generation 2** box.

Premium Generation 2 (preview)

Improve performance and easily track your usage with Premium Generation 2. Enable the preview today. [Learn more](#)

Disabled

Management Health

CAPACITY SIZE

The Premium SKU size you purchased is a P2, which gives you access to 16 v-cores.

REGION

West Central US

USER PERMISSIONS

▶ Capacity admins

▶ Contributor permissions
Enabled for a subset of the organization

MORE OPTIONS

3. Select the **Manage auto-scale** button to enable and configure **Autoscale**, and the **Auto-scale settings** pane appears. Select the **Enable auto scale**.

The screenshot shows the 'Auto-scale settings' page in the Azure portal. At the top, there is a navigation bar with icons for search, notifications, settings, help, and user profile. The main title 'Auto-scale settings' is displayed. Below the title, a descriptive text explains that auto-scale allows users to use as much capacity as needed, adding a temporary v-core for 24 hours and billing it to the Azure subscription of choice. A link to 'Read more about pricing' is provided. A single checkbox labeled 'Enable auto scale' is present. At the bottom right, there are 'Save' and 'Cancel' buttons.

4. You can then 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, select the **Resource group** you created in the previous section, from the list of resource groups available to the subscription.

The screenshot shows the 'Auto-scale settings' page. At the top, there's a search bar and several navigation icons. Below the header, a descriptive text block explains auto-scale functionality, followed by a link to 'Read more about pricing'. A checked checkbox labeled 'Enable auto scale' is present. A dropdown menu titled 'Select an Azure subscription to use for billing' contains the option 'Pay-As-You-Go - [redacted]'. Another dropdown menu titled 'Resource group' contains the option 'powerBIPremiumAutoscaleCores' with a small hand cursor icon over it. A section titled 'Set an auto-scale maximum' includes a note about controlling costs and limiting v-cores. An input field for 'Auto-scale max' shows the value '0 v-cores'. At the bottom right, there are 'Save' and 'Cancel' buttons.

5. Next, assign the maximum number of v-cores to use for Autoscale, and then select **Save** to save your settings. Power BI applies your changes, then closes the pane and returns the view to **Capacity settings**, where you can see your settings have been applied. In the following image, there were a maximum of two v-cores configured for Autoscale.

The screenshot shows the Power BI Admin portal interface. On the left, there's a sidebar with various icons and links. The 'Capacity settings' link is highlighted. The main content area is titled 'Power BI Premium > AutoScale test'. It shows two boxes: one for 'Size | P1' with a large '8' and 'Base v-cores' below it, and another for 'Auto scale | Off' with a large '0' and 'Additional v-cores in use Max = 0' below it. Below these boxes, there's a note about the Premium SKU being P1, which gives access to 8 v-cores. At the bottom, there are 'Change size' and 'Manage auto-scale' buttons.

Here's a short video that shows how quickly you can configure Autoscale for Power BI Premium Gen2:

This screenshot shows the Power BI Admin portal with 'Premium Generation 2 (preview)' enabled. The sidebar and main content area are similar to the first screenshot, but the 'Capacity settings' section now includes a note about improving performance and tracking usage with Premium Generation 2. The 'Enabled' toggle switch is shown as being turned on. The 'Size | P1' and 'Auto scale | Off' boxes are identical to the first screenshot, showing 8 base v-cores and 0 additional v-cores respectively. The notes at the bottom remain the same.

Next steps

[What is Power BI Premium?](#)

[Power BI Premium FAQ](#)

Power BI Premium Per User FAQ

Add or change Azure subscription administrators

Configure workloads in a Premium capacity

Article • 12/15/2022 • 15 minutes to read

This article lists the workloads for Power BI Premium, and describes their capacities. Use the *Gen2* and *Gen1* tabs to review the differences between workloads for these Premium offerings.

ⓘ Important

Premium Gen1, also known as the original version of Premium, is being deprecated. If you're still using Premium Gen1, you need to migrate your Power BI content to Premium Gen2. For more information, see [Plan your transition to Power BI Premium Gen2](#).

ⓘ Note

Workloads can be enabled and assigned to a capacity by using the [Capacities REST APIs](#).

Supported workloads

Gen2

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 Gen2 SKUs supports each workload:

- **AI** - All SKUs are supported apart from the *EM1/A1* SKUs
- **Datasets** - 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.

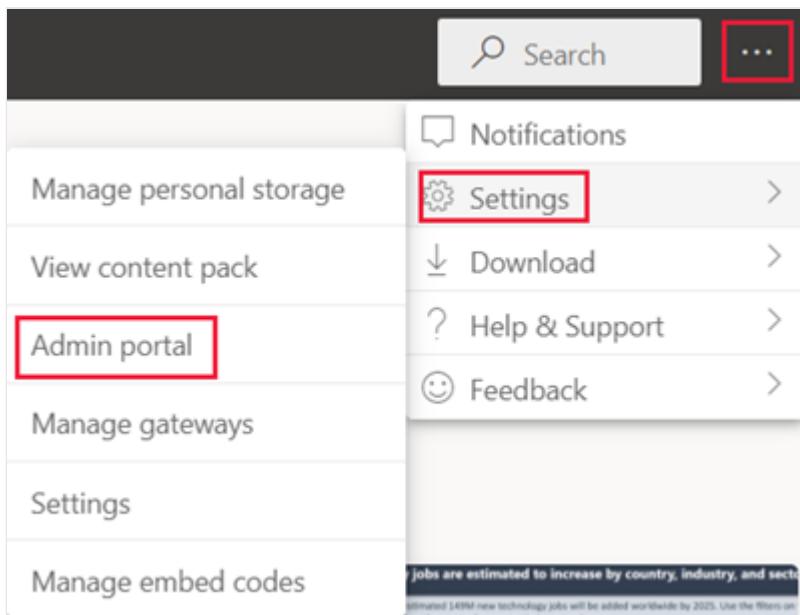
Gen2

ⓘ 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 [Power BI Premium utilization and 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 [capacity and reliability 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.

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 Gen2 doesn't require memory settings to be changed. Memory in Premium Gen2 is automatically managed by the underlying system.

Datasets

This section describes the following datasets 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.

 Note

In Premium Gen1, the datasets workload is enabled by default and cannot be disabled.

Setting Name	Description
Max Memory (%)¹	The maximum percentage of available memory that datasets 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 datasets 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 2147483646. The upper limit may need to be further constrained based on what the datasource supports.
Max Offline Dataset Size (GB)	The maximum size of the offline dataset 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 Set Count	The maximum number of rows returned in a DAX query. The default value is -1 (no limit), 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.

Setting Name	Description
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 Gen2 doesn't require memory settings to be changed. Memory in Premium Gen2 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 dataset 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 dataset, increase this setting to fetch more rows.

This setting affects only DirectQuery queries, whereas [Max Result Row Set Count](#) affects DAX queries.

Max Offline Dataset Size

Use this setting to prevent report creators from publishing a large dataset that could negatively impact the capacity. Power BI can't determine actual in-memory size until the dataset is loaded into memory. It's possible that a dataset with a smaller offline size can have a larger memory footprint than a dataset with a larger offline size.

If you have an existing dataset that is larger than the size you specify for this setting, the dataset will fail to load when a user tries to access it. The dataset can also fail to load if it's larger than the Max Memory configured for the datasets workload.

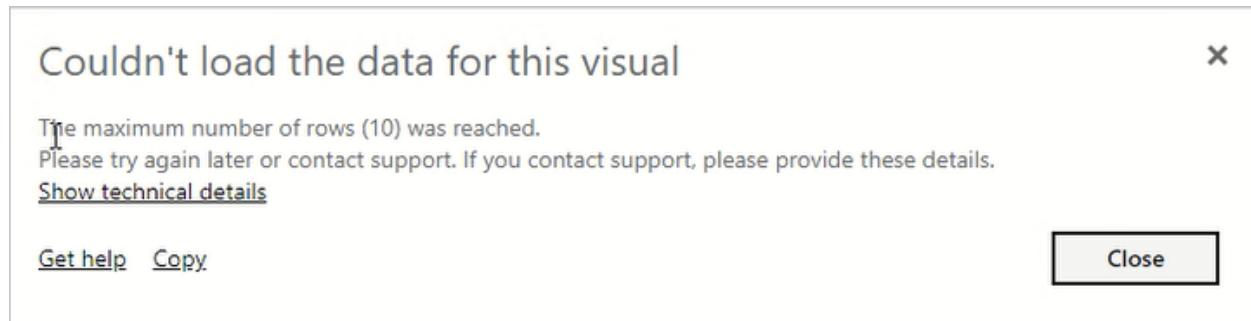
This setting is applicable for models in both small dataset storage format (ABF format) and large dataset storage format (PremiumFiles), although the offline size of the same model might differ when stored in one format vs another. For more information, see [Large models in Power BI Premium](#).

To safeguard the performance of the system, an additional SKU-specific hard ceiling for max offline dataset size is applied, regardless of the configured value. The additional SKU-specific hard ceiling in the below table does not apply to Power BI datasets stored in large dataset storage format.

	EM1/A1	EM2/A2	EM3/A3	P1/A4	P2/A5	P3/A6	P4/A7	P5/A8
Hard ceiling for Max Offline Dataset Size	3 GB	5 GB	6 GB	10 GB	10 GB	10 GB	10 GB	10 GB

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 datasets 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 may also execute DAX queries as part of refreshing the dashboard tiles and visual caches after the data in the dataset has been refreshed. Such queries may 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 dataset was successfully updated.

The default setting is 0, which results in the following SKU-specific automatic query memory limit being applied.

	EM1/A1	EM2/A2	EM3/A3	P1/A4	P2/A5	P3/A6	P4/A7	P5/A8
Automatic Query Memory Limit	1 GB	2 GB	2 GB	6 GB	6 GB	10 GB	10 GB	10 GB

To safeguard the performance of the system, a hard ceiling of 10 GB is enforced for all queries executed by Power BI reports, regardless of the query memory limit configured by the user. This hard ceiling doesn't apply to queries issued by tools that use the Analysis Services protocol (also known as XMLA). Users should consider simplifying the query or its calculations if the query is too memory intensive.

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 may also execute DAX queries as part of refreshing the dashboard tiles and visual caches after the data in the dataset has been refreshed. Such queries may 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 dataset 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 dataset 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 **Datasets** section.

The screenshot shows the Power BI Admin portal interface. The left sidebar includes links for Home, Favorites, Recent, Create, Datasets, Apps, Shared with me, Learn, Workspaces, and My workspace. The main content area is titled "Admin portal" and contains sections for Usage metrics, Users, Premium Per User, Audit logs, Tenant settings, Capacity settings (which is currently selected), Refresh summary, Embed Codes, Organizational visuals, Azure connections (preview), Workspaces, Custom branding, Protection metrics, and Featured content. On the right, there are several toggle switches and input fields under sections like "Allow building machine learning models", "DATASETS", and "Change detection measure". A red box highlights the "Automatic page refresh" section, which includes a toggle switch set to "On" and a dropdown menu showing "1 Seconds". Other settings shown include "Minimum refresh interval" (set to "30 Seconds") and "XMLA Endpoint" (set to "Read Write").

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.

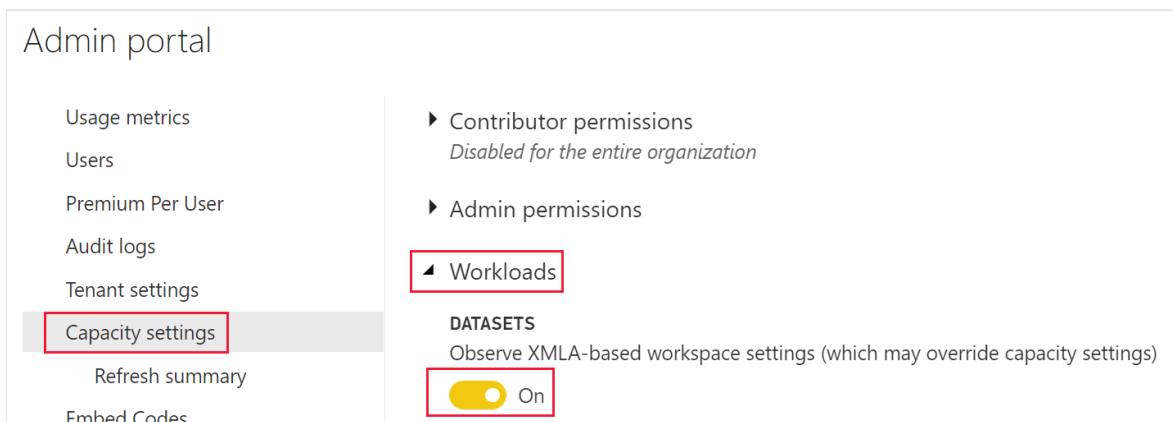
Analysis Services server properties

Power BI Premium Gen2 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 *datasets*, select the setting you want for the **Observe XMLA-based workspace settings (which may 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 Gen1.

Setting Name	Description
Max Memory (%) ¹	The maximum percentage of available memory that dataflows can use in a capacity.

Setting Name	Description
Enhanced Dataflows Compute Engine (Preview)	Enable this option for up to 20x faster calculation of computed entities when working with large scale data volumes. You must restart the capacity to activate the new engine. For more information, see Enhanced dataflows compute engine .
Container Size	The maximum size of the container that dataflows use for each entity in the dataflow. The default value is 700 MB. For more information, see Container size .

¹ Premium Gen2 doesn't require memory settings to be changed. Memory in Premium Gen2 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.

Container size

When refreshing a dataflow, the dataflow workload spawns a container for each entity in the dataflow. Each container can take memory up to the volume specified in the Container Size setting. The default for all SKUs is 700 MB. You might want to change this setting if:

- Dataflows take too long to refresh, or dataflow refresh fails on a timeout.
- Dataflow entities include computation steps, for example, a join.

It's recommended you use the [Power BI Premium Capacity Metrics](#) app to analyze Dataflow workload performance.

In some cases, increasing container size may not improve performance. For example, if the dataflow is getting data only from a source without performing significant calculations, changing container size probably won't help. Increasing container size might help if it will enable the Dataflow workload to allocate more memory for entity refresh operations. By having more memory allocated, it can reduce the time it takes to refresh heavily computed entities.

The Container Size value can't exceed the maximum memory for the Dataflows workload. For example, a P1 capacity has 25 GB of memory. If the Dataflow workload Max Memory (%) is set to 20%, Container Size (MB) can't exceed 5000. In all cases, the Container Size can't exceed the Max Memory, even if you set a higher value.

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.

 Note

You need to enable this workload with Power BI Premium Gen1 capacities.

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 global admin or a Power BI service admin 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**.

Admin portal

- Usage metrics
- Users
- Premium Per User
- Audit logs
- Tenant settings
- Capacity settings**
- Refresh summary
- Embed Codes
- Organizational visuals
- Azure connections
- Workspaces
- Custom branding
- Protection metrics
- Featured content

◀ Workloads
Unapplied changes

DATASETS

Query Memory Limit (%)
0

Query Timeout (seconds)
3600

Max Intermediate Row Count
1000000

Max Result Row Count
2147483647

Max Offline Dataset Size (GB)
0

Automatic page refresh
 On

Minimum refresh interval
5 Minutes ▾

Change detection measure
 On

Minimum execution interval
30 Seconds ▾

XMLA Endpoint
Read Only ▾

AI
Allow usage from Power BI Desktop
 On

PAGINATED REPORTS

Outbound Connectivity Disabled
 On

Apply **Discard**

Gen2

The paginated reports workload is enabled automatically, and is always enabled.

Next steps

[Power BI Premium Generation 2](#)

[Self-service data prep in Power BI with Dataflows](#)

[What are paginated reports in Power BI?](#)

[Automatic page refresh in Power BI Desktop \(preview\)](#)

Large datasets in Power BI Premium

Article • 12/15/2022 • 7 minutes to read

Power BI datasets can store data in a highly compressed in-memory cache for optimized query performance, enabling fast user interactivity. With Premium capacities, large datasets beyond the default limit can be enabled with the **Large dataset storage format** setting. When enabled, dataset size is limited by the Premium *capacity* size or the maximum size set by the administrator.

Large datasets can be enabled for all Premium P SKUs, Embedded A SKUs, and with Premium Per User (PPU). The large dataset size limit in Premium is comparable to Azure Analysis Services, in terms of data model size limitations.

While required for datasets to grow beyond 10 GB, enabling the Large dataset storage format setting has other benefits. If you're planning to use XMLA endpoint-based tools for dataset write operations, be sure to enable the setting, even for datasets that you wouldn't necessarily characterize as a *large* dataset. When enabled, the large dataset storage format can improve XMLA write operations performance.

Large datasets in the service don't affect the Power BI Desktop model upload size, which is still limited to 10 GB. Instead, datasets can grow beyond that limit in the service on refresh.

ⓘ Important

Power BI Premium does support large datasets. Enable the **Large dataset storage format** option to use datasets in Power BI Premium that are larger than the default limit.

Enable large datasets

Steps here describe enabling large datasets for a new model published to the service. For existing datasets, only step 3 is necessary.

1. Create a model in Power BI Desktop. If your dataset will become larger and progressively consume more memory, be sure to configure [Incremental refresh](#).
2. Publish the model as a dataset to the service.
3. In the service > dataset > **Settings**, expand **Large dataset storage format**, set the slider to **On**, and then select **Apply**.

▲ Large dataset storage format

The size of your dataset is 1 MB. For most Premium capacities, using large dataset storage format can improve performance. [Learn more](#)

 On



Discard

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 datasets created in a workspace assigned to a Premium capacity can have the large dataset storage format enabled by default. If the region doesn't support large datasets, the *large dataset 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 dataset storage format**, and then select **Save**.

Premium capacity *(i)*

On

Choose an available Premium capacity for this workspace

Power BI - West Central US

Default storage format

Small dataset storage format

Small dataset storage format

Large dataset storage format

powerbi://api.powerbi.com/v1.0/myorg/Adventure Works

Copy

Delete workspace Save Cancel

Enable with PowerShell

You can also enable large dataset storage format by using PowerShell. You must have capacity admin and workspace admin privileges to run the PowerShell cmdlets.

1. Find the dataset ID (GUID). On the **Datasets** tab for the workspace, under the dataset settings, you can see the ID in the URL.

General Alerts Subscriptions Dashboards **Datasets** Workbooks Reports Dataflows

AdventureWorks AdventureWorksM2M

Settings for AdventureWorks
This dataset has been configured by [Refresh history](#)

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 dataset storage mode.

```
PowerShell
```

```
Login-PowerBIServiceAccount
```

```
(Get-PowerBIDataset -Scope Organization -Id <Dataset 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
--	-----
<Dataset 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 <Dataset ID> -TargetStorageMode PremiumFiles
```

```
(Get-PowerBIDataset -Scope Organization -Id <Dataset ID> -Include  
actualStorage).ActualStorage
```

The response should be the following. The storage mode is now set to Premium Files.

Id	StorageMode
--	-----
<Dataset ID>	PremiumFiles

You can check the status of dataset conversions to and from Premium Files by using the [Get-PowerBIWorkspaceMigrationStatus](#) cmdlet.

Dataset eviction

Dataset eviction is a Premium feature that allows the sum of dataset sizes to be significantly greater than the memory available for the purchased SKU size of the capacity. A single dataset is still constrained to the memory limits of the SKU. Power BI uses dynamic memory management to evict inactive datasets from memory. Datasets are evicted so that Power BI can load other datasets to address user queries. For more info on dynamic memory management, see [Dataset eviction](#).

ⓘ Note

If you have to wait for an evicted dataset to be reloaded, you might experience a noticeable delay.

On-demand load

On-demand load is enabled by default for large datasets, and can provide significantly improved load time of evicted datasets. 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 datasets are quickly made available for queries.

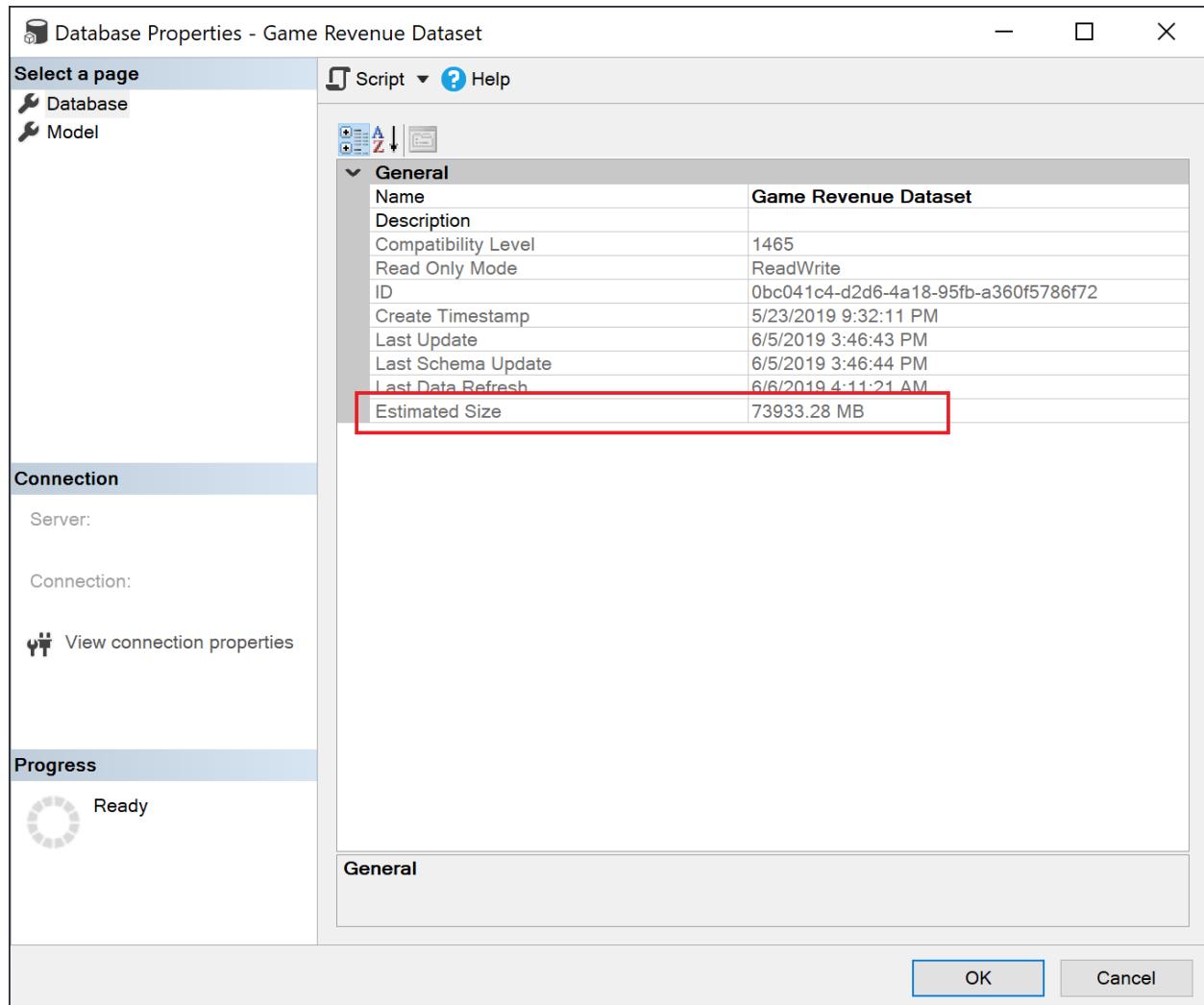
On-demand loading surfaces additional Dynamic Management View (DMV) information that can be used to identify usage patterns and understand the state of your models. For example, you can check the *Temperature* and *Last Accessed* statistics for each column in the dataset, by running the following DMV query from SQL Server Management Studio (SSMS):

SQL

```
Select * from SYSTEMRESTRICTSCHEMA  
($System.DISCOVER_STORAGE_TABLE_COLUMN_SEGMENTS, [DATABASE_NAME] = '<Dataset  
Name>')
```

Checking dataset size

After loading historical data, you can use [SSMS](#) through the [XMLA endpoint](#) to check the estimated dataset size in the model properties window.



You can also check the dataset size by running the following DMV queries from SSMS. Sum the DICTIONARY_SIZE and USED_SIZE columns from the output to see the dataset size in bytes.

```
SQL

SELECT * FROM SYSTEMRESTRICTSCHEMA
($System.DISCOVER_STORAGE_TABLE_COLUMNS,
 [DATABASE_NAME] = '<Dataset Name>') //Sum DICTIONARY_SIZE (bytes)

SELECT * FROM SYSTEMRESTRICTSCHEMA
($System.DISCOVER_STORAGE_TABLE_COLUMN_SEGMENTS,
 [DATABASE_NAME] = '<Dataset Name>') //Sum USED_SIZE (bytes)
```

Default segment size

For datasets using the large dataset 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 datasets:

- **Download to Power BI Desktop:** If a dataset is stored on Premium Files, [downloading as a .pbix file](#) will fail.
- **Supported regions:** Large datasets 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 dataset size:** Maximum dataset size can be set by administrators. For more information, see *Max Memory* in [Datasets](#).
- **Refreshing large datasets:** Datasets that are close to half the size of the capacity size (for example, a 12-GB dataset 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 datasets:** Push datasets don't support the large dataset storage format.
- **Pro isn't supported** - Large datasets aren't supported in Pro workspaces. If a workspace is migrated from Premium to Pro, any datasets with the *large dataset storage format* setting, will fail to load.
- You can't use REST APIs to change the settings of a workspace to allow new datasets to use the large dataset storage format by default.

Region availability

Large datasets in Power BI are only available in Azure regions that support [Azure Premium Files Storage](#).

The following list provides regions where large datasets in Power BI are available. Regions not in the following list aren't supported for large models.

 Note

Once a large dataset is created in a workspace, it must stay in that region. You cannot reassign a workspace with a large dataset 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
South Central US	southcentralus

Azure region	Azure region abbreviation
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 datasets](#)

[Power BI Premium Generation 2](#)

Automate Premium workspace and dataset tasks with service principals

Article • 11/22/2022 • 3 minutes to read

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 dataset management tasks such as provisioning workspaces, deploying models, and dataset 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 Datasets workload must have the [XMLA endpoint enabled for read-write operations](#). Datasets 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**.

Admin portal

Tenant settings

Usage metrics

Users

Premium Per User

Audit logs

Capacity settings

Refresh summary

Embed Codes

Organizational visuals

Azure connections

Workspaces

Custom branding

Protection metrics

Featured content

Developer settings

- ▶ Embed content in apps
Enabled for the entire organization
- ◀ Allow service principals to use Power BI APIs
Unapplied changes

Web apps registered in Azure Active Directory (Azure AD) will use an assigned service principal to access Power BI APIs without a signed in user. To allow an app to use service principal authentication its service principal must be included in an allowed security group. [Learn more](#)

 Enabled

! Service principals can use APIs to access tenant-level features controlled by Power BI service admins and enabled for the entire organization or for security groups they're included in. You can control access of service principals by creating dedicated security groups for them and using these groups in any Power BI tenant level-settings. [Learn more](#)

Apply to:

The entire organization

Specific security groups (Recommended)

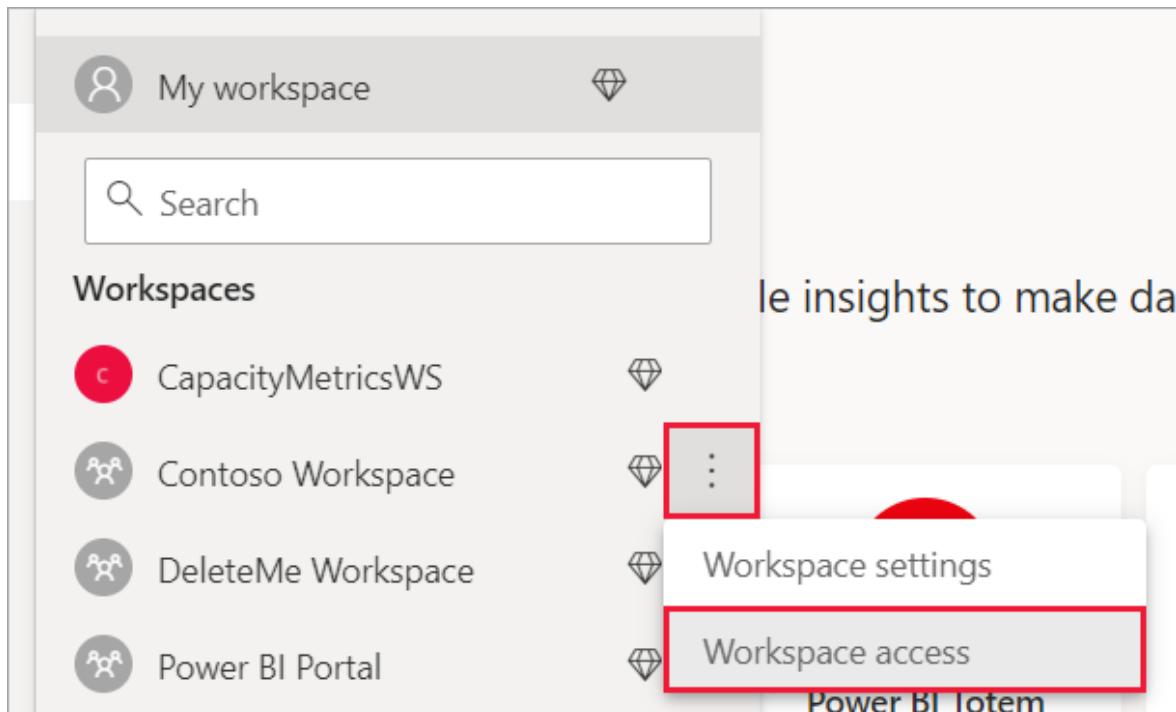
Except specific security groups

Apply Cancel

Workspace access

In order for your service principal to have the necessary permissions to perform Premium workspace and dataset 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.

A screenshot of the 'Customer Profitability' workspace access settings. It shows a dropdown menu where 'Admin' is selected. The 'Admin' option is highlighted with a blue background.

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 dataset 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

[Dataset connectivity with the XMLA endpoint](#)

[Azure Automation](#)

[Azure Logic Apps](#)

[Power BI REST APIs](#)

Dataset connectivity with the XMLA endpoint

Article • 12/07/2022 • 19 minutes to read

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 datasets. 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 **Datasets workload** in a capacity. With read-only, data visualization applications and tools can query dataset model data, metadata, events, and schema.

Read-write operations using the endpoint can be enabled. Read-write provides more dataset management, governance, advanced semantic modeling, debugging, and monitoring. When enabled, datasets have more parity with Azure Analysis Services and SQL Server Analysis Services enterprise grade tabular modeling tools and processes.

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 dataset 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 dataset, backup or restore operation, or trigger a data refresh. The user account or app identity that the client application uses to access a dataset must have a valid Premium Per User (PPU) license unless the dataset resides on a Premium capacity.

Multi-user application - The application provides multiple users with access to a Power BI dataset. For example, a middle-tier application integrating a dataset into a business solution and accessing the dataset 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 datasets. 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 datasets, 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 datasets:

Microsoft Excel – Excel PivotTables are one of the most common tools used to summarize, analyze, explore, and present summary data from Power BI datasets. 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 datasets 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 dataset 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 dataset 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 dataset ([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 dataset management tasks like refresh operations. Requires XMLA read-write. Requires version 21.1.18256 (for Premium Gen2 capacities, see [Premium Gen2 prerequisites](#)) or higher of the [SqlServer PowerShell module](#). Azure Analysis Services cmdlets in the Az.AnalysisServices module aren't supported for Power BI datasets. 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 datasets, 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 datasets. 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 datasets 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](#).

The minimum required client library versions for Premium Gen2 capacities are listed in the [Premium Gen2 prerequisites](#).

Optimize datasets for write operations by enabling large models

When using the XMLA endpoint for dataset management with write operations, it's recommended you enable the dataset for large models. This reduces the overhead of write operations, which can make them considerably faster. For datasets over 1 GB (after compression), the difference can be significant. To learn more, see [Large models in Power BI Premium](#).

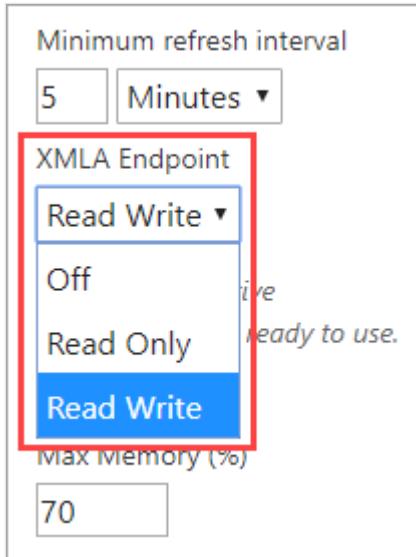
Enable XMLA read-write

By default, Premium capacity or Premium Per User dataset workloads have the XMLA endpoint property setting enabled for read-only. This means applications can only query a dataset. 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 datasets* 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 **Dataset 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.
```

Users with UPNs in the same tenant (not B2B) can replace the tenant name with `myorg`. For example:

```
powerbi://api.powerbi.com/v1.0/myorg/Sales Workspace.
```

B2B users must specify their organization UPN in tenant name. For example:

```
powerbi://api.powerbi.com/v1.0/fabrikam.com/Sales Workspace.
```

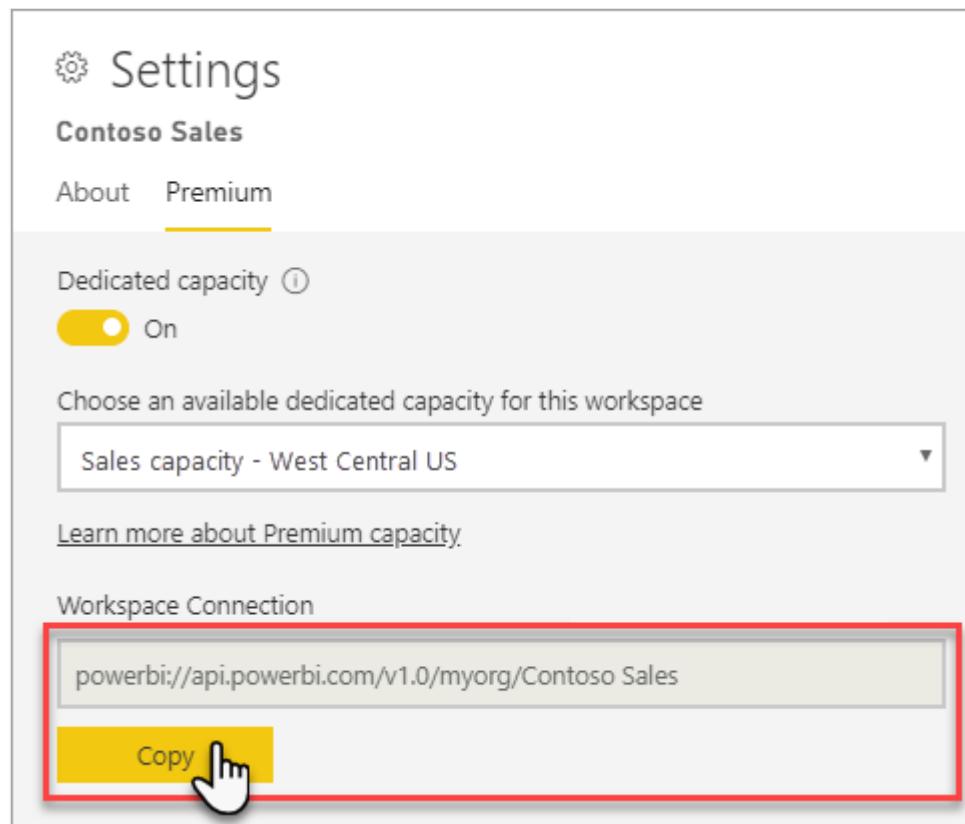
To determine the primary domain name and ID of a Power BI tenant, sign into the Azure portal, select Azure Active Directory from the main menu, and then note the information on the Azure Active Directory Overview page. For more information, see [Find the Microsoft Azure AD tenant ID and primary domain name](#).

ⓘ Note

Connecting to a **My Workspace** by using the XMLA endpoint is currently not supported.

To get the workspace connection URL

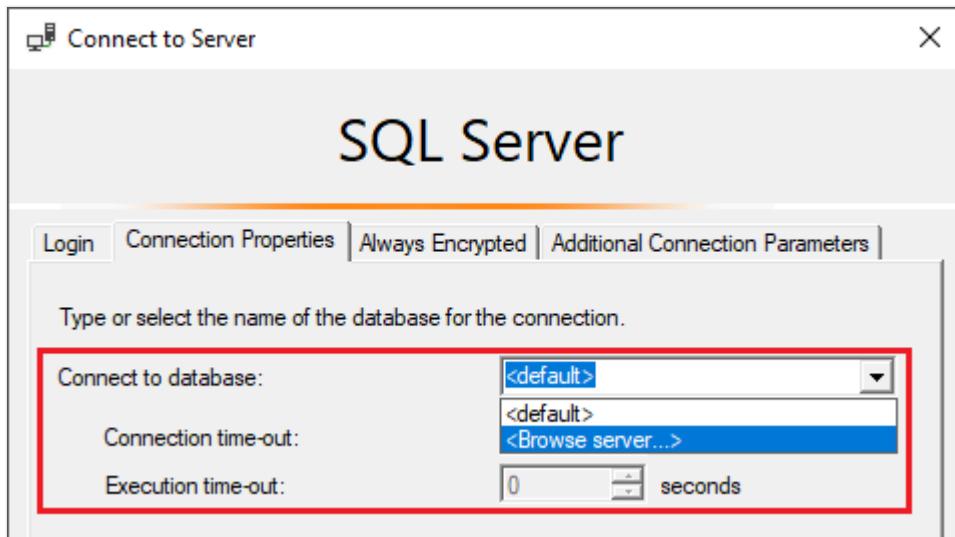
In workspace **Settings > Premium > Workspace Connection**, select **Copy**.



Connection requirements

Initial catalog

With some tools, such as SQL Server Profiler, you must specify an *Initial Catalog*, which is the dataset (database) to connect to in your workspace. In the **Connect to Server** dialog, select **Options > Connection Properties > Connect to database**, enter the dataset 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 dataset name

To connect to a dataset with the same name as another dataset in the same workspace, append the dataset guid to the dataset name. You can get both dataset name and guid when connected to the workspace in SSMS.

Delay in datasets shown

When you connect to a workspace, changes from new, deleted, and renamed datasets can take up to a few minutes to appear.

Unsupported datasets

The following datasets aren't accessible by using the XMLA endpoint. These datasets won't appear under the workspace in SSMS or in other tools:

- Datasets based on a live connection to an Azure Analysis Services or SQL Server Analysis Services model.
- Datasets based on a live connection to a Power BI dataset in another workspace. To learn more, see [Intro to datasets across workspaces](#).
- Datasets with Push data by using the REST API.
- Datasets in My Workspace.
- Excel workbook datasets.

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 datasets** 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 **Allow live connections** should also be enabled. These settings are both enabled by default.

Allow XMLA endpoints and Analyze in Excel with on-premises datasets is an integration setting.

Integration settings

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

Enabled for the entire organization

Users in the organization can use Excel to view and interact with on-premises Power BI datasets. This also allows connections to XMLA endpoints.



Apply to:

The entire organization

Specific security groups

Except specific security groups

Apply

Cancel

The following table describes the implications of the setting **Export data for XMLA and Analyze in Excel (AIXL)**:

Setting	Allow XMLA endpoints and Analyze in Excel with on-premises datasets = disabled	Allow XMLA endpoints and Analyze in Excel with on-premises datasets = enabled
Allow Live Connections toggle = disabled	XMLA <i>disallowed</i> , Analyze in Excel <i>disallowed</i> , AIXL for on-premises datasets <i>disallowed</i>	XMLA <i>allowed</i> , Analyze in Excel <i>disallowed</i> , AIXL for on-premises datasets <i>allowed</i>
Allow Live Connections toggle = enabled	XMLA <i>disallowed</i> , Analyze in Excel <i>allowed</i> , AIXL for on-premises datasets <i>disallowed</i>	XMLA <i>allowed</i> , Analyze in Excel <i>allowed</i> , AIXL for on-premises datasets <i>allowed</i>

Allow live connections is an export and sharing setting.

Export and sharing settings

Allow live connections

Enabled for the entire organization

Users in the organization can use Power BI service Live Connect. This includes Analyze in Excel. [Learn more](#)



Apply to:

The entire organization

Specific security groups

Except specific security groups

[Apply](#)

[Cancel](#)

Access through the XMLA endpoint will honor security group membership set at the workspace/app level.

Workspace contributors and above have Write dataset permissions, which are effectively the same as Analysis Services database admins. They can deploy new datasets from Visual Studio and execute TMSL scripts in SSMS.

Users with Build dataset permissions are equivalent to Analysis Services database readers. They can connect to and browse datasets for data consumption and visualization. Row-level security (RLS) rules are honored and they cannot see internal dataset 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 datasets. The account specified in EffectiveUserName must be in the tenant's Azure Active Directory and must have both **Read** and **Build** permissions for the dataset 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 Azure Active Directory (Azure AD). 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 datasets 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 datasets 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 dataset is required for read access through the XMLA endpoint, regardless of the existence of dataset 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 dataset settings page in the Power BI Service.

Service principals

Service principals are an Azure Active Directory 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 dataset management tasks such as provisioning workspaces, deploying models, and dataset refresh with:

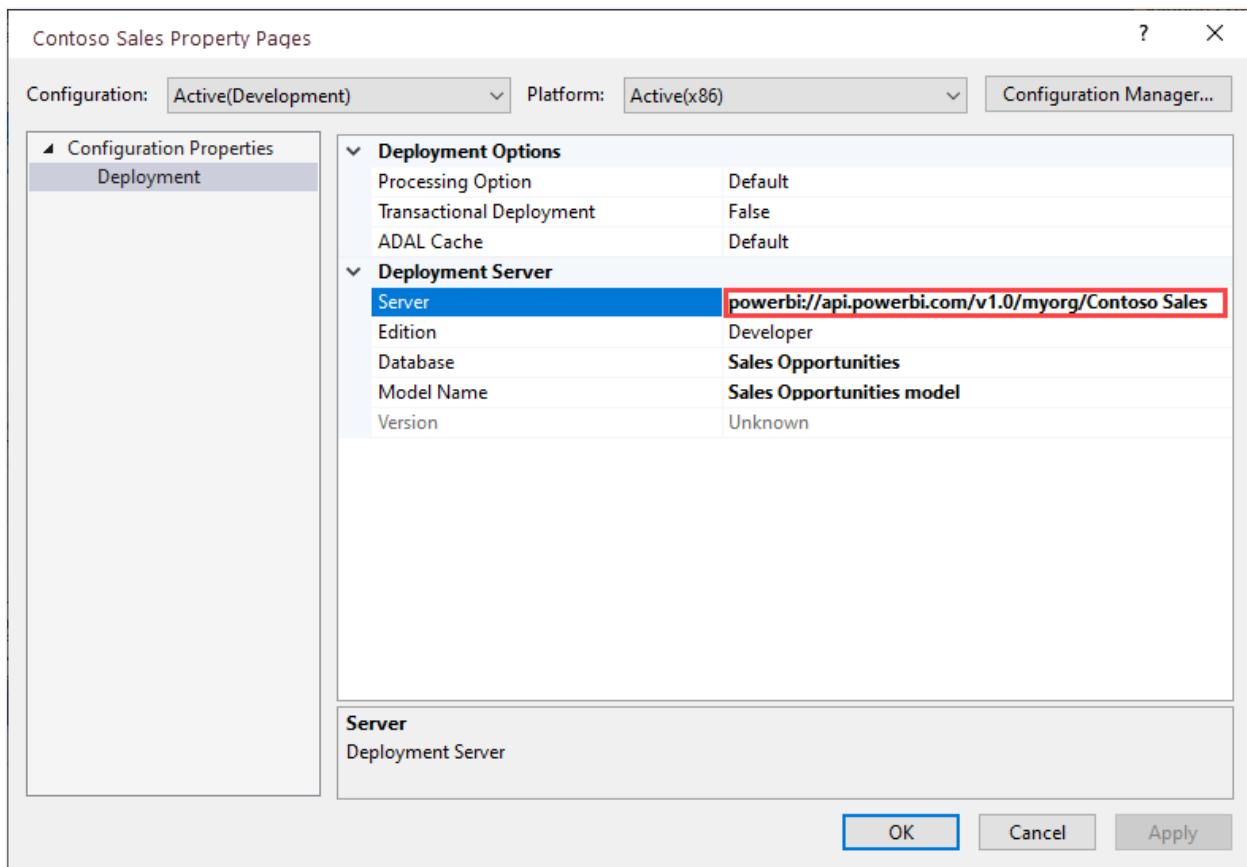
- PowerShell
- Azure Automation
- Azure Logic Apps
- Custom client applications

To learn more, see [Automate Premium workspace and dataset 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 dataset on the workspace.

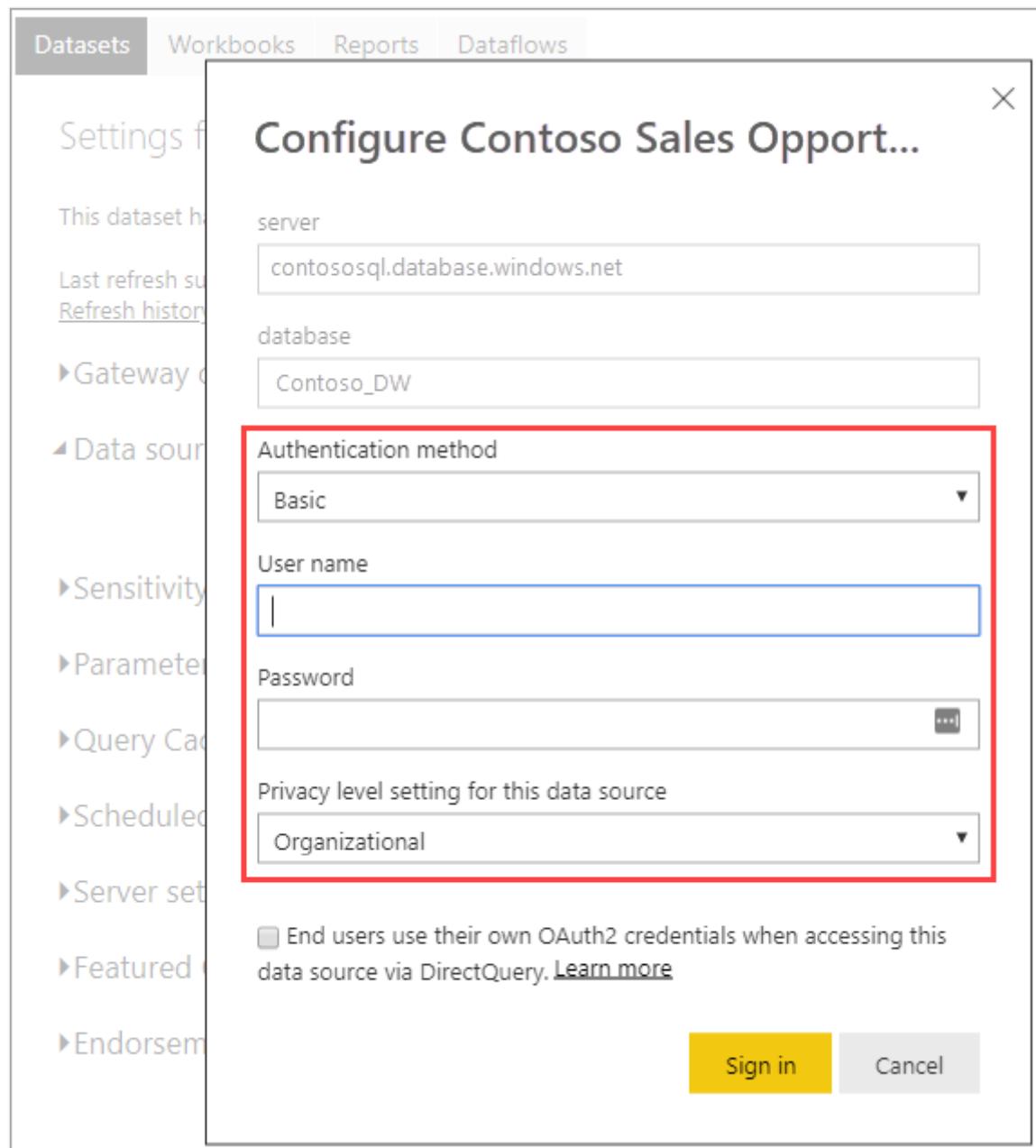
To deploy a tabular model project authored in Visual Studio, set the workspace connection URL in the project **Deployment Server** property. In Visual Studio, in **Solution Explorer**, right-click the project > **Properties**. In the **Server** property, paste the workspace connection URL.



When the Deployment Server property is specified, the project can be deployed.

When deployed the first time, a dataset is created in the workspace by using metadata from the model.bim. As part of the deployment operation, after the dataset is created in the workspace from model metadata, processing to load data into the dataset 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 dataset is created, data source credentials are then specified in the Power BI Service in dataset settings. In the workspace, select **Datasets > Settings > Data source credentials > Edit credentials**.



When data source credentials are specified, you can then refresh the dataset in the Power BI service, configure schedule refresh, or process (refresh) from SQL Server Management Studio to load data into the dataset.

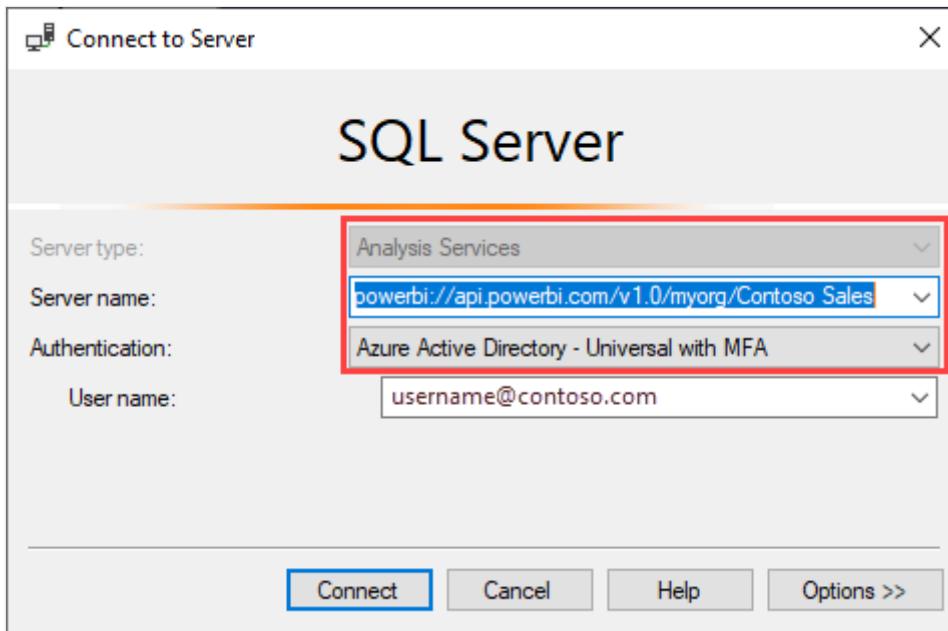
The deployment **Processing Option** property specified in the project in Visual Studio is observed. However, if a data source has not had credentials specified in the Power BI service, even if the metadata deployment succeeds, processing will fail. You can set the property to **Do Not Process**, preventing 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 dataset, processing as part of subsequent deployment operations will then succeed.

Connect with SSMS

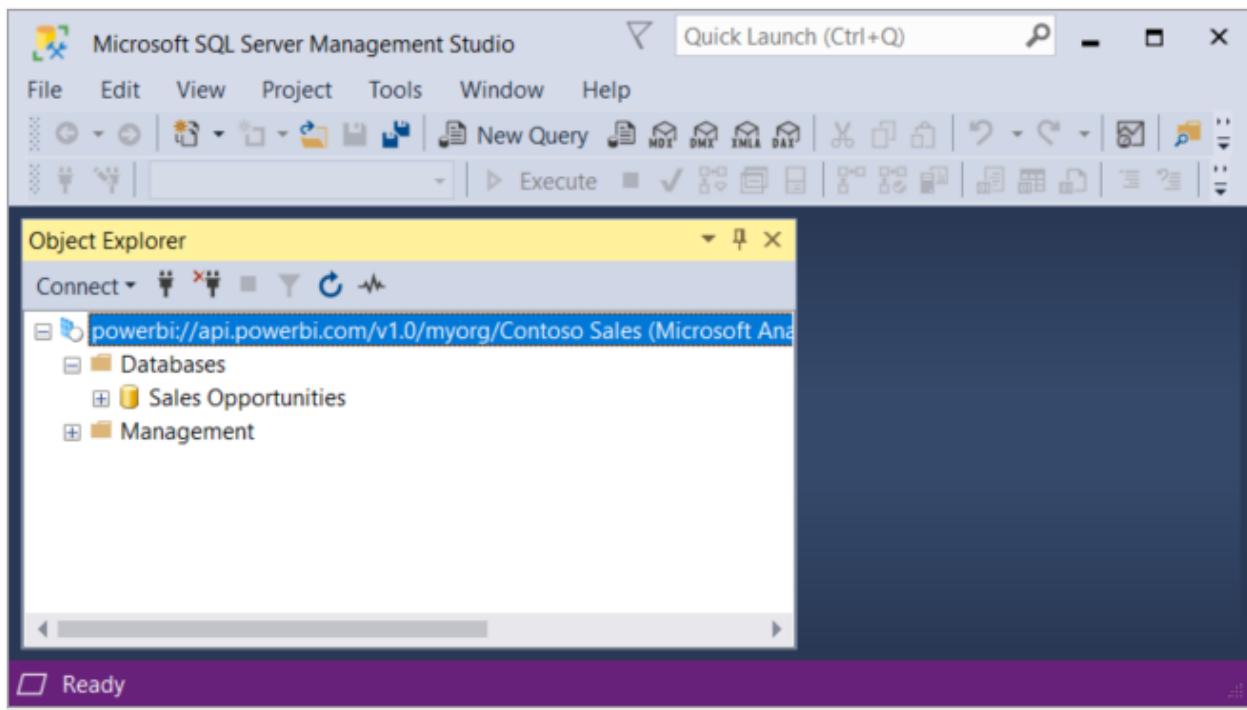
Using SSMS to connect to a workspace is just like connecting to an Azure or SQL Server Analysis Services server. The only difference is you specify the workspace URL in server name, and you must use **Active Directory - Universal with MFA** authentication.

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 datasets 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 \(TMSL\)](#)

Dataset 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 dataset refresh operations that include a write transaction through the XMLA endpoint are recorded and shown in dataset 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.

Refresh history

Scheduled OneDrive

On demand	7/14/2021, 12:17:07 PM	7/14/2021, 12:25:05 PM	Completed
Via XMLA Endpoint	7/14/2021, 11:32:49 AM	7/14/2021, 11:41:23 AM	Completed
On demand	7/14/2021, 11:18:38 AM	7/14/2021, 11:27:48 AM	Completed
On demand	7/14/2021, 10:55:10 AM	7/14/2021, 11:03:54 AM	Completed
On demand	7/14/2021, 9:21:54 AM	7/14/2021, 9:33:23 AM	Completed
Scheduled	7/14/2021, 7:04:01 AM	7/14/2021, 7:23:55 AM	Completed
On demand	7/13/2021, 10:15:28 PM	7/13/2021, 10:29:35 PM	Completed
On demand	7/13/2021, 6:13:34 PM	7/13/2021, 6:22:32 PM	Completed
On demand	7/13/2021, 4:21:05 PM	7/13/2021, 4:31:17 PM	Completed

Close

Dynamic Management Views (DMV)

Analysis Services [DMVs](#) provide visibility of dataset 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 datasets

Enhanced metadata

XMLA write operations on datasets authored in Power BI Desktop and published to a Premium workspace require enhanced metadata. To learn more, see [Enhanced dataset metadata](#).

 **Caution**

At this time, a write operation on a dataset 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

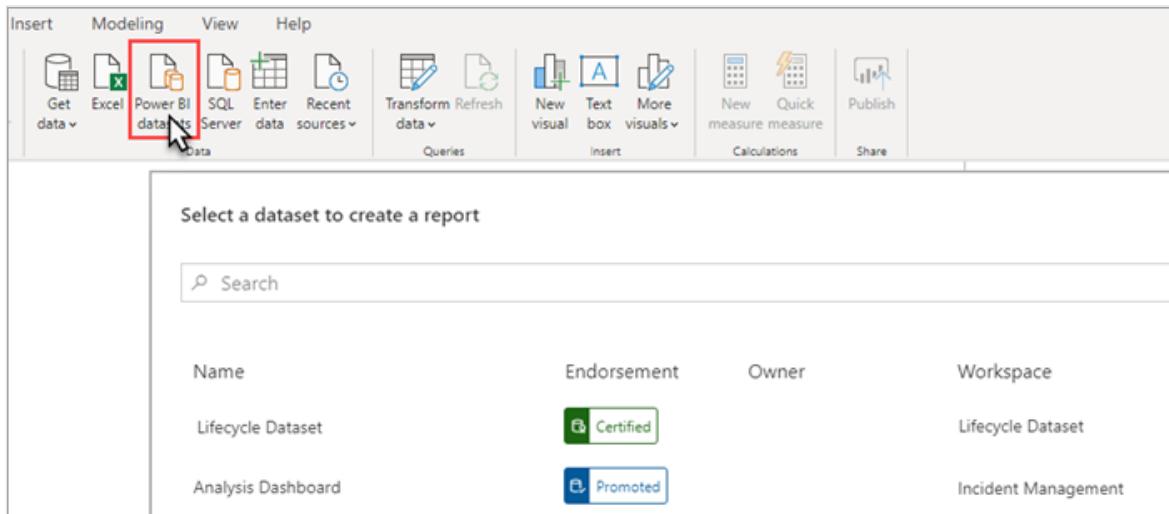
When connecting to data sources and querying data, Power BI Desktop uses Power Query M expressions as inline data source declarations. While supported in Premium

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](#).

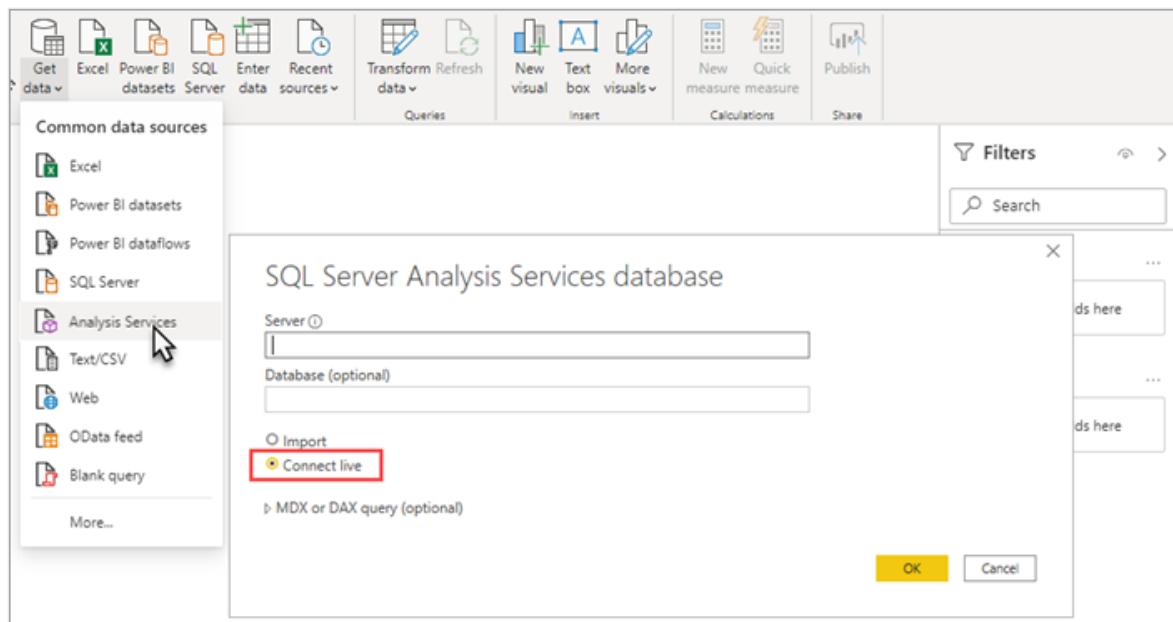
Power BI Desktop in live connect mode

Power BI Desktop can connect to a Power BI Premium dataset 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 datasets**, and then select a dataset to create a report. This is the **recommended** way for users to connect live to datasets. This method provides an improved discover experience showing the endorsement level of datasets. Users don't need to find and keep track of workspace URLs. To find a dataset, users simply type in the dataset name or scroll to find the dataset 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 dataset. In this case, Power BI Desktop uses the XMLA endpoint to connect live to the dataset 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 datasets 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:

Operation friendly name	Operation name
Connected to Power BI dataset from an external application	ConnectFromExternalApplication
Requested Power BI dataset refresh from an external application	RefreshDatasetFromExternalApplication
Created Power BI dataset from an external application	CreateDatasetFromExternalApplication
Edited Power BI dataset from an external application	EditDatasetFromExternalApplication
Deleted Power BI dataset from an external application	DeleteDatasetFromExternalApplication

To learn more, see [Auditing Power BI](#).

See also

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](#) ↗

Interactive and background operations

Article • 08/05/2022 • 2 minutes to read

Power BI 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 clicks on 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 dataset 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.

Operation list

The table below lists the Power BI operations. It provides a short description for each operation and identifies the operation's type.

Operation	Description	Workload	Type
Artificial intelligence (AI)	AI function evaluation	AI	Background
Background query	Queries for refreshing tiles and creating report snapshots	Datasets	Background
Dataflow DirectQuery	Connect directly to a dataflow without the need to import the data into a dataset	Dataflows	Interactive

Operation	Description	Workload	Type
Dataflow refresh	An on demand or scheduled background dataflow refresh, performed by the service or with REST APIs	Dataflows	Background
Dataset on-demand refresh	A background dataset refresh initiated by the user, using the service, REST APIs or public XMLA endpoints	Datasets	Background
Dataset scheduled refresh	A scheduled background dataset refresh, performed by the service, REST APIs or public XMLA endpoints	Datasets	Background
Full report email subscription	A PDF or PowerPoint copy of an entire Power BI report, attached to an email subscription	Report	Background
Interactive query	Queries initiated by an on-demand data request from a user. For example, loading a model when opening a report, or user interaction with a report	Datasets	Interactive
PublicApiExport	A Power BI report exported with the Export report to file REST API	Report	Background
Render	A Power BI paginated report exported with the Export paginated report to file REST API	Paginated report	Background
Render	A Power BI paginated report viewed in Power BI service	Paginated report	Interactive
XMLA read	XMLA read operations initiated by the user, for queries and discoveries	Datasets	Interactive
XMLA write	A background XMLA write operation that changes the model	Datasets	Background

Next steps

[What is Power BI Premium Gen2?](#)

[Power BI Premium Gen2 architecture](#)

[Managing Premium Gen2 capacities](#)

[Use the gen2 metrics app](#)

Premium support for China North

Article • 12/15/2022 • 2 minutes to read

China North is only supported when using [Premium Gen1](#).

[Premium Gen2](#) and Gen2 features are not supported when using *China North*.

If you require support for Gen2 or for any of the features listed in this article, use one of the other China regions, *China East*, *China East 2* or *China North 2*.

To learn how to migrate your tenant to another region, see [Move between regions](#).

Unsupported features

This section lists the Power BI features that aren't supported for *China North*.

- [Premium Gen2](#)
- Any Gen2 features
- [Paginated reports](#)
- Export Power BI reports to [PDF](#) and [PowerPoint](#)
- [Email subscriptions](#)
- [Copy paste visuals](#) in Power BI reports

Next steps

[What is Power BI Premium?](#)

Troubleshoot XMLA endpoint connectivity

Article • 12/19/2022 • 14 minutes to read

XMLA endpoints in Power BI rely on the native Analysis Services communication protocol for access to Power BI datasets. 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 [Dataset 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 dataset 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=<application secret>

For example:

```
Data Source=powerbi://api.powerbi.com/v1.0/myorg/Contoso;Initial  
Catalog=PowerBI_Dataset;User ID=app:91ab91bb-6b32-4f6d-8bbc-97a0f9f8906b@19373176-316e-  
4dc7-834c-328902628ad4;Password=6drX...;
```

If you receive the following error:

"We cannot connect to the dataset 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 Azure Active Directory B2B

With support for Azure Active Directory (Azure AD) business-to-business (B2B) in Power BI, you can provide external guest users with access to datasets 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 Azure AD B2B](#).

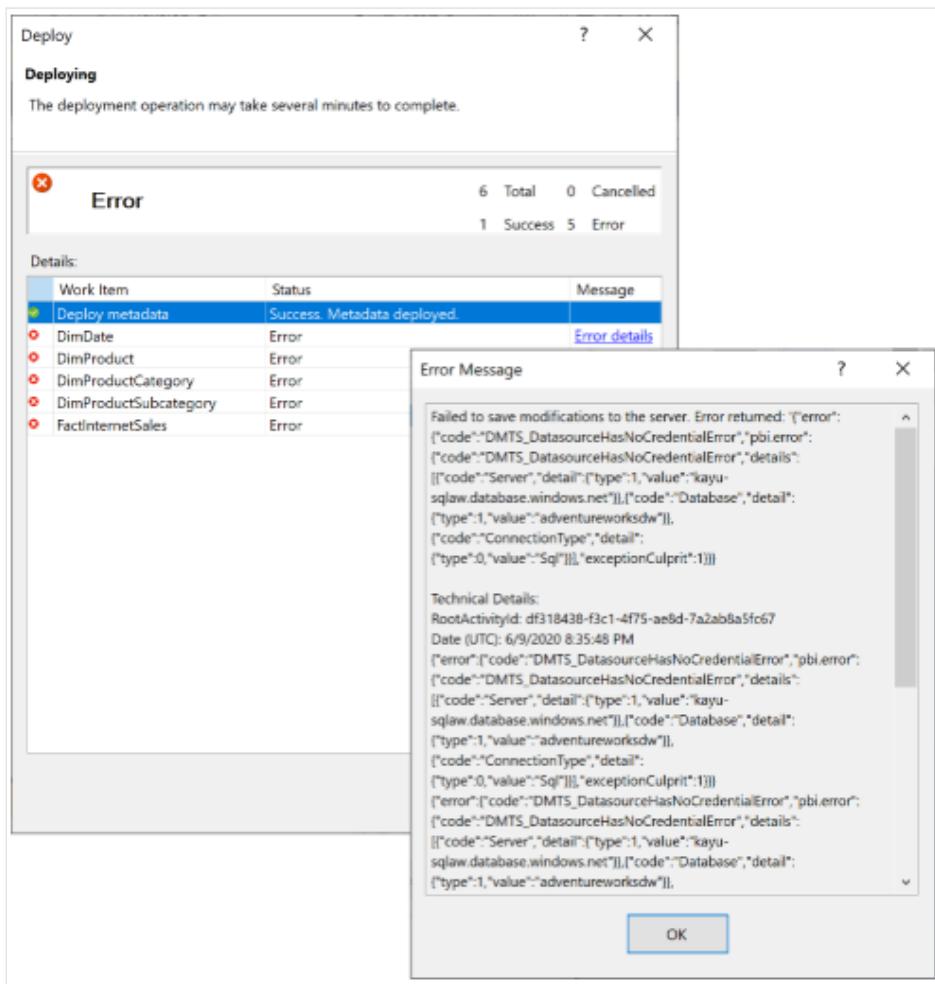
Deploying a dataset

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 Dataset connectivity with the XMLA endpoint article.

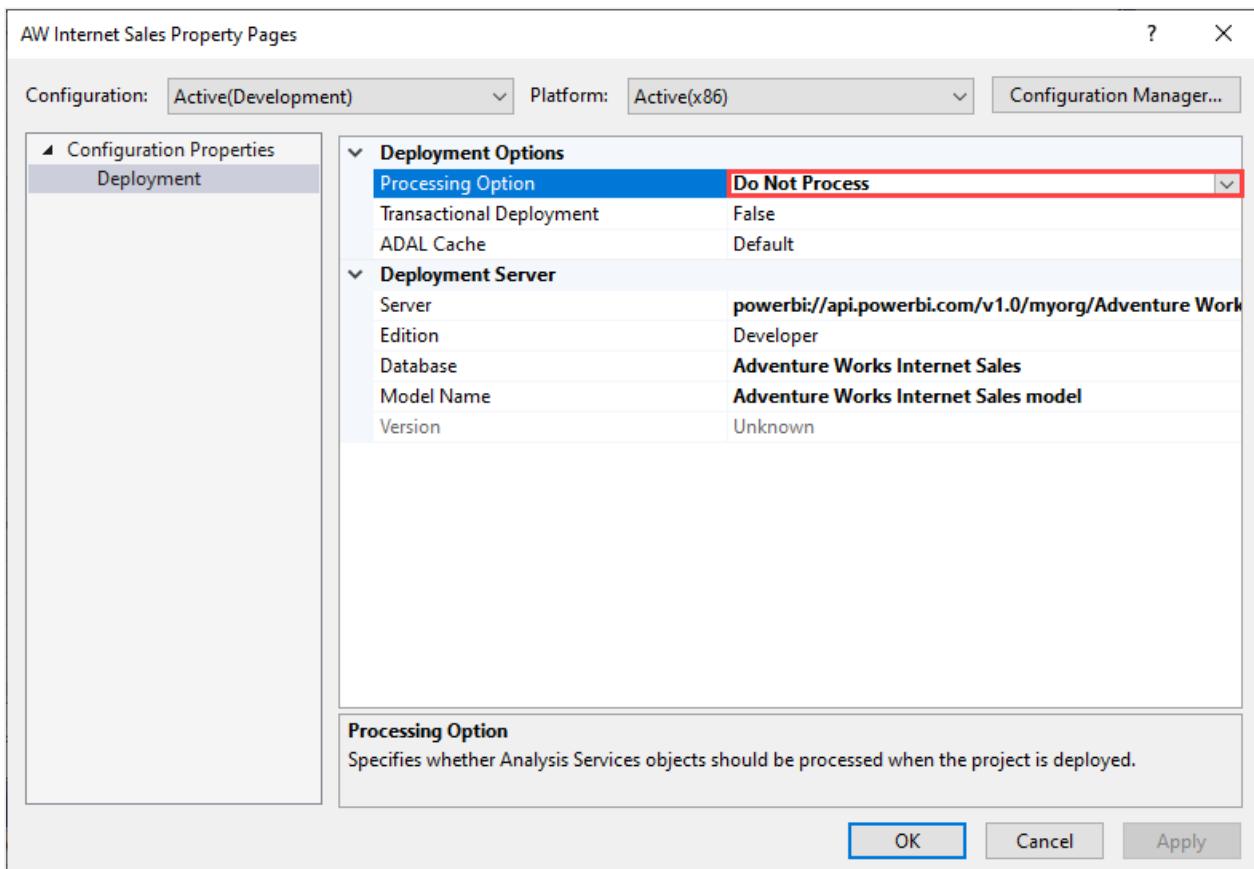
Deploying a new model

In the default configuration, Visual Studio attempts to process the model as part of the deployment operation to load data into the dataset 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 datasets, you must specify the data source credentials in the dataset settings using the Power BI user interface (**Datasets > 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 dataset, after metadata deployment has succeeded and the dataset has been created.

If Power BI cannot bind your new dataset 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 dataset in the Power BI user interface.



New project from an existing dataset

Creating a new tabular project in Visual Studio by importing the metadata from an existing dataset is not supported. However, you can connect to the dataset by using SQL Server Management Studio, script out the metadata, and reuse it in other tabular projects.

Migrating a dataset 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.

OLE DB Driver for SQL Server	.NET Framework Data Provider for SQL Server
Provider=SQLNCLI11;Data	Data Source=sqldb.database.windows.net;Initial
Source=sqldb.database.windows.net;Initial	Catalog=AdventureWorksDW2016;Integrated
Catalog=AdventureWorksDW;Trusted_Connection=yes;	Security=SSPI;Encrypt=true;TrustServerCertificate=false

Cross-referencing partition sources

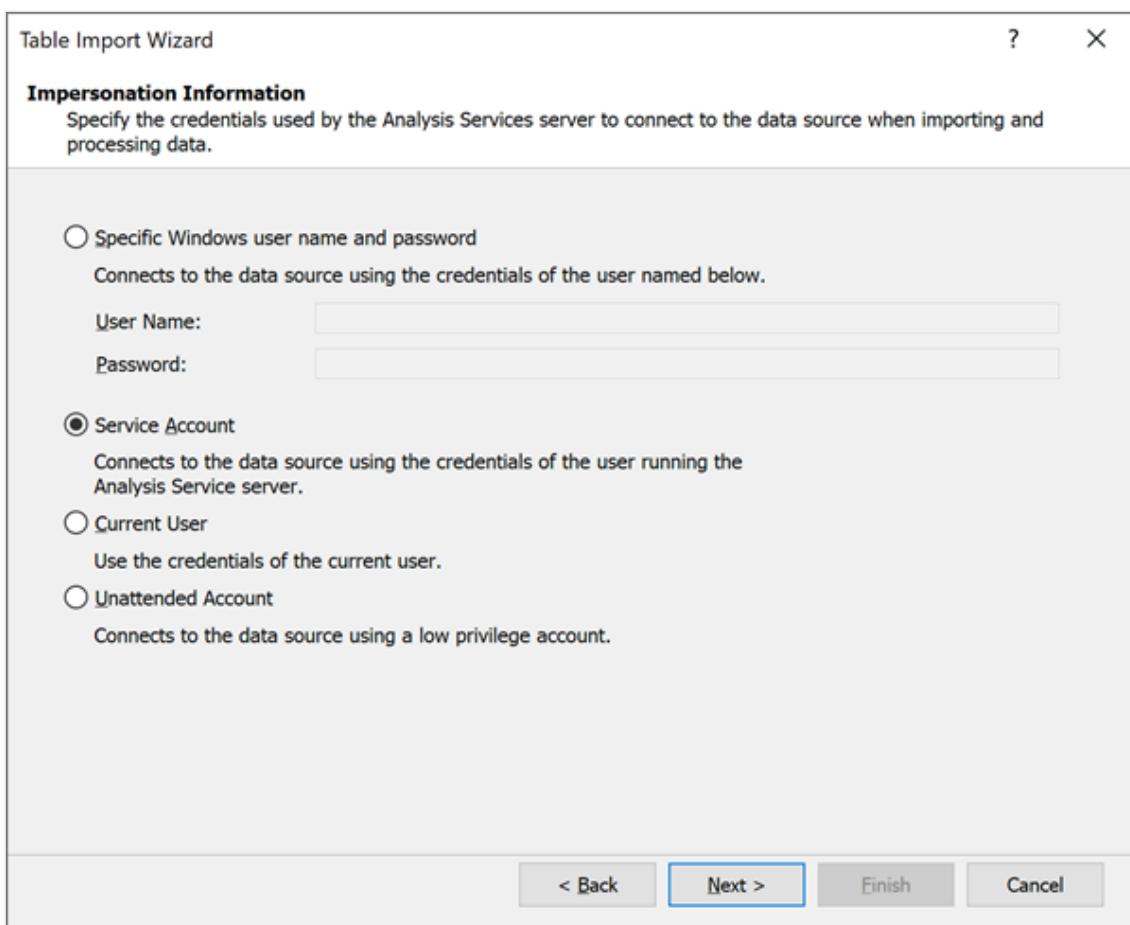
Just as there are multiple data source types, there are also multiple partition source types a tabular model can include to import data into a table. Specifically, a partition can use a query partition source or an M partition source. These partition source types, in turn, can reference provider data 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 dataset, the following table describes supported configurations:

Data source	Partition source	Comments	Supported with XMLA endpoint
Provider data source	Query partition source	The AS engine uses the cartridge-based connectivity stack to access the data source.	Yes
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

Data source	Partition source	Comments	Supported with XMLA endpoint
Structured data source	M partition source	The AS engine uses the Mashup engine to import the data.	Yes

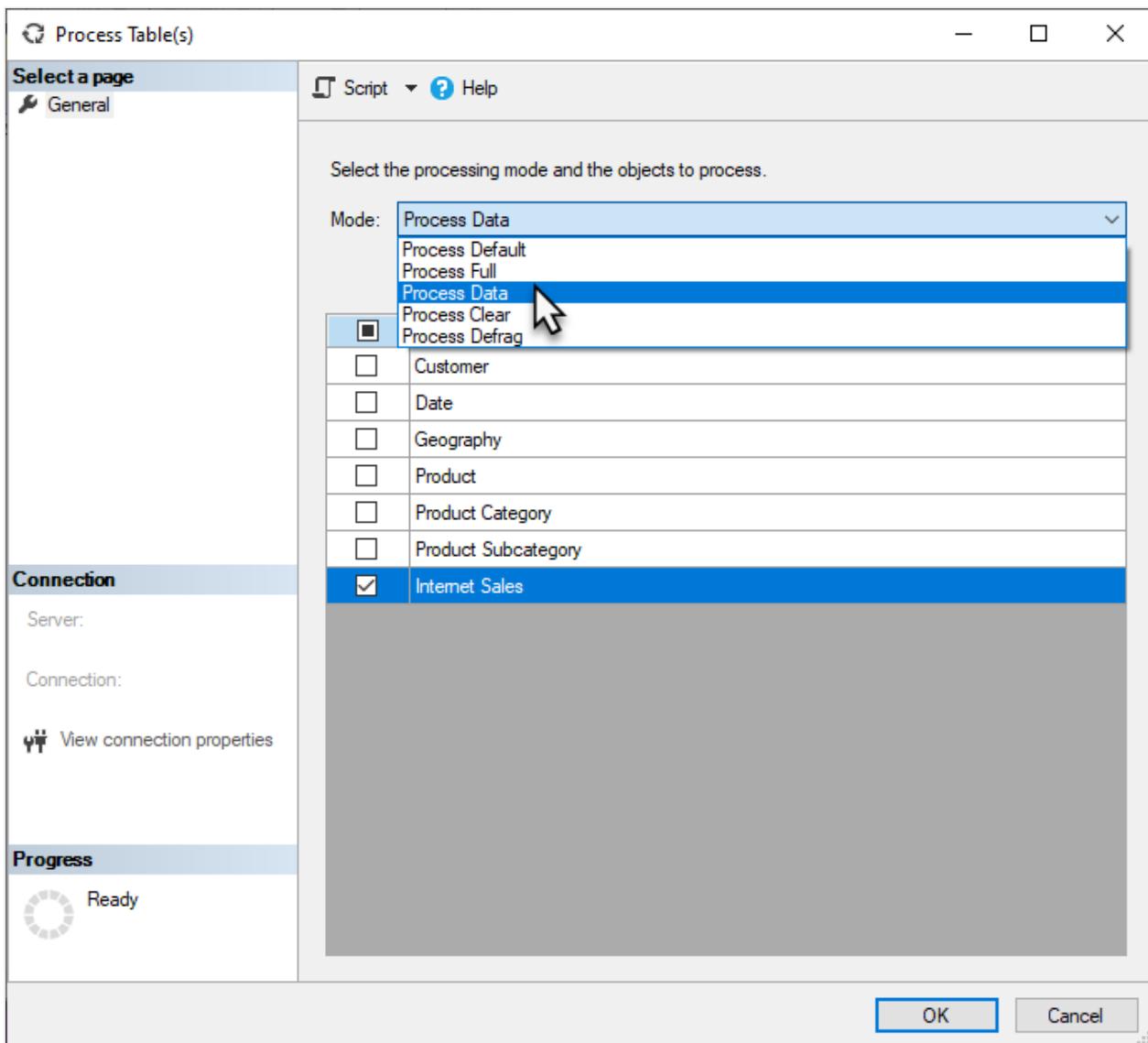
Data sources and impersonation

Impersonation settings you can define for provider data sources are not relevant for Power BI. Power BI uses a different mechanism based on dataset 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 dataset. 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

Datasets that are refreshed using an XMLA endpoint don't trigger an [email subscription](#).

Errors on Premium Gen 2 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 datasets](#) 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 [Premium Gen2](#) or an [Embedded Gen2](#) 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](#).

Refresh operations in SSMS

When using SSMS v18.7.1 or lower to perform a long running (>1 min) refresh operation on a dataset in a Premium Gen2 or an [Embedded Gen2](#) capacity, SSMS may display an error like the following even though the refresh operation succeeds:

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

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](#).

Other client applications and tools

Client applications and tools such as Excel, Power BI Desktop, SSMS, or external tools connecting to and working with datasets in Power BI Premium Gen2 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 datasets in a Premium Gen2 capacity through the XMLA endpoint are:

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 dataset, 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:

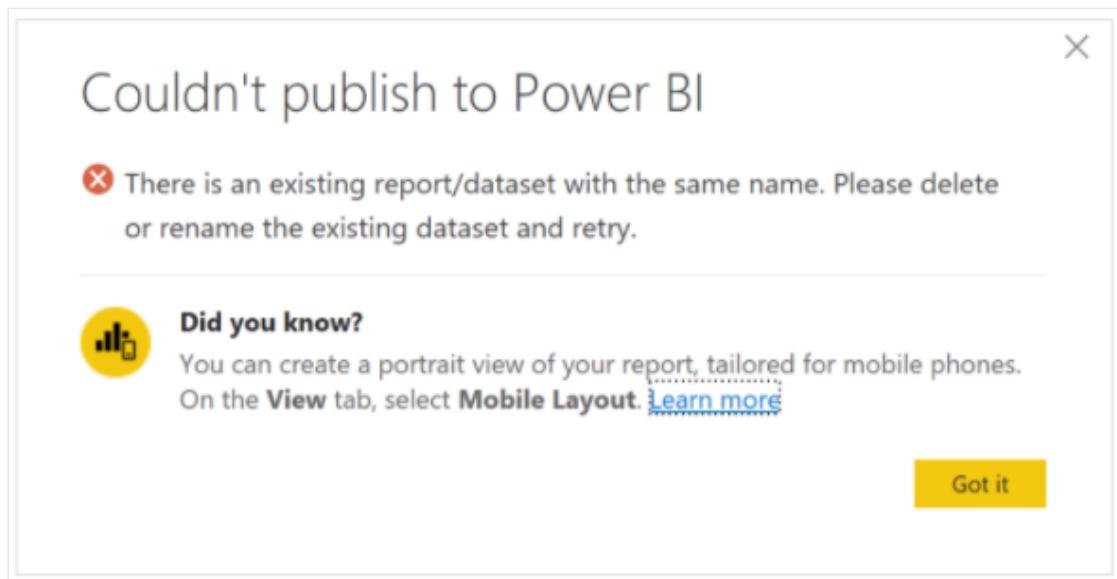
JSON

```
{  
  "createOrReplace": {
```

```
"object": {
    "database": "AdventureWorks",
    "role": "Role"
},
"role": {
    "name": "Role",
    "modelPermission": "read",
    "members": [
        {
            "memberName": "xxxx",
            "identityProvider": "AzureAD"
        },
        {
            "memberName": "xxxx"
            "identityProvider": "AzureAD"
        }
    ]
}
}
```

Publish Error - Live connected dataset

When republishing a live connected dataset utilizing the Analysis Services connector, the following error, **"There is an existing report/dataset with the same name. Please delete or rename the existing dataset and retry."** may be shown.



This is due to the dataset being published having a different connection string but having the same name as the existing dataset. To resolve this issue, either delete or rename the existing dataset. 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.

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 Gen 2

Premium Gen2 capacities use resource governing to ensure no single dataset 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 dataset (database) size, the effective memory limit also applies to underlying dataset 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 dataset by the capacity (25 GB, 50 GB, 100 GB) and how much memory the dataset is already consuming when the command starts executing. For example, a dataset 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 dataset 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 dataset is hosted or reduce the memory footprint of your dataset 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 dataset 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 dataset is hosted or reduce the memory footprint of your dataset 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 dataset.
- Reduce the memory footprint of your dataset 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.

See also

[Dataset connectivity with the XMLA endpoint](#)

[Automate Premium workspace and dataset tasks with service principals](#)

[Troubleshooting Analyze in Excel](#)

[Tabular model solution deployment](#)

Power BI Premium Gen2 FAQ

FAQ

This article addresses questions frequently asked about Power BI Premium Gen2. For an overview, see [What is Power BI Premium Gen2?](#).

- If you have other questions, [try asking the Power BI Community](#).
- Still have an issue? Visit the [Power BI support page](#).

Power BI Premium Gen2

This section addresses questions and answers for Power BI Premium Gen2.

What is Power BI Premium Generation 2?

Power BI Premium recently released a new version of Power BI Premium, **Premium Gen2**. Premium Gen2 will simplify the management of Premium capacities, and reduce management overhead. For more information about Premium Gen2, see [Power BI Premium Generation 2](#).

How can I control the costs of autoscaling?

Autoscaling is an optional feature of Premium Gen2, 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. If the subscription's budget is exhausted, Power BI is prevented from using the v-core resources for that subscription, and autoscale shuts off. You can set a budget for the Azure subscription that autoscale uses by following the [Azure budget tutorial](#).

How does resource utilization cause Gen2 to autoscale?

Power BI Premium Gen2 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 twenty-four hours, where each background operation contributes only 1/2880 of its total CPU cost (there are 2880 evaluation cycles in each 24-hour period).

A capacity consists of a defined number of v-cores. The [Power BI Premium Utilization and 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 will autoscale 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 have already autoscaled using one v-core, your maximum capacity is now at 270 ($240 + 1 \times 30$) 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?

If a capacity's utilization exceeded a 100% and it cannot use autoscale, due to being turned off or already at its maximum v-core utilization value, the capacity enters into a temporary *interactive request delay* mode, during which each interactive request (such as report load, visual interaction, and so on) is delayed before it is sent to the engine for execution. The amount of delay is proportional to the amount of overload detected. Overload of 100% will incur a delay of 20 seconds.

The capacity stays in *interactive request delay* mode if the previous evaluation is at greater than 100% resource usage.

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 from step 1 is multiplied by the count of interactive operations that were 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. You can use the report to indicate how close you are to your capacity's maximum resources, and if you save monthly snapshots, you can compare them to indicate trends of growth and extrapolate the rate in which you will arrive at 100% utilization of your resources.

How can my utilization data inform me I should turn on autoscale?

Utilization data does not currently indicate whether requests were throttled due to capacity being in *interactive request delay* mode. The information will be 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 will be 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 Gen2 beyond CPU time?

Today, customers don't have visibility through utilization data to the memory footprint of their operations, and cannot 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](#).

By displaying your capacity's CPU usage levels, the [Power BI Premium Utilization and Metrics](#) app helps you understand how your capacity is performing. To provide a simple 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 that's displayed in the app.

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 Gen2?](#)
- [Using Autoscale with Power BI Premium](#)
- [Extended Pro Trial activation](#)
- [Power BI Embedded FAQ](#)

More questions? [Try asking the Power BI Community](#) ↗

Metadata scanning

Article • 12/07/2022 • 4 minutes to read

Metadata scanning facilitates governance over your organization's Power BI data by making it possible to quickly catalog and report on all the metadata of your organization's Power BI artifacts. It accomplishes this using a set of Admin REST APIs that are collectively known as the scanner APIs.

With the scanner APIs, you can extract information such as artifact name, owner, sensitivity label, endorsement status, and last refresh. For datasets, you can also extract metadata of some of the objects they contain, such as table and column names, measures, DAX expressions, mashup queries, and so forth. The metadata of these dataset internal objects is referred to as sub-artifact metadata.

For a more extensive list of the artifact and sub-artifact metadata that metadata scanning returns, see the [documentation for the Admin - WorkspaceInfo GetScanResult API](#).

The following are the scanner APIs. They support both public and sovereign clouds.

- [GetModifiedWorkspaces](#)
- [WorkspaceGetInfo](#)
- [WorkspaceScanStatus](#)
- [WorkspaceScanResult](#)

Before metadata scanning can be run, a Power BI admin needs to set it up. See [Setting up metadata scanning in an organization](#).

Important

The app you develop for scanning can authenticate via either a standard delegated admin access token or a service principal. The two authentication paths are mutually exclusive. **When running under a service principal, there must be no Power BI admin-consent-required permissions set on your app.** For more information, see [Enable service principal authentication for read-only admin APIs](#).

Run metadata scanning

The following short walkthrough shows how to use the scanner APIs to retrieve metadata from your organizations artifacts. It assumes that a Power BI admin has set up

metadata scanning in your organization.

Step 1: Perform a full scan

Call [workspaces/modified](#) without the **modifiedSince** parameter to get the complete list of workspace IDs in the tenant. This retrieves all the workspaces in the tenant, including personal workspaces and shared workspaces. If you wish to exclude personal workspaces from the scan, use the [workspaces/modified](#) **excludePersonalWorkspaces** parameter.

Divide the list into chunks of 100 workspaces at most.

For each chunk of 100 workspaces:

Call [workspaces/getInfo](#) to trigger a scan call for these 100 workspaces. You'll receive the scanId in the response to use in the next steps. In the location header, you'll also receive the URI to call for the next step.

ⓘ Note

Not more than 16 calls can be made simultaneously. The caller should wait for a scan succeed/failed response from the [scanStatus](#) API before invoking another call.

If some metadata you expected to receive is not returned, check with your Power BI admin to make sure they have **enabled all relevant admin switches**.

Use the URI from the location header you received from calling [workspaces/getInfo](#) and poll on [workspaces/scanStatus/{scan_id}](#) until the status returned is "Succeeded". This means the scan result is ready. It's recommended to use a polling interval of 30-60 seconds. In the location header, you'll also receive the URI to call in the next step. Use it only once the status is "Succeeded".

Use the URI from the location header you received from calling [workspaces/scanStatus/{scan-id}](#) and read the data using [workspaces/scanResult/{scan_id}](#). The data contains the list of workspaces, artifact info, and other metadata based on the parameters passed in the [workspaces/getInfo](#) call.

Step 2: Perform an incremental scan

Now that you have all the workspaces and the metadata and lineage of their assets, it's recommended that you perform only incremental scans that reference the previous scan that you did.

Call [workspaces/modified](#) with the `modifiedSince` parameter set to the start time of the last scan in order to get the workspaces that have changed and which therefore require another scan. The `modifiedSince` parameter should be set for a date within the last 30 days.

Divide this list into chunks of up to 100 workspaces, and get the data for these changed workspaces using the three API calls, [workspaces/getInfo](#), [workspaces/scanStatus/{scan_id}](#), and [workspaces/scanResult/{scan_id}](#), as described in Step 1 above.

Considerations and limitations

- Datasets that haven't been refreshed or republished will be returned in API responses but without their sub-artifact information and expressions. For example, you'll see dataset name and lineage in the response, but not the dataset's table and column names.
- Datasets containing only DirectQuery tables will return sub-artifact metadata only if they've been republished since enhanced metadata scanning has been enabled. This is because DirectQuery datasets don't use the regular Power BI dataset refresh flow that triggers caching. If, however, a dataset also contains tables that use import mode, caching takes place upon dataset refresh as described above, and it isn't necessary for the dataset to be republished in order for sub-artifact metadata to be returned.
- Autogenerated datasets, [real-time datasets](#), datasets with [Object Level Security](#), datasets with a live connection to AS-Azure and AS on-premises, and Excel full fidelity datasets aren't supported for sub-artifact metadata. For unsupported datasets, the response returns the reason for not getting the sub-artifact metadata from the dataset. It's found in a field named `schemaRetrievalError`, for example, `schemaRetrievalError: Unsupported request for RealTime model`.
- The API doesn't return sub-artifact metadata for dataset tables whose `Enable load` property is set to off. For instance, if your dataset has four tables, but one has the `Enable load` property turned off, metadata will be returned only for three tables. The `Enable load` property is typically on, but it may be turned off in some cases where it was deemed desirable not to load the table for some reason. See [Managing loading of queries](#), for instance.
- The API doesn't return sub-artifact metadata for datasets that are larger than 1 GB in shared workspaces. For Premium workspaces there's no size limitation.

Licensing

Metadata scanning requires no special license. It works for all of your tenant metadata, including that of artifacts that are located in non-Premium workspaces.

Next steps

- [Power BI REST Admin APIs](#)
- [Set up metadata scanning](#)
- [Enable service principal authentication for read-only admin APIs](#)
- [WorkspaceInfo GetScanResult](#).
- More questions? Try asking the [Power BI Community](#) ↗

Data protection in Power BI

Article • 12/29/2022 • 2 minutes to read

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 datasets, 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](#)
- [Microsoft Business Applications Summit video session - Power BI and Microsoft Purview Information Protection - The game changer for secure BI](#)
- [Power BI implementation planning: Information protection and data loss prevention](#)

Sensitivity labels in Power BI

Article • 12/29/2022 • 20 minutes to read

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 datasets, 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, datasets, 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 will not 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 dataset, 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 (Service only), 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 dataset.
- PivotTable in Excel with a live connection to a Power BI dataset, 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 dataset have different labels, the more restrictive label will be applied to the .pbix file.

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.

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Finance Report	Report	Finance Department	10/29/19, 3:49:04 PM	—	—	Confidential/Internal...	<input checked="" type="checkbox"/> Yes
New Report	Report	Finance Department	6/5/19, 2:21:33 AM	—	—	Highly Confidential/Internal...	<input checked="" type="checkbox"/> Yes
Sales 2019	Dashboard	Finance Department	—	—	—	Confidential/Internal...	<input checked="" type="checkbox"/> Yes
Sales 2019 - External	Report	Finance Department	6/7/19, 6:32:05 PM	—	—	Confidential/Internal...	<input checked="" type="checkbox"/> Yes
T - Profitability	Workbook	Finance Department	6/5/19, 2:21:33 AM	—	—	—	<input checked="" type="checkbox"/> Yes

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](#).

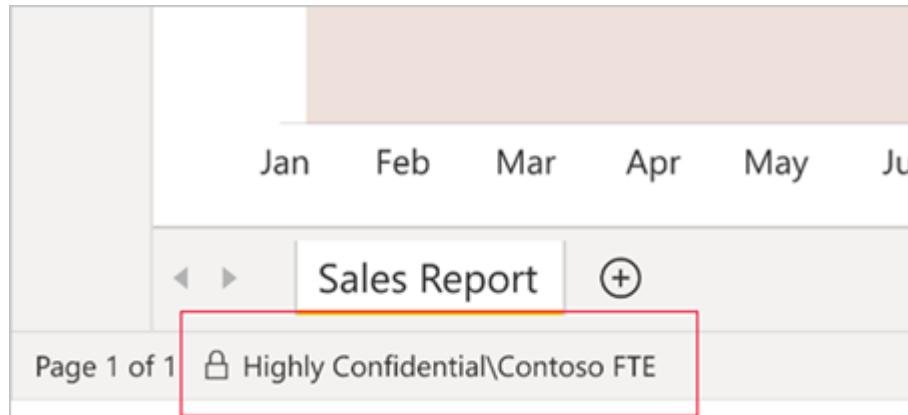
If you apply a sensitivity label in Desktop, when you publish your work to the service, or when you upload a .pbix file of that work to the service, the label travels with the data into the service. In the service, the label will be applied to both the dataset and the report that you get with the file. If the dataset 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 dataset 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 dataset 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 dataset or report. For example, a new report created on top of a dataset that has a "Highly Confidential" sensitivity label will automatically receive the "Highly Confidential" label as well.

The following image shows how a dataset's sensitivity label is automatically applied on a new report that is built on top of the dataset.

Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Report	Finance Department	10/29/19, 3:49:04 PM	—	—	Highly Confidential/internal...	<input checked="" type="checkbox"/> Yes
Dashboard	Finance Department	—	—	—	Confidential/internal...	<input checked="" type="checkbox"/> Yes
Report	Finance Department	6/7/19, 6:32:05 PM	—	—	Confidential/internal...	<input checked="" type="checkbox"/> Yes
Workbook	Finance Department	6/5/19, 2:21:33 AM	—	—	—	<input checked="" type="checkbox"/> Yes

ⓘ 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 (preview)

Power BI datasets that connect to sensitivity-labeled data in supported data sources can inherit those labels so that the data remains classified and secure when brought into Power BI. 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 dataset or report in the Power BI service, it is possible to have the label trickle down and be automatically applied to content that is built from that dataset 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 (preview)

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 Power BI \(preview\)](#) 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](#).

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 programmatically. See the following:

- [Admin - InformationProtection SetLabelsAsAdmin](#)
- [Admin - InformationProtection RemoveLabelsAsAdmin](#)

Auditing for activity on sensitivity labels

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. 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 (service only) 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 dataset 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.

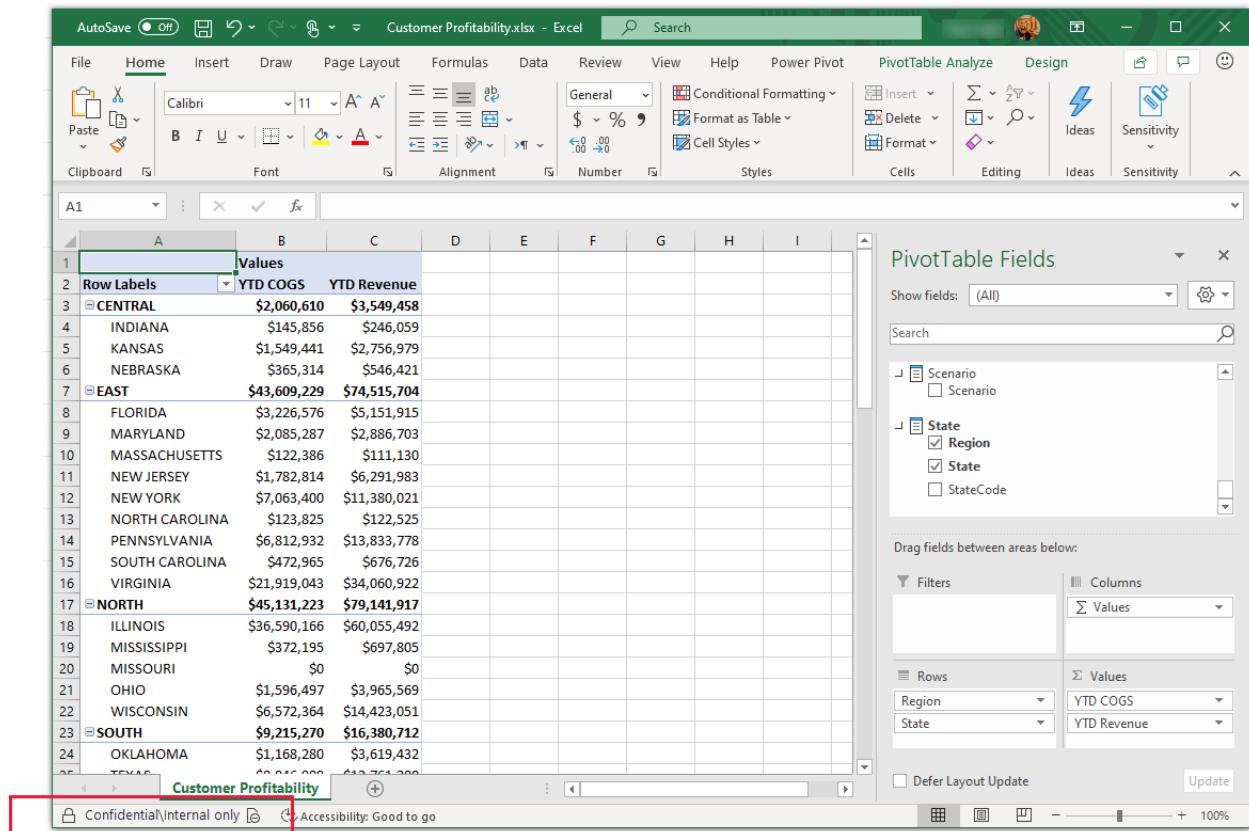
Applying a sensitivity label and protection to an exported file doesn't add content marking to the file. However, if the label is configured to apply content markings, the markings are automatically applied by the Azure Information Protection unified labeling client when the file is opened in Office 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, click 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 dataset (you can do this either from Power BI through [Analyze In Excel](#) or from [Excel](#)), the dataset's

sensitivity label is inherited and applied to your Excel file, along with any associated protection. If the label on the dataset later changes to a more restrictive one, the label applied on the linked Excel file will automatically update upon data refresh.



The screenshot shows a Microsoft Excel window titled "Customer Profitability.xlsx - Excel". A PivotTable is displayed with columns for "YTD COGS" and "YTD Revenue". The PivotTable Fields pane on the right shows fields for "Region", "State", and "StateCode". A banner at the bottom left of the Excel window reads "Confidential/Internal only" and "Accessibility: Good to go".

	B	C
1	Values	
2 Row Labels	YTD COGS	YTD Revenue
3 CENTRAL	\$2,060,610	\$3,549,458
4 INDIANA	\$145,856	\$246,059
5 KANSAS	\$1,549,441	\$2,756,979
6 NEBRASKA	\$365,314	\$546,421
7 EAST	\$43,609,229	\$74,515,704
8 FLORIDA	\$3,226,576	\$5,151,915
9 MARYLAND	\$2,085,287	\$2,886,703
10 MASSACHUSETTS	\$122,386	\$111,130
11 NEW JERSEY	\$1,782,814	\$6,291,983
12 NEW YORK	\$7,063,400	\$11,380,021
13 NORTH CAROLINA	\$123,825	\$122,525
14 PENNSYLVANIA	\$6,812,932	\$13,833,778
15 SOUTH CAROLINA	\$472,965	\$676,726
16 VIRGINIA	\$21,919,043	\$34,060,922
17 NORTH	\$45,131,223	\$79,141,917
18 ILLINOIS	\$36,590,166	\$60,055,492
19 MISSISSIPPI	\$372,195	\$697,805
20 MISSOURI	\$0	\$0
21 OHIO	\$1,596,497	\$3,965,569
22 WISCONSIN	\$6,572,364	\$14,423,051
23 SOUTH	\$9,215,270	\$16,380,712
24 OREGON	\$1,168,280	\$3,619,432
TEXAS	\$0	\$0

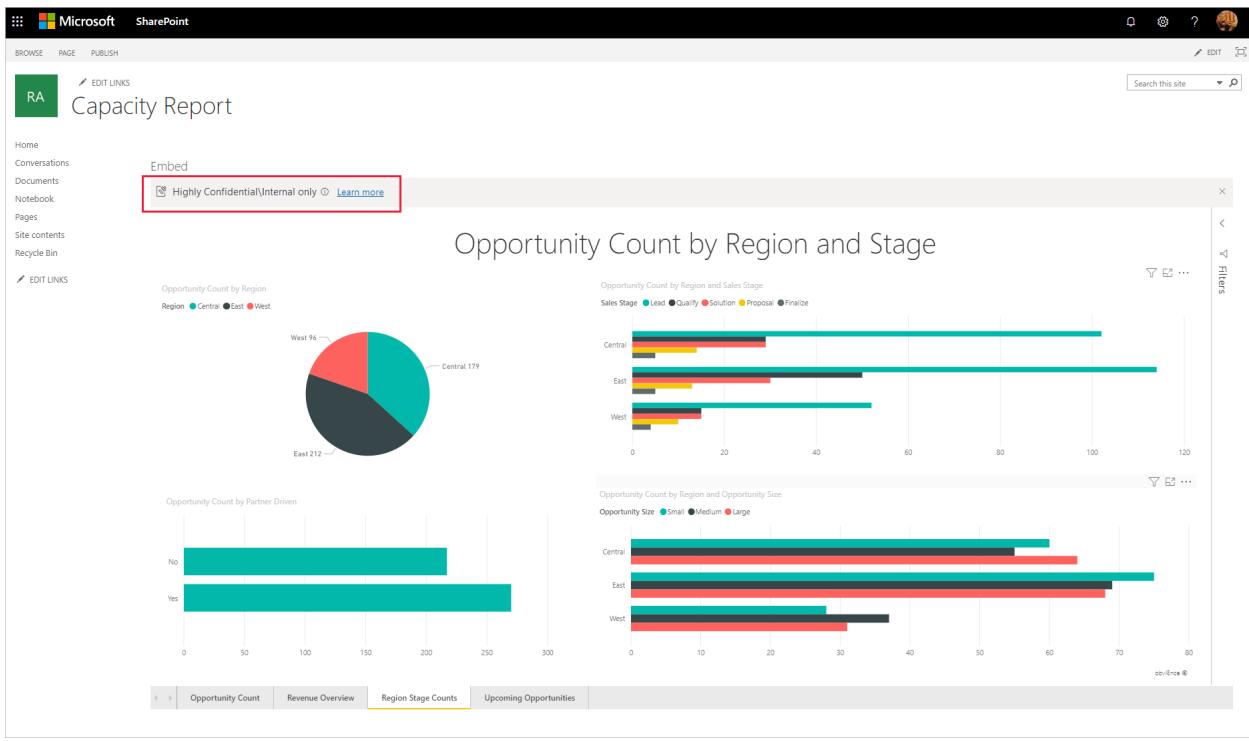
Sensitivity labels in Excel that were manually set aren't automatically overwritten by the dataset's sensitivity label. Rather, a banner notifies you that the dataset has a sensitivity label and recommends that you apply it.

! Note

If the dataset'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

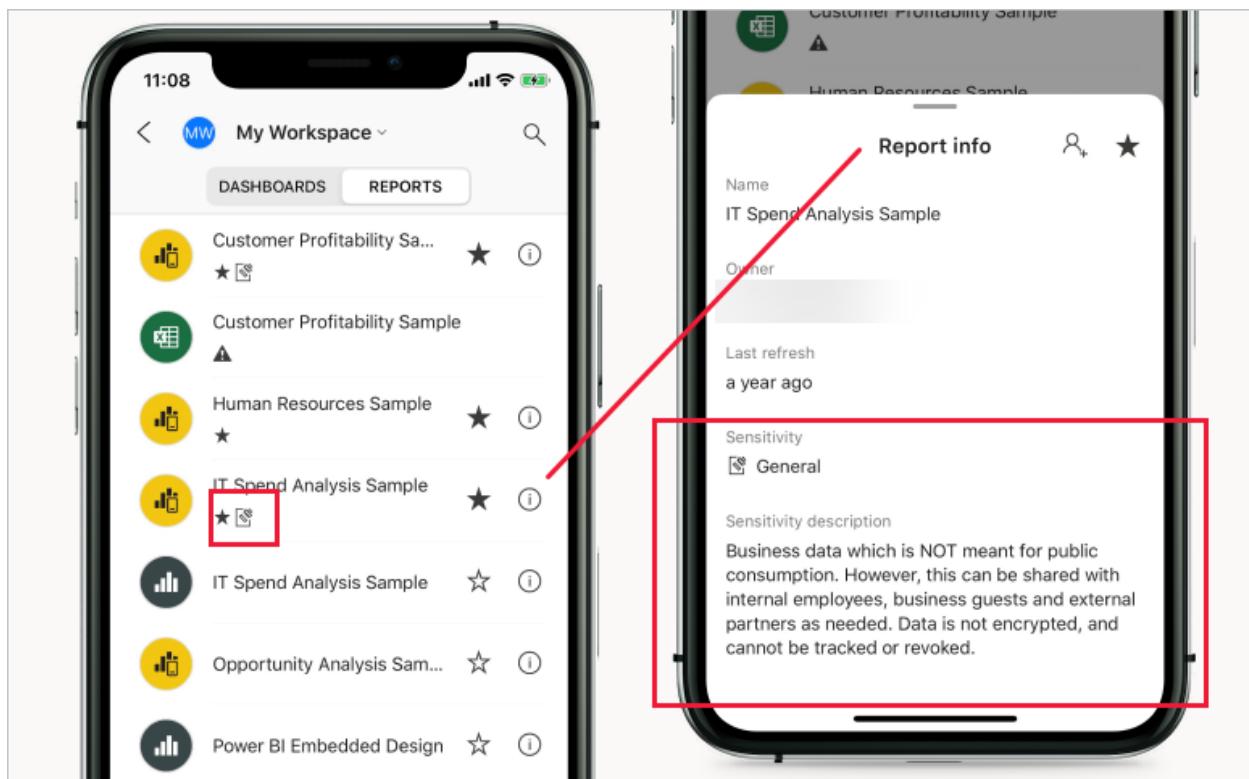
Sensitivity labels can be applied to paginated reports hosted in the Power BI service. After uploading a paginated report to the service, you apply the label to the report just as you would to a regular Power BI report. See [Sensitivity label support for paginated reports](#) for detail.

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 clouds:

- [US Government](#): GCC, GCC High, DoD
- China

Sensitivity labels are not currently supported in other national clouds.

Licensing and requirements

See [Licensing and requirements](#).

Sensitivity label creation and management

Sensitivity labels are created and managed in the [Purview compliance portal](#).

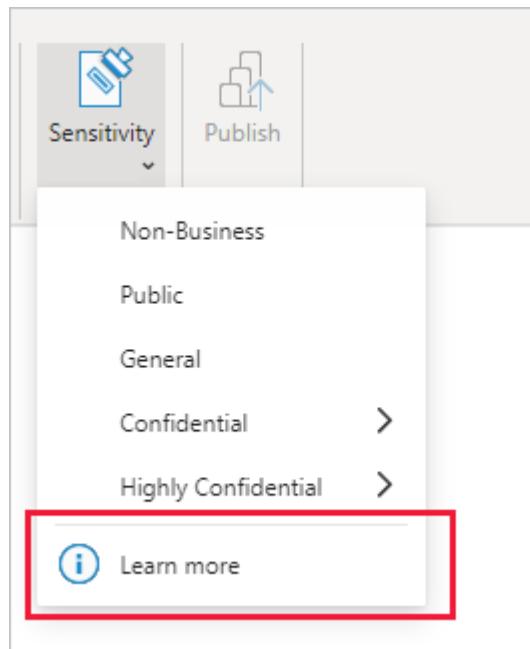
To access sensitivity labels in either of these centers, navigate to **Classification > Sensitivity labels**. These sensitivity labels can be used by multiple Microsoft services such Azure Information Protection, Office apps, and Office 365 services.

ⓘ 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

- Don't use parent labels. A parent label is a label that has sublabels. You cannot 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 will not be inherited.
- Mandatory label policies will not 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 is 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 dataset 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.
- Power BI doesn't support sensitivity labels of the [Do Not Forward](#), [user-defined](#), and [HYOK](#) protection types. The Do Not Forward and user-defined protection types refer to labels defined in the [Purview compliance portal](#).
- 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 will not 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, datasets, 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 dataset refresh from such files, is supported, with the exception of 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 will not be updated.
 - When the .pbix file has had a new sensitivity label applied that the dataset owner doesn't have usage rights to. In this case, refresh will fail. Neither report content nor label will be updated.
 - If the dataset 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

- 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.
- To open a protected .pbix file, a user must 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.

- If the label applied to a .pbix file hasn't been published to the user in the Purview compliance portal, the user won't be able to save the file in Desktop.
- 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** doesn't support sensitivity labels. In Desktop, if you export a file that has a sensitivity label to PDF, the PDF won't receive the label and no protection will be applied.
- If you overwrite a labeled dataset or report in the service with an unlabeled .pbix file, the labels in the service will be retained.

Next steps

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](#)

Enable sensitivity labels in Power BI

Article • 12/08/2022 • 4 minutes to read

In order for [sensitivity labels](#) from Microsoft Purview Information Protection to be used in Power BI, they must be enabled on the tenant. This article shows Power BI admins how to do this. For an overview about sensitivity labels in Power BI, see [Sensitivity labels in Power BI](#). For information about applying sensitivity labels in Power BI, see [Applying sensitivity labels](#)

When sensitivity labels are enabled:

- Specified users and security groups in the organization can classify and [apply sensitivity labels](#) to their Power BI content. In the Power BI service, this means their reports, dashboards, datasets, and dataflows. In Power BI Desktop, it means their .pbix files.
- In the service, all members of the organization will be able to see those labels. In Desktop, only members of the organization who have the labels published to them will be able to 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 Power BI'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 in Power BI. 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 them to be used in Power BI. [Learn more about migrating sensitivity labels.](#)

- To be able to apply labels to Power BI content and files, 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 on the tenant before they can be used in both the service and in Desktop. This section describes how to enable them in the tenant settings.

To enable sensitivity labels on the tenant, go to the [Power BI Admin portal](#), open the [Tenant settings](#) pane, and find the [Information protection](#) section.

The screenshot shows the Power BI Admin portal interface. On the left, there's a sidebar with various navigation options like Usage metrics, Users, Audit logs, Capacity settings, and Workspaces. The 'Tenant settings' option is highlighted with a red box. In the main content area, under 'Information protection', there's a list of settings. One item, 'Allow users to apply sensitivity labels for Power BI content', is also highlighted with a red box. A tooltip for this setting says 'Enabled for the entire organization'. To the right of the main content, there's a vertical menu with options like 'Manage personal storage', 'View content pack', 'Admin portal' (which is also highlighted with a red box), 'Manage gateways', 'Settings', and 'Manage embed codes'. The top right corner has a search bar and some icons.

In the **Information Protection** section, perform the following steps:

1. Open **Allow users to apply sensitivity labels for Power BI content**.
2. Enable the toggle.
3. Define who can apply and change sensitivity labels in Power BI assets. By default, everyone in your organization will be able to apply sensitivity labels. However, you can choose to enable setting sensitivity labels only for specific users or security groups. With either the entire organization or specific security groups selected, you can exclude specific subsets of users or security groups.
 - When sensitivity labels are enabled for the entire organization, exceptions are typically security groups.
 - When sensitivity labels are enabled only for specific users or security groups, exceptions are typically specific users.This approach makes it possible to prevent certain users from applying sensitivity labels in Power BI, even if they belong to a group that has permissions to do so.
4. Press **Apply**.

Information protection

1

- Allow users to apply sensitivity labels for Power BI content

With this setting enabled, Microsoft Information Protection sensitivity labels published to users by your organization can be applied in Power BI. All [prerequisite steps](#) must be completed before enabling this setting.

Note: Sensitivity label settings, such as encryption and content marking for files and emails, are not applied to content within Power BI. [Learn more](#)

Visit the [M365 Compliance Center](#) to view sensitivity label settings for your organization.

Note: Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files, that are controlled by "Export to Excel" and "Export reports as PowerPoint presentation or PDF documents" settings. All other export and sharing options do not support the application of sensitivity labels and protection.

2



Enabled

3

The setting below determines which users in the organization can apply and change sensitivity labels. All other users in the organization can only view the labels.

Apply to:

- The entire organization
- Specific security groups

Enter security groups

Except specific security groups

4

Apply

Cancel

Important

Only Power BI Pro users who have *create* and *edit* permissions on the asset, and who are part of the relevant security group that was set in this section, will be able to set and edit the sensitivity labels. Users who are not part of this group won't be able to set or edit the label.

Troubleshooting

Power BI uses sensitivity labels from 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 Power BI.
- 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 Power BI, see [Sensitivity labels in Power BI](#).

Next steps

This article described how to enable sensitivity labels in Power BI. The following articles provide more details about data protection in Power BI.

- [Overview of 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](#)

How to apply sensitivity labels in Power BI

Article • 11/24/2022 • 5 minutes to read

Sensitivity labels from Microsoft Purview Information Protection on your reports, dashboards, datasets, 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 about sensitivity labels in Power BI, see [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!

Apply sensitivity labels in the Power BI service

In the Power BI service, you can apply sensitivity labels to reports, dashboards, datasets, and dataflows.

Requirements needed 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 wish to label.
- Sensitivity labels must be enabled for your organization. Contact your Power BI admin if you aren't sure about this.
- 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 have been met.

When data protection is enabled on your tenant, sensitivity labels appear in the sensitivity column in the list view of dashboards, reports, datasets, and dataflows.

The screenshot shows the Power BI 'My workspace' interface. On the left is a sidebar with various icons. The main area displays three items under the 'Content' tab:

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity
Sales and Marketing Sample	Dashboard	Megan Bowen	—	—	—	General ⓘ
Sales and Marketing Sample	Report	Megan Bowen	5/27/21, 10:59:15 AM	—	—	Confidential for Finance ⓘ
Sales and Marketing Sample	Dataset	Megan Bowen	5/27/21, 10:59:15 AM	N/A	—	Highly Confidential Pr... ⓘ

To apply or change a sensitivity label on a report or dashboard:

1. Go to **Settings**.
2. In the settings side pane, go to the Sensitivity label section and select the appropriate sensitivity label.
3. Save the settings.

The following image illustrates these steps on a report

Sensitivity label

Classify the sensitivity of this report content. [Learn more](#)

Confidential for Finance

ⓘ Some sensitivity label settings, such as file encryption settings and content marking, are not enforced in Power BI. [Learn more](#)

Apply this label to the report's downstream content (preview) [Learn more](#)

[See the downstream items in lineage view](#) ↗

ⓘ Note

If the label is greyed out, you might not have the correct usage rights to change the label. If you need to change a sensitivity label and can't, either ask the person

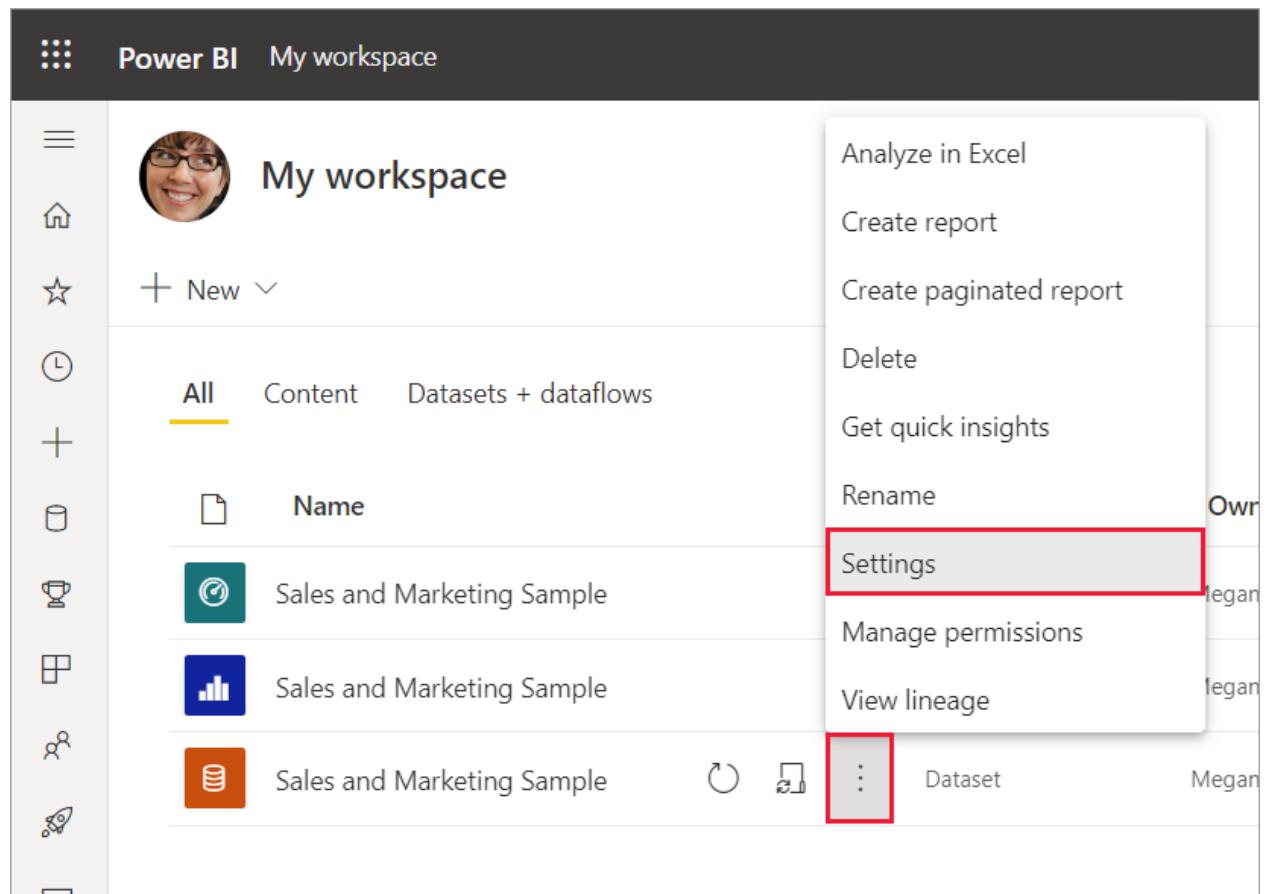
who applied the label in the first place to modify it, or contact the Microsoft 365/Office security administrator and request the necessary **usage rights** for the label.

To apply or change a sensitivity label on a dataset or dataflow:

1. Go to **Settings**.
2. Select the datasets or dataflows tab, whichever is relevant.
3. Expand the sensitivity labels section and choose the appropriate sensitivity label.
4. Apply the settings.

The following two images illustrate these steps on a dataset.

Select **More options (...)** and then **Settings**.



On the settings datasets tab, open the sensitivity label section, choose the desired sensitivity label, and select **Apply**.

▲ Sensitivity label

Classify the sensitivity of this dataset [Learn more](#)

Confidential for Finance ▼

ⓘ Some sensitivity label settings, such as file encryption settings and content marking, are not enforced in Power BI. [Learn more](#)

Apply this label to the dataset's downstream content (preview) [Learn more](#)
[See the downstream items in lineage view](#) ↗

Apply Discard

ⓘ Note

If the label is greyed out, you might not have the correct **usage rights** to change the label. If you need to change a sensitivity label and can't, either ask the person who applied the label in the first place to modify it, or contact the Microsoft 365/Office security administrator and request the necessary **usage rights** for the label.

Apply sensitivity labels in Power BI Desktop

To use 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 if you aren't sure about this.
- 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 have been met.
- You must be signed in.

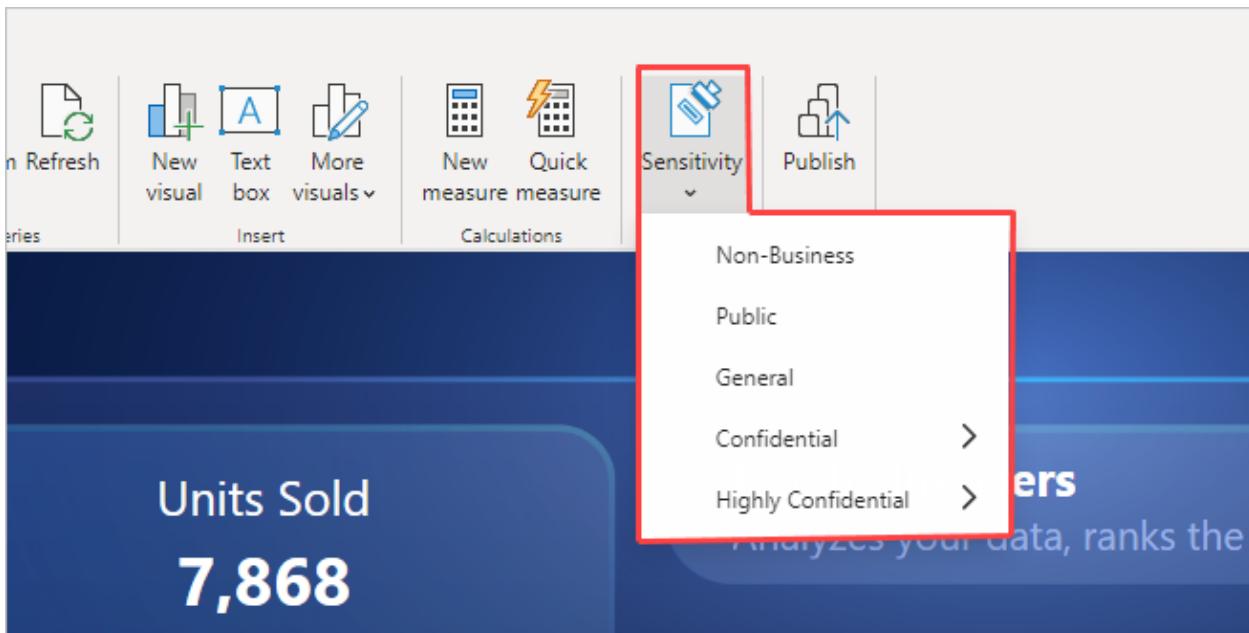
Watch a short video on applying sensitivity labels and then try it out yourself.

ⓘ Note

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

<https://www.microsoft.com/en-us/videoplayer/embed/RE4M5Gj?postJsIMsg=true> ↗

To apply a sensitivity label on the file you're working on, select the sensitivity button in the home tab and choose the desired label from the menu that appears.

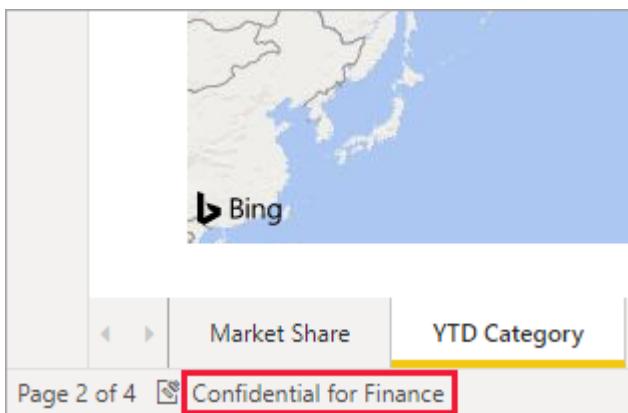


ⓘ Note

If the sensitivity button is greyed out, it might indicate that you don't have an appropriate license or that you don't belong to a security group that has permissions to apply sensitivity labels, as described in [Enable sensitivity labels in Power BI](#).

If a particular label you wish to change is greyed out, you might not have the correct [usage rights](#) to change that label. If you need to change a sensitivity label and can't, either ask the person who applied the label in the first place to modify it, or contact the Microsoft 365/Office security administrator and request the necessary [usage rights](#) for the label.

After you've applied the label, it will be visible in the status bar.



Sensitivity labels when uploading or downloading .pbix files to/from the service

- When you publish a .pbix file to the Power BI service from Desktop, or when you upload a .pbix file to the Power BI service directly using [Get data](#), the .pbix file's label is applied to both the report and the dataset that are created in the service. If the .pbix file you're publishing or uploading replaces existing assets (that is, that have the same name as the .pbix file), a dialog will prompt you to choose whether to keep the labels on those assets or to have the .pbix file's label overwrite those labels. If the .pbix file is unlabeled, the labels in the service will be retained.
- When you download a .pbix file from the Power BI service using [Download this file](#), if the report and dataset being downloaded both have labels, and those labels are different, the label that will be applied to the .pbix file is the more restrictive of the two.

Remove sensitivity labels

You can remove sensitivity labels in both the service and in Desktop.

Service

To remove a sensitivity label from a report, dashboard, dataset, or dataflow, follow the [same procedure used for applying labels in the Power BI service](#), but choose **(None)** when prompted to classify the sensitivity of the data.

Desktop

To remove a sensitivity label from a .pbix file, reselect the label in the sensitivity drop-down menu.

Considerations and limitations

For the list of sensitivity label limitations in Power BI, 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](#)

Default label policy for Power BI

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

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.

This article describes how to enable a default label policy, both in the [Microsoft Purview compliance portal](#) and by using the [Security & Compliance PowerShell setLabelPolicy API](#).

 **Note**

The default label policy settings for Power BI are independent of the default label policy settings for files and email.

What happens when a default label policy is in effect?

- In Power BI Desktop, when a user to whom the policy applies opens a new .pbix file or an existing unlabeled .pbix file, the default label will be applied to the file. If the user is working offline, the label is applied when the user signs in.
- In the Power BI service, when a user to whom the policy applies creates a new dataset, report, dashboard, dataflow or scorecard, the default label will be applied to that item.

Enabling a default label policy for Power BI

A Microsoft 365 administrator can enable a default label policy for Power BI by selecting the desired label in the **Apply this default label to Power BI content** dropdown menu in the policy settings for Power BI in the [Microsoft Purview compliance portal](#). For more information, see [What label policies can do](#).

The screenshot shows the 'Create policy' wizard in the Microsoft 365 compliance portal. On the left, a navigation tree has 'Labels to publish' and 'Users and groups' checked, while 'Settings' is selected. Under 'Settings', 'Power BI' is also selected and highlighted with a red box. The main panel title is 'Apply a default label to Power BI content'. It explains that the chosen label will be applied to new Power BI reports, dashboards, and datasets, noting that users can change it if needed. A dropdown menu titled 'Apply this default label to Power BI content' is shown, with options 'None' (selected), 'None', and 'General', all enclosed in a red box.

For existing policies, it's also possible to enable default label policies for Power BI using the [Security & Compliance PowerShell setLabelPolicy API](#).

The screenshot shows a PowerShell window with the command:

```
Set-LabelPolicy -Identity "<default label policy name>" -AdvancedSettings @{"powerbidefaultlabelid=<LabelId>"}
```

Where:

- `<default label policy name>` is the name of the policy whose associated sensitivity label you want to be applied by default to unlabeled content in Power BI.

ⓘ Important

If a user has more than one label policy, the default label setting is always taken from the policy with the highest priority, make sure to configure the default label on that policy.

Requirements for using PowerShell

- The Exchange Online PowerShell V2 (EXO V2) module. For more information, see [About the Exchange Online PowerShell V2 module](#)
- A connection to the Microsoft Purview compliance portal. For more information, see [Connect to Security & Compliance PowerShell](#)

Documentation

- [Admin Guide: Custom configurations for the Azure Information Protection unified labeling client](#)
- [Create and configure sensitivity labels and their policies](#)
- [Set-LabelPolicy documentation](#)

Considerations and limitations

- Default labeling in Power BI covers most common scenarios, but there may be some less common flows that still allow users to open or create unlabeled .pbix files or Power BI artifacts.
- Default label policy settings for Power BI are independent of the default label policy settings for files and email.
- Default labeling in Power BI isn't supported for service principals and APIs. Service principals and APIs aren't subject to default label policies.
- Default label policies in Power BI aren't supported for [external guest users \(Azure AD B2B\)](#). When a B2B user opens or creates an unlabeled .pbix file in Power BI Desktop or Power BI artifact in the Power BI service, no default label is applied automatically.

Next steps

- [Mandatory label policy for Power BI](#)
- [Sensitivity labels in Power BI](#)
- [Data protection metrics report](#)
- [Audit schema for sensitivity labels in Power BI](#)

Mandatory label policy for Power BI

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

To help ensure comprehensive protection and governance of sensitive data, you can require your organization's Power BI users to apply sensitivity labels to content they create or edit in Power BI. You do this by enabling, in their sensitivity label policies, a special setting for mandatory labeling in Power BI. This article describes the user actions that are affected by a mandatory labeling policy, and explains how to enable a mandatory labeling policy for Power BI.

ⓘ Note

The mandatory label policy setting for Power BI is independent of the mandatory label policy setting for files and email.

Mandatory labeling in Power BI isn't supported for service principals and APIs. Service principals and APIs aren't subject to mandatory label policies.

What happens when a mandatory label policy is in effect?

In the Power BI service:

- Users must apply a sensitivity label before they can save new reports, dashboards, or datasets.
- Users must apply a sensitivity label before they can save changes to the settings or content of existing, unlabeled reports and dashboards.
- If users try to import data from an unlabeled .pbix file, a prompt requires them to select a label before the import can continue. The label they select is applied to the resulting dataset and report in the service. **It is not applied to the .pbix file itself.**

In Power BI Desktop:

- Users must apply sensitivity labels to unlabeled .pbix files before they can save or publish to the service.

Enabling a mandatory label policy for Power BI

A Microsoft 365 administrator can enable a mandatory label policy for Power BI by selecting the **Require users to apply a label to their Power BI content** checkbox in the [Microsoft Purview compliance portal](#). For more information, see [What label policies can do](#).

The screenshot shows the 'Create policy' wizard in the Microsoft Purview compliance portal. The left sidebar shows steps: 'Labels to publish' (checked), 'Users and groups' (checked), 'Settings' (highlighted with a red box), 'Name' (unchecked), and 'Finish' (unchecked). The main area is titled 'Policy settings' with the sub-instruction 'Configure settings for the labels included in this policy.' It lists several checkboxes:

- Users must provide a justification to remove a label or lower its classification**: Users will need to provide a justification before removing a label or replacing it with a one that has a lower-order number. You can use activity explorer to review label changes and justification text.
- Require users to apply a label to their emails and documents**: Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).
Support and behavior for this setting varies across apps and platforms. [Learn more](#)
- Require users to apply a label to their Power BI content**: Users will be required to apply labels to unlabeled content they create or edit in Power BI. [Learn more about mandatory labeling in Power BI](#)
- Provide users with a link to a custom help page**: If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. [Learn more about this help page](#)

If you have an existing policy, and you want to enable mandatory labeling in Power BI, you can use the [Security & Compliance PowerShell setLabelPolicy API](#).

PowerShell

```
Set-LabelPolicy -Identity "<policy name>" -AdvancedSettings @{"powerbimandatory=true"}
```

Where:

- `<policy name>` is the name of the policy where you want to set labeling in Power BI as mandatory.

Requirements for using PowerShell

- You need the Exchange Online PowerShell (EXO) module to run this command. For more information, see [About the Exchange Online PowerShell module](#).
- A connection to the Purview compliance portal is also required. For more information, see [Connect to Security & Compliance PowerShell using the EXO module](#).

Documentation

- [Admin Guide: Custom configurations for the Azure Information Protection unified labeling client](#)
- [Create and configure sensitivity labels and their policies](#)

- [Set-LabelPolicy documentation](#)

Considerations and limitations

- Mandatory labeling in Power BI covers most common scenarios, but there may be some less common flows that still allow a user to create or edit unlabeled content.
- The mandatory label policy setting for Power BI is independent of the mandatory label policy setting for files and email.
- Mandatory labeling in Power BI isn't supported for service principals and APIs. Service principals and APIs aren't subject to mandatory label policies.
- Mandatory labeling in Power BI isn't supported for [external guest users \(B2B users\)](#). B2B users aren't subject to mandatory label policies.

Next steps

- [Default label policy for Power BI](#)
- [Sensitivity labels in Power BI](#)
- [Data protection metrics report](#)
- [Audit schema for sensitivity labels in Power BI](#)

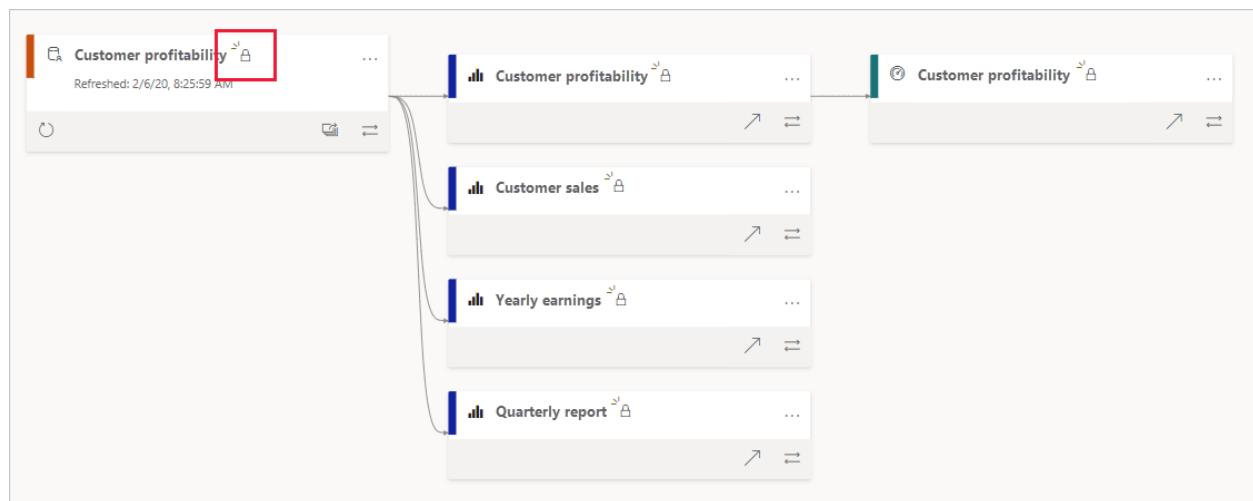
Sensitivity label downstream inheritance

Article • 12/05/2022 • 3 minutes to read

When a sensitivity label is applied to a dataset or report in the Power BI service, it's possible to have the label trickle down and be applied to content that's built from that dataset or report. For datasets, this means other datasets, reports, and dashboards. For reports, this means dashboards. 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.

Downstream inheritance is illustrated below using [lineage view](#). When a label is applied to the dataset "Customer profitability", that label filters down and gets applied to the dataset's downstream content – the reports that are built using that dataset, and, in this case, a dashboard that's built from visuals from one of those reports.



ⓘ Important

- Downstream inheritance never overwrites labels that were applied manually.
- Downstream inheritance never overwrites a label with a less restrictive label.

Downstream inheritance modes

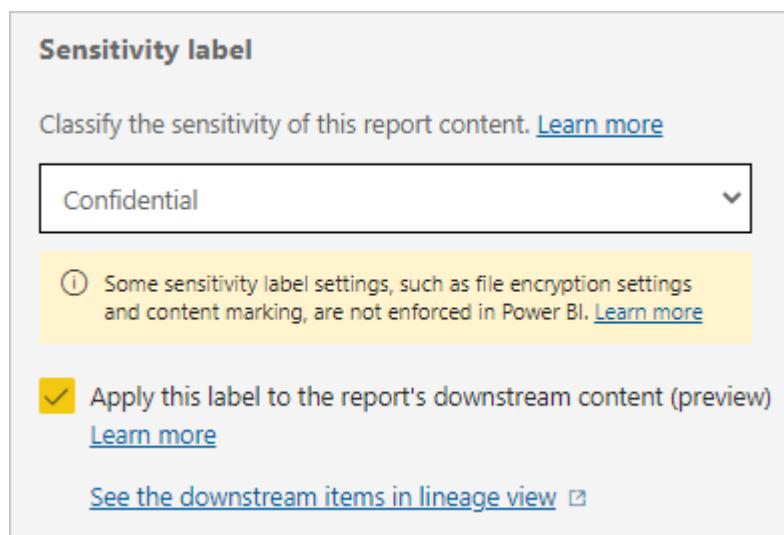
Downstream inheritance operates in one of two modes. The Power BI admin decides via a [tenant setting](#) which mode is operable on the tenant.

- **Downstream inheritance with user consent** (default): In this mode, when users apply sensitivity labels on datasets or reports, they can choose whether to also apply that label downstream. They make their choice by selecting the box that appears with the sensitivity label selector.
- **Fully automated downstream inheritance** (when enabled by a Power BI admin): In this mode, downstream inheritance happens automatically whenever a label is applied to a dataset or report. There's no checkbox provided for user consent.

The two downstream inheritance modes are explained in more detail in the following sections.

Downstream inheritance with user consent

In user consent mode, when a user applies a sensitivity label to a dataset or report, they can choose whether to apply the label to its downstream content as well. A checkbox appears along with the label selector:



By default, the checkbox is selected. This means that when the user applies a sensitivity label to a dataset or report, the label will filter down to its downstream content. For each downstream item, the label will be applied only if:

- The user who applied or changed the label has Power BI edit permissions on the downstream item (that is, the user is an admin, member, or contributor in the workspace where the downstream item is located).
- The user who applied or changed the label is **authorized** to change the sensitivity label that already exists on the downstream item.

Clearing the checkbox prevents the label from being inherited downstream.

Fully automated downstream inheritance

In fully automated mode, a label applied to either a dataset or report will automatically be propagated and applied to the dataset or report's downstream content, without regard to edit permissions on the downstream item and the [usage rights](#) on the label.

Relaxed label change enforcement

In certain cases, downstream inheritance (like other automated labeling scenarios) can result in a situation where no user has all the required permissions needed to change a label. For such situations, label change enforcement relaxations are in place to guarantee access to affected items. See [Relaxations to accommodate automatic labeling scenarios](#) for detail.

Enabling fully automated downstream inheritance

By default, downstream inheritance operates in user consent mode. To switch downstream inheritance in the tenant to fully automated mode, the Power BI admin must enable the **Automatically apply sensitivity labels to downstream content** tenant setting in the admin portal.

Information protection

- ▶ Allow users to apply sensitivity labels for Power BI content
Enabled for the entire organization
- ▶ Require users to apply sensitivity labels to Power BI content (preview)
Disabled for the entire organization
- ▶ Apply sensitivity labels from data sources to their data in Power BI (preview)
Disabled for the entire organization

- ◀ Automatically apply sensitivity labels to downstream content
Enabled for the entire organization

With this setting enabled, whenever a sensitivity label is changed or applied to Power BI content, the label will also be applied to its eligible downstream content. [Learn more](#)



Apply to:

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

Considerations and limitations

- Downstream inheritance is limited to 80 items. If the number of downstream items exceeds 80, no downstream inheritance takes place. Only the item the label was actually applied to will receive the label.
- Downstream inheritance never overwrites manually applied labels.
- Downstream inheritance never replaces a label on downstream content with a label that's less restrictive than the currently applied label.
- [Sensitivity labels inherited from data sources](#) are automatically propagated downstream only when fully automated downstream inheritance mode is enabled.

Next steps

- [Sensitivity label overview](#)
- [Label change enforcement](#)

Sensitivity label inheritance from data sources (preview)

Article • 12/15/2022 • 2 minutes to read

Power BI datasets that connect to sensitivity-labeled data in supported data sources can inherit those labels, so that the data remains classified and secure when brought into Power BI.

Currently supported data sources:

- Excel*
- Azure Synapse Analytics (formerly SQL Data Warehouse)
- Azure SQL Database

*Inheritance from Excel files stored behind a gateway isn't supported. See the [considerations and limitations](#) for more detail.

To be operative, [sensitivity label inheritance from data sources must be enabled on the tenant](#).

Requirements

- The data in the data source must be labeled with sensitivity labels from Microsoft Purview Information Protection.

For Azure Synapse Analytics and Azure SQL Database, this is accomplished using a two-step Purview flow:

1. [Automatically apply sensitivity labels to your data.](#)
 2. [Classify your Azure SQL data using Azure Purview labels.](#)
- The scope of the labels must be [Files and emails](#) and [Azure Purview assets](#). See [Extending sensitivity labels to Azure Purview](#) and [Creating new sensitivity labels or modifying existing labels](#).
 - [Sensitivity labels must be enabled in Power BI](#).
 - All conditions for applying a label must be met.
 - The [Apply sensitivity labels from data sources to their data in Power BI \(preview\)](#) tenant admin setting must be enabled. **Note:** This requirement applies to the Power BI service only. In Desktop, a .pbix file will inherit the label from the data

source even if the tenant admin setting is off. However, after publishing to the service, upon refresh, changes to the label in the data source will only be inherited by the report and dataset if the setting is enabled.

Inheritance behavior

- In the Power BI service, when the dataset is connected to the data source, Power BI inherits the label and applies it automatically to the dataset. Subsequently, inheritance occurs upon dataset refresh. In Power BI Desktop, when you connect to the data source via **Get data**, Power BI inherits the label and automatically applies it to the *.pbix* file (both the dataset and report). Subsequently inheritance occurs upon refresh.
- If the data source has sensitivity labels of different degrees, the most restrictive is chosen for inheritance. In order to be applied, that label (the most restrictive) must be published for the dataset owner.
- Labels from data sources never overwrite manually applied labels.
- Less restrictive labels from the data source never overwrite more restrictive labels on the dataset.
- In Desktop, if the incoming label is more restrictive than the label that is currently applied in Desktop, a banner will appear that recommends to the user to apply the more restrictive label.
- Dataset refresh will succeed even if for some reason the label from the data source isn't applied.

Note

No inheritance takes place if the dataset owner is not authorized to apply sensitivity labels in Power BI, or if the specific label in question has not been published for the dataset owner.

Considerations and limitations

- Inheritance from data sources is supported only for datasets with enhanced metadata. See [Using enhanced dataset metadata](#) for more information.
- Inheritance from data sources is supported only for datasets using the Import data connectivity mode. Live connection and DirectQuery connectivity isn't supported.
- Inheritance from data sources isn't supported in connections via gateways or Azure Virtual Network (VNet). This means that inheritance from an Excel file located on a local machine won't work, because this requires a gateway.

Next steps

- [Enable sensitivity label inheritance from data sources](#)
- [Sensitivity label overview](#)

Sensitivity label change enforcement

Article • 08/29/2022 • 2 minutes to read

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**.

Admin portal

Usage metrics

Users

Premium Per User

Audit logs

Tenant settings

Capacity settings

Refresh summary

Embed Codes

Organizational visuals

Azure connections (preview)

Workspaces

Custom branding

Protection metrics

Featured content

Information protection

- ▶ Allow users to apply sensitivity labels for Power BI content
Enabled for the entire organization
- ▶ Apply sensitivity labels from data sources to their data in Power BI
Disabled for the entire organization
- ◀ Allow workspace admins to override automatically applied sensitivity labels
Unapplied changes

With this setting enabled, workspace admins can change or remove sensitivity labels that were applied automatically by Power BI, for example, as a result of label inheritance.
[Learn more](#)

Enabled

Apply **Cancel**

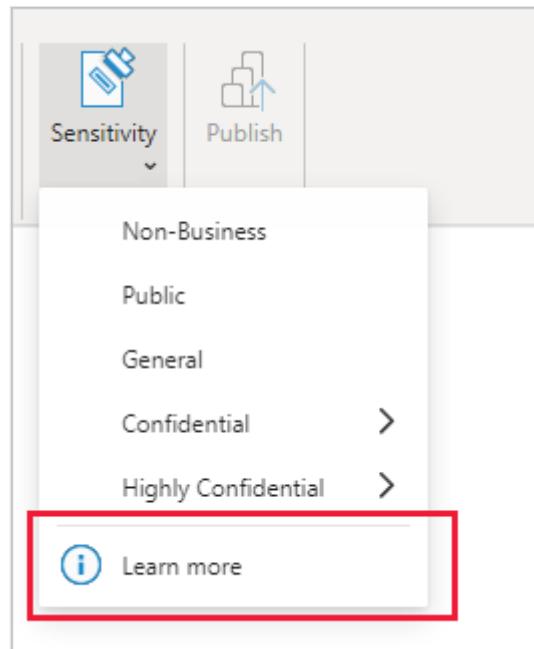
Next steps

- [Sensitivity label overview](#)

Custom help link for sensitivity labels

Article • 12/21/2022 • 2 minutes to read

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](#).

Sensitivity label policy > Create policy

Labels to publish

Users and groups

Settings

Name

Finish

Policy settings

Configure settings for the labels included in this policy.

Users must provide a justification to remove a label or lower its classification
Users will need to provide a justification before removing a label or replacing it with one that has a lower-order number. You can use activity explorer to review label changes and justification text.

Require users to apply a label to their emails and documents
Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).
Support and behavior for this setting varies across apps and platforms. [Learn more about managing sensitivity labels](#)

Require users to apply a label to their Power BI content
Users will be required to apply labels to unlabeled content they create or edit in Power BI. [Learn more about mandatory labeling in Power BI](#)

Provide users with a link to a custom help page
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. [Learn more about this help page](#)

Enter URL to custom help page

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.

Next steps

- [Sensitivity labels in Power BI](#)

Sensitivity label support for paginated reports

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

Sensitivity labels can be applied to paginated reports hosted in the Power BI service. After uploading a paginated report to the service, apply the label to the report just as you would to a [regular Power BI report](#).

When you export data from a labeled paginated report to a supported file type (Excel, PDF, PPTX, and Word), the sensitivity label on the paginated report is applied to the exported file.

Sensitivity labels on paginated reports are included in protection metrics (as part of the Report count), and can be audited (label-change audits only) and modified by public APIs, just like labels on regular Power BI reports.

Considerations and limitations

- [Downstream inheritance](#) isn't supported. The label of an upstream model won't propagate down to its downstream paginated reports. Likewise, the label of a paginated report won't propagate down to the report's downstream content.
- [Mandatory labeling](#) doesn't apply to paginated reports.

Paginated Report visuals

A Paginated Report visual is a special type of visual that you can include in a regular Power BI report. It renders a selected paginated report inside the regular Power BI report.

When a supported file type is exported from a Paginated Report visual that is included in a Power BI report, and the original paginated report being rendered in the visual has a sensitivity label, the exported file inherits the sensitivity label of the original paginated report. If the original paginated report doesn't have a label, the exported file inherits the label of the Power BI report, if it has one.

Next steps

- [Apply sensitivity labels in Power BI](#)
- [Sensitivity label overview](#)

Set or remove sensitivity labels using Power BI REST admin APIs

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

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, you can use Power BI admin REST APIs to programmatically [setLabels](#) and [removeLabels](#) on large numbers of Power BI artifacts.

The APIs set or remove labels from artifacts by artifact ID.

Requirements and considerations

- Users must have administrator rights (such as Microsoft 365 Global Administrator or Power BI Service Administrator) to call these APIs.
- The admin user (and the delegated user, if provided) must have sufficient [usage rights](#) to set or remove labels.
- To set a sensitivity label using the `setLabels` API, the admin user (or the delegated user, if provided) must have the label included in their label policy.
- The APIs allow a maximum of 25 requests per hour. Each request can update up to 2000 artifacts.
- **Required scope:** Tenant.ReadWrite.All

API documentation

- [setLabels](#)
- [removeLabels](#)

Sample

The following sample demonstrates how to set and remove sensitivity labels on Power BI dashboards. Similar code can be used to set and remove labels on datasets, reports, and dataflows.

HTTP

```
const string adminBearerToken = "<adminBearerToken>";
const string ApiUrl = "<api url>";
```

```

        var persistedDashboardId = Guid.Parse("<dashboard object Id>");
        var credentials = new TokenCredentials(adminBearerToken,
"Bearer");

        var artifacts = new InformationProtectionArtifactsChangeLabel();
        artifacts.Dashboards = new List<ArtifactId> { new ArtifactId(id:
persistedDashboardId) };

        using (PowerBIClient client = new PowerBIClient(credentials))
{
    client.BaseUri = new Uri(ApiUrl);

    // Delete labels

    var removeResponse =
client.InformationProtection.RemoveLabelsAsAdmin(artifacts);

    foreach (var updateLabelResult in removeResponse.Dashboards)
{
    if (updateLabelResult.Status == Status.Succeeded)
    {
        Console.WriteLine($"label has been deleted from
artifact {updateLabelResult.Id}");
    }
    else
    {
        Console.WriteLine($"label has not been deleted from
artifact {updateLabelResult.Id}");
    }
}

    // Set labels

    var setLabelRequest = new
InformationProtectionChangeLabelDetails();
    setLabelRequest.Artifacts = artifacts;
    setLabelRequest.LabelId = Guid.Parse("<label Id>");

    // assignmentMethod (optional)
    setLabelRequest.AssignmentMethod =
AssignmentMethod.Privileged;

    // delegatedUser (optional)
    var delegatedUser = new DelegatedUser();
    delegatedUser.EmailAddress = "<delegated user email
address>";

    setLabelRequest.DelegatedUser = delegatedUser;

    var setResponse =
client.InformationProtection.SetLabelsAsAdmin(setLabelRequest);
    foreach (var updateLabelResult in setResponse.Dashboards)
{
    if (updateLabelResult.Status == Status.Succeeded)
    {

```

```
        Console.WriteLine($"label has been upsert on  
artifact {updateLabelResult.Id}");  
    }  
    else  
    {  
        Console.WriteLine($"label has not been upsert on  
artifact {updateLabelResult.Id}");  
    }  
}  
  
}
```

Next steps

- [setLabels API](#)
- [removeLabels API](#)
- [Sensitivity label overview](#)

Audit schema for sensitivity labels in Power BI

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

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.

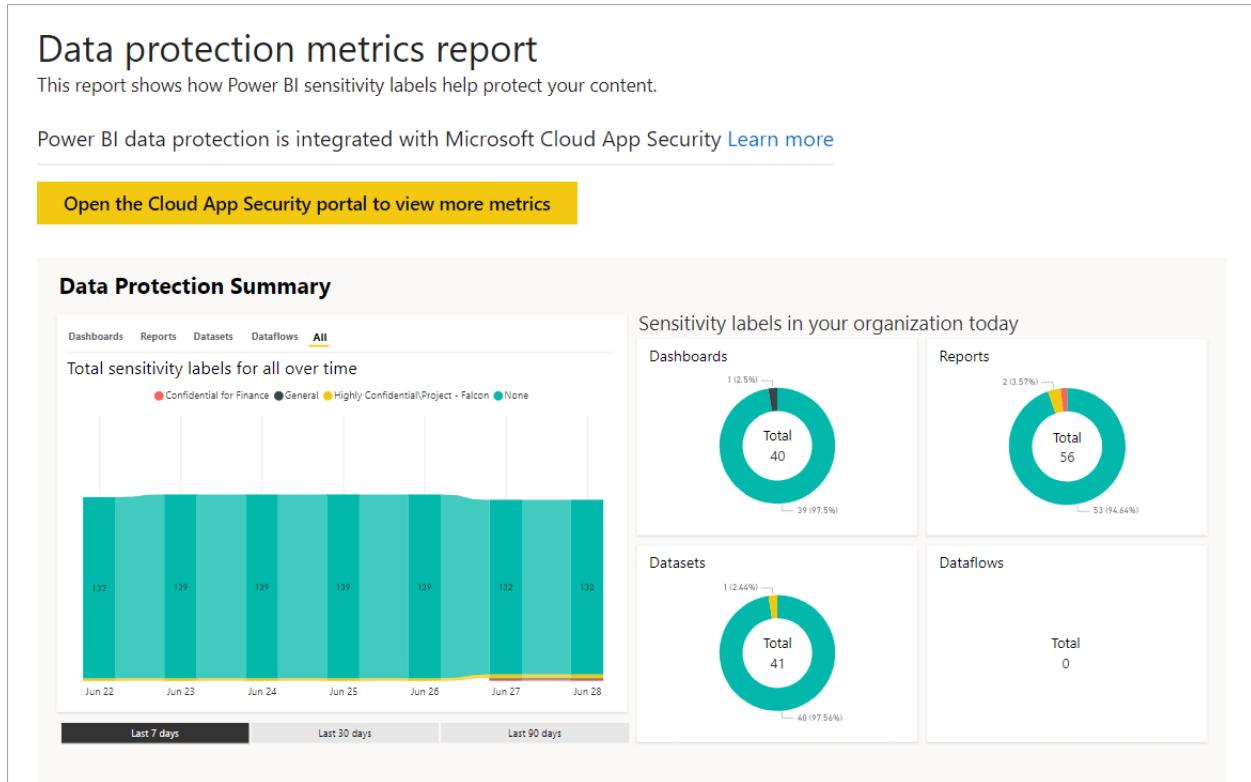
Next steps

- [Sensitivity labels in Power BI](#)
- [Track user activities in Power BI](#)

Data protection metrics report

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

The data protection metrics report is a dedicated report that [Power BI administrators](#) can use to monitor and track sensitivity label usage and adoption in their tenant.



The report features:

- A 100 percent stacked column chart that shows daily sensitivity label usage in the tenant for the last 7, 30, or 90 days. This chart makes it easy to track the relative usage of the different label types over time.
- Donut charts that show the current state of sensitivity label usage in the tenant for dashboards, reports, datasets, and dataflows.
- A link to the Defender for Cloud Apps portal where Power BI alerts, users-at-risk, activity logs, and other information is available. For more information, see [Using Microsoft Defender for Cloud Apps controls in Power BI](#).

The report refreshes every 24 hours.

View the data protection metrics report

You must have a [Power BI administrator role](#) to open and view the report. To view the report, go to **Settings > Admin portal**, and then select **Protection metrics**.

The screenshot shows the Power BI Admin portal interface. On the left is a navigation sidebar with various icons and links. In the center, under the heading 'Admin portal', there are two main sections: 'Help and support settings' and 'Workspace settings'. The 'Help and support settings' section contains several configuration items with status indicators like 'Enabled for the entire organization' or 'Disabled for the entire organization'. The 'Workspace settings' section also contains similar items. At the top right of the central content area, there is a vertical menu with options: 'Manage personal storage', 'View content pack', 'Admin portal' (which is highlighted with a red box), 'Manage gateways', 'Settings', and 'Manage embed codes'. The 'Admin portal' option is specifically highlighted with a red box.

The first time you open the data protection metrics report, it can take a few seconds to load. A report and a dataset entitled **Data protection metrics (automatically generated)** are created in your private environment under **My workspace**. We don't recommend viewing it here because it isn't the full-featured report. Instead, view the report in the Admin portal as described earlier.

✖ Caution

Don't change the report or dataset in any way, because new versions of the report are rolled out from time to time, and any changes you make to the original report are overwritten if you update to the new version.

Report updates

Improved versions of the data protection metrics report are released periodically. When you open the report, if a new version is available, you can open the new version. If you accept the new version, the report loads and then overwrites the old version. Any changes you made to the old report or dataset are lost. If you don't accept the new version, you can't take advantage of the new version's improvements.

Notes and considerations

- In order for the data protection metrics report to be successfully generated, you must enable [sensitivity labels](#) on your tenant, and [sensitivity labels should be applied to reports](#).

- In order to access Defender for Cloud Apps information, your organization must have the appropriate [Defender for Cloud Apps license](#).
- Before you share information from the data protection metrics report with a user who isn't a Power BI administrator, keep in mind that this report contains sensitive information about your organization.
- The data protection metrics report is a special report and doesn't show up in the **Shared with me**, **Recent**, and **Favorites** lists.
- The data protection metrics report isn't available to [external users such as Azure Active Directory B2B \(Azure AD B2B\) guest users](#).

Next steps

- [Sensitivity labels in Power BI](#)
- [Using Microsoft Defender for Cloud Apps controls in Power BI](#)
- [Understanding Power BI administrator roles](#)
- [Enable sensitivity labels in Power BI](#)

Sensitivity labels troubleshooting

Article • 12/12/2022 • 15 minutes to read

Licensing and requirements

What licenses do I need to be able to view and apply sensitivity labels?

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view sensitivity labels from Microsoft Purview Information Protection in Power BI.
- To be able to apply labels to Power BI content and files, 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](#).

What requirements and prerequisites are there for enabling sensitivity labels in my tenant?

- If your organization uses Azure Information Protection sensitivity labels, they need to be migrated to the Microsoft Purview Information Protection Unified Labeling platform in order for them to be used in Power BI. [Learn more about migrating 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 and later.

General problems with sensitivity labels

I can't enable sensitivity labels on my tenant

Power BI 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:

- You don't have an Azure Information Protection license.
- Sensitivity labels haven't been migrated to the Microsoft Purview Information Protection version supported by Power BI.
- No sensitivity labels from Microsoft Purview Information Protection have been defined in the organization.

I can't apply sensitivity labels

To be able to apply or change a sensitivity label, you must

- Have a Power BI Pro or Premium Per User (PPU) license.
- Have create and edit permissions on the item you want to apply the label to.
- Belong to a security group that has permissions to apply sensitivity labels, as described in [Enable sensitivity labels in Power BI](#).

The sensitivity label I want to apply is greyed out

If a particular label you wish to change is greyed out, you may not have the correct [usage rights](#) to change that label. If you need to change a sensitivity label and can't, either ask the person who applied the label in the first place to modify it, or contact the Microsoft 365/Office security administrator and request the necessary usage rights for the label.

The sensitivity button in Desktop is greyed out

If the sensitivity button is greyed out, it may indicate that you don't have an appropriate license or that you don't belong to a security group that has permissions to apply sensitivity labels, as described in [Enable sensitivity labels in Power BI](#).

The sensitivity label doesn't protect an exported file

Sensitivity labels and file encryption protect data only when it leaves Power BI via [supported export paths](#). Data that leaves Power BI via unsupported export paths will not inherit the sensitivity label and will not be encrypted.

To prevent leakage of sensitive data, the Power BI admin can block export from non-supported export paths using Power BI's [export and sharing settings](#).

Miscellaneous problems with sensitivity labels

- Don't use parent labels. A parent label is a label that has sublabels. You cannot 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 will not be inherited.
- Mandatory label policies will not 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 is 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.
- In the Power BI service, if a dataset has a label that has been deleted from the label admin center, you won't 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. In Desktop, if a .pbix file has such an invalid label, you won't be able to save the file.
- Power BI doesn't support sensitivity labels of the [Do Not Forward](#), [user-defined](#), and [HYOK](#) protection types. The Do Not Forward and user-defined protection types refer to labels defined in the [Purview compliance portal](#).
- 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 will not be inherited. See [Sensitivity label inheritance from data sources](#) for detail.

Problems with PBIX files

I can see a report and dataset in the Power BI service, but when I download them to pbix, I get a message that says I don't have sufficient permissions to open the file

In the Power BI service, sensitivity labeling doesn't affect access to content. Access to content in the service is determined solely by the permissions a user has on the content. While the labels are visible in the service, 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 [supported export paths](#).

In Power BI Desktop, sensitivity labels with encryption settings 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.

Can't open protected .pbix file in Desktop

Using sensitivity labels in Desktop requires the Desktop December 2020 release and later. 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.

Protected .pbix files can be only opened by a user who has [Full control and/or Export usage rights](#) for the relevant label. The user that set the label also has Full control and can never be locked out. [See more detail](#)

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).

Can't save a labeled .pbix file in Desktop

If the label applied to a .pbix file hasn't been published to the user in the Microsoft Purview compliance portal, the user won't be able to save the file in Desktop.

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.

Can't publish or get data of a protected .pbix file

"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.

Can't publish or import a .pbix file with a sensitivity label to the service using 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.

Can't upload a protected file to Desktop via Get data

Import of sensitivity-labeled .pbix files (both protected and unprotected) stored on OneDrive or SharePoint Online, as well as on-demand and automatic dataset refresh from such files, is supported, **with the exception of 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 will not be updated.
- When the .pbix file has had a new sensitivity label applied that the dataset owner doesn't have usage rights to. In this case, refresh will fail. Neither report content nor label will be updated.
- If the dataset owner's access token for OneDrive/SharePoint has expired. In this case, refresh will fail. Neither report content nor label will be updated.

Can't open protected .pbix file in Power BI Desktop for Power BI Report Server

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.

Sovereign clouds

Sensitivity labels are supported in the following sovereign clouds:

- [US Government](#): GCC, GCC High, DoD
- China: 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](#).

Sensitivity label support in template apps

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.

Default labeling

No default label is applied to new content I create in the Power BI service.

Default labeling in Power BI covers most common scenarios, but there may be some less common flows that still allow users to open or create unlabeled .pbix files or Power BI artifacts.

Default labeling in Power BI isn't supported for service principals and APIs. Service principals and APIs aren't subject to default label policies.

Default label policies in Power BI aren't supported for [external guest users \(Azure AD B2B\)](#). When a B2B user opens or creates an unlabeled .pbix file in Power BI Desktop or Power BI artifact in the Power BI service, no default label is applied automatically.

The pbix file I created didn't get the default label, even though default labeling is enabled on my tenant

Default labeling in Power BI covers most common scenarios, but there may be some less common flows that still allow users to open or create unlabeled .pbix files or Power BI artifacts.

The default label applied to my Power BI content isn't the same as the label applied to my emails and files

Default label policy settings for Power BI are independent of the default label policy settings for files and email.

B2B users manage to open and create unlabeled .pbix files, even though default labeling is on.

Default label policies in Power BI aren't supported for external guest users (B2B users). When a B2B user opens or creates an unlabeled file in Power BI Desktop, no default label will be applied to the file automatically.

Mandatory labeling

Mandatory labeling for Power BI is enabled but some artifacts are getting created or saved without a label having to be applied.

Mandatory labeling in Power BI isn't supported for service principals and APIs. Service principals and APIs aren't subject to mandatory label policies.

There may be flows that allow the user to create or edit unlabeled content.

Mandatory labeling in Power BI isn't supported for external guest users (B2B users). B2B users aren't subject to mandatory label policies.

Downstream inheritance

Downstream inheritance is enabled, but some or all downstream items don't inherit the label

Downstream inheritance is limited to 80 items. If the number of downstream items exceeds 80, no downstream inheritance takes place. Only the item the label was actually applied to will receive the label.

Downstream inheritance never overwrites labels that were applied manually.

Downstream inheritance never overwrites a label with a less restrictive label.

Sensitivity labels inherited from data sources are automatically propagated downstream only when [fully automated downstream inheritance mode](#) is enabled.

Sensitivity label inheritance from data sources

Sensitivity labels from a data source aren't inherited into Power BI.

- The data in the data source must be labeled with sensitivity labels from Microsoft Purview Information Protection.
- The scope of the labels must be Files and emails and Azure Purview assets. See Extending sensitivity labels to Azure Purview and Creating new sensitivity labels or modifying existing labels.
- Sensitivity labels must be enabled in Power BI.
- The [Apply sensitivity labels from data sources to their data in Power BI \(preview\)](#) tenant admin setting must be enabled.
- All conditions for applying a label must be met.
- Inheritance from data sources isn't supported for datasets located in classic workspaces. My Workspace and V2 workspaces are supported.
- Inheritance from data sources is supported only for datasets with enhanced metadata. See [Using enhanced dataset metadata](#) for more information.
- Inheritance from data sources is supported only for datasets using the Import data connectivity mode. Live connection and DirectQuery connectivity isn't supported.
- Inheritance from data sources isn't supported in connections via gateways or Azure Virtual Network (VNet). This means that inheritance from an Excel file located on a local machine won't work, because this requires a gateway.

Problems setting and removing sensitivity labels using Power BI REST APIs

Can't set or remove sensitivity labels using Power BI REST admin APIs

- Users must have administrator rights (such as Microsoft 365 Global Administrator or Power BI Service Administrator) to call these APIs.
- The admin user (and the delegated user, if provided) must have sufficient [usage rights](#) to set or remove labels.
- To set a sensitivity label using the setLabels API, the admin user (or the delegated user, if provided) must have the label included in their label policy.
- The APIs allow a maximum of 25 requests per hour. Each request can update up to 2000 artifacts.

- Required scope: Tenant.ReadWrite.All

Defender for Cloud Apps

To use Defender for Cloud Apps with Power BI, you must use and configure relevant Microsoft security services, some of which are set outside Power BI. In order to have Defender for Cloud Apps in your tenant, you must have one of the following licenses:

- Defender for Cloud Apps: Provides Defender for Cloud Apps capabilities for all supported apps, part of the EMS E5 and Microsoft 365 E5 suites.
- Office 365 Cloud App Security (a subset of Defender for Cloud Apps): Provides Cloud App Security capabilities only for Office 365, part of the Office 365 E5 suite.

Using Defender for Cloud Apps with Power BI is designed to help secure your organization's content and data, with detections that monitor user sessions and their activities. When using Defender for Cloud Apps with Power BI, there are a few considerations and limitations you should keep in mind:

- Defender for Cloud Apps can only operate on Excel, PowerPoint, and PDF files.
- If you want to use sensitivity labels capabilities in your session policies for Power BI, you need to have an Azure Information Protection Premium P1 or Premium P2 license. Microsoft Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See [Azure Information Protection pricing](#) for detail. In addition, sensitivity labels must have been applied on your Power BI assets.
- Session control is available for any browser on any major platform on any operating system. We recommend using Internet Explorer 11, Microsoft Edge (latest), Google Chrome (latest), Mozilla Firefox (latest), or Apple Safari (latest). Power BI public API calls and other non-browser-based sessions aren't supported as part of Defender for Cloud Apps session control. [See more detail](#).
- If you experience login difficulties, such as having to login more than once, it could be related to the way some apps handle authentication. See [Slow login in the Defender for Cloud Apps documentation](#) for more information and remediation steps.

⊗ Caution

In the session policy, in the "Action" part, the "protect" capability works only if no label exists on the item. If a label already exists, the "protect" action won't apply; you can't override an existing label that has already been applied to an item in Power BI.

Data protection metrics report

I open the data protection metrics page but no report is generated

In order for the data protection metrics report to be successfully generated, [information protection](#) must be enabled on your tenant and [sensitivity labels should have been applied](#).

The data protection metrics report isn't available to [external users such as Azure Active Directory B2B \(Azure AD B2B\) guest users](#).

I can't access the Defender for Cloud Apps information.

In order to access Defender for Cloud Apps information, your organization must have the appropriate [Defender for Cloud Apps license](#).

I don't see the data protection metrics report in Shared with me, Recents, or Favorites

The data protection metrics report is a special report and doesn't show up in the [Shared with me](#), [Recent](#), and [Favorites](#) lists.

I can't share the data protection metrics report with external users

The data protection metrics report isn't available to [external users \(Azure Active Directory B2B guest users\)](#).

Paginated reports

My paginated report doesn't inherit the sensitivity label of the model it's based on.

Downstream inheritance isn't supported. The label of an upstream model won't propagate down to its downstream paginated reports.

The sensitivity label on my paginated report doesn't get applied to the report's downstream content.

The label of a paginated report won't propagate down to the report's downstream content.

I can create and save paginated reports with no sensitivity label even though mandatory labeling is enabled.

Mandatory labeling won't apply to paginated reports.

Data loss prevention policies for Power BI (preview)

Article • 12/29/2022 • 8 minutes to read

To help organizations detect and protect their sensitive data, Power BI supports [Microsoft Purview Data Loss Prevention \(DLP\) policies](#). When a DLP policy for Power BI detects a sensitive dataset, a policy tip can be attached to the dataset in the Power BI service that explains the nature of the sensitive content, and an alert can be registered in the data loss prevention **Alerts** tab in the Microsoft Purview compliance portal for monitoring and management by administrators. In addition, email alerts can be sent to administrators and specified users.

Considerations and limitations

- DLP policies for Power BI are defined in the [Microsoft Purview compliance portal](#).
- DLP policies apply to workspaces. Only workspaces hosted in [Premium Gen2 capacities](#) and [Premium Per User](#) workspaces are supported.
- DLP dataset evaluation workloads impact capacity. See [CPU metering for DLP policy evaluation](#) for more information.
- DLP policy templates aren't yet supported for Power BI DLP policies. When creating a DLP policy for Power BI, choose the "custom policy" option.
- Power BI DLP policy rules currently support sensitivity labels and sensitive info types as conditions.
- DLP policies for Power BI aren't supported for sample datasets, [streaming datasets](#), or datasets that connect to their data source via [DirectQuery](#) or [live connection](#).
- DLP policies for Power BI aren't supported in sovereign clouds.
- Custom sensitive info types of the type *Keyword list* and *Keyword dictionary* are currently not supported when using DLP policies for the Power BI location.
- Currently, DLP policies for Power BI don't support scanning for sensitive info types in data stored in the Southeast Asia region. See [How to find the default region for your organization](#) to learn how to find your organization's default data region.

Licensing and permissions

SKU/subscriptions licensing

Before you get started with DLP for 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

Permissions

Data from DLP for Power BI 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.

- Global administrator
- Compliance administrator
- Security administrator
- Compliance data administrator

CPU metering for DLP policy evaluation

This section is relevant only for workspaces hosted on Premium Gen2 capacities. It doesn't apply to Premium Per User workspaces.

DLP policy evaluation uses CPU from the premium capacity associated with the workspace where the dataset being evaluated is located. CPU consumption of the evaluation is calculated as 30% of the CPU consumed by the action that triggered the evaluation. For example, if a refresh action costs 30 milliseconds of CPU, the DLP scan will cost another 9 milliseconds. This fixed 30% additional CPU consumption for DLP evaluation helps you predict the impact of DLP policies on your overall Capacity CPU utilization, and perform capacity planning when rolling out DLP policies in your organization.

Use the Power BI Premium Capacity Metrics App to monitor the CPU usage of your DLP policies. For more information, see [Use the Gen2 metrics app](#).

Note

As mentioned, metering of DLP evaluation to calculate CPU consumption applies only to workspaces hosted on Premium Gen2 capacities. DLP evaluation in Premium Per User workspaces is included in the PPU license.

How do DLP policies for Power BI work

You define a DLP policy in the data loss prevention section of the compliance 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 dataset that contains sensitive data of the kind you specified. DLP policies for Power BI support two 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 compliance portal.

When a dataset is evaluated by DLP policies, if it matches the conditions specified in a DLP policy, the actions specified in the policy occur. A dataset is evaluated against DLP policies whenever one of the following events occurs:

- Publish
- Republish
- On-demand refresh
- Scheduled refresh

ⓘ Note

DLP evaluation of the dataset does not occur if either of the following is true:

- The initiator of the event is a service principal.
- The dataset owner is either a service principal or a B2B user.

What happens when a dataset is flagged by a Power BI DLP policy

When a DLP policy detects an issue with a dataset:

- If "user notification" is enabled in the policy, the dataset will be marked in the Power BI service with a shield that indicates that a DLP policy has detected an issue with the dataset.

The screenshot shows the Microsoft Power BI interface. At the top, there's a general dataset named "General" with a message: "Your organization has identified policy issues with this dataset. Open it to take a look." Below it is a dataset named "Quarterly Sales" and another named "NowFunctionTest". On the right side of the main area, there are icons for shield, refresh, and dataset, followed by the word "Dataset". At the bottom right, there's a "Report" button.

Open the dataset details page to see a policy tip that explains the policy violation and how the detected type of sensitive information should be handled.

This screenshot shows the "Dataset details" page for the "Quarterly Sales" dataset. At the top, there's a toolbar with various options like File, Refresh, Share, Create a report, Analyze in Excel, Lineage, Chat in Teams, and Show tables. A red box highlights a yellow banner at the top stating "Rule match: 'Confidential by users permissions' label applied to the dataset." To the right of the banner is a "Hide" button. Below the banner, the dataset details are listed: Workspace (Customers West), Refreshed (11/21/21, 11:04:27 AM), Sensitivity (Public), Description (Add a description), and a link to Add a description.

⚠ Note

If you hide the policy tip, it doesn't get deleted. It will appear the next time you visit the page.

- If alerts are enabled in the policy, an alert will be recorded on the data loss prevention **Alerts** tab in the compliance portal, and (if configured) an email will be sent to administrators and/or specified users. The following image shows the **Alerts** tab in the data loss prevention section of the compliance portal.

This screenshot shows the Microsoft 365 compliance portal. The left sidebar has a navigation menu with sections like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Trials, Solutions, Catalog, Audit, Content search, Communication compliance, Data loss prevention (which is highlighted with a red box), eDiscovery, Information governance, Information protection, and Insider risk management. The main content area is titled "Data loss prevention" and shows the "Alerts" tab selected. It displays a table of alerts with columns: Alert name, Severity, Status, and Time detected. The table lists several alerts, all of which are active and have been detected between November 8, 2021, and November 25, 2021. The severity levels shown are Medium and Low.

Alert name	Severity	Status	Time detected
DLP-Protected Sensitive data validation	Medium	Active	Nov 25, 2021 6:43 AM
DLP-Public data validation	Low	Active	Nov 25, 2021 6:41 AM
DLP-Flight Numbers	Low	Active	Nov 24, 2021 5:15 PM
DLP-Floating Point Numbers	Low	Active	Nov 24, 2021 5:15 PM
DLP-Protected Sensitive data validation	Medium	Active	Nov 24, 2021 4:12 PM
DLP-Email control	Medium	Active	Nov 24, 2021 4:04 PM
DLP-Protected Sensitive data validation	Medium	Active	Nov 24, 2021 4:04 PM
DLP-Control Credit cards	Medium	Active	Nov 24, 2021 3:46 PM
DLP-Control Credit cards	Medium	Active	Nov 24, 2021 3:45 PM
DLP-Public data validation	Low	Active	Nov 24, 2021 2:12 PM

Configure a DLP policy for Power BI

1. Log into the [Microsoft Purview compliance portal](#).
2. Choose the **Data loss prevention** solution in the navigation pane, select the **Policies** tab, choose **Create policy**.

The screenshot shows the Microsoft Purview compliance portal interface. The left sidebar is titled "Microsoft 365 compliance" and contains the following navigation items:

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies (selected)
- Permissions
- Trials

Solutions section:

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention (selected)
- eDiscovery
- Information governance

The main content area is titled "Data loss prevention". It has tabs: Overview, Policies (selected), Alerts, Endpoint DLP settings, and Activity explorer. Below the tabs is a sub-header: "Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)".

Below the sub-header is a toolbar with "Create policy" (button), "Export", "Refresh", a count of "12 items", and a "Search" input field.

The main table lists 12 DLP policies:

Name	Order	Last modified	Status
Choose WS V2 PPC	0	Nov 21, 2021 6:41 PM	Off
Choose WS V2 PPU	1	Nov 8, 2021 6:09 PM	On
Exclude WS V2 PPC	2	Nov 8, 2021 6:20 PM	On
Exclude WS V2 PPU	3	Nov 8, 2021 6:24 PM	On
Exclude WS V2 Shared	4	Nov 8, 2021 6:28 PM	On
Choose V1 PPC WS	5	Nov 9, 2021 10:29 AM	On
Exclude V1 PPC WS	6	Nov 9, 2021 10:45 AM	On
Password control	7	Dec 7, 2021 3:12 PM	On
email control	8	Nov 23, 2021 9:04 AM	On
Floating points, Flight numbers, Israel ph...	9	Nov 24, 2021 2:12 PM	On

3. Choose the **Custom** category and then the **Custom policy template**.

⚠ Note

No other categories or templates are currently supported.

The screenshot shows the Microsoft 365 compliance 'Create policy' wizard. On the left, a vertical navigation pane lists steps: 'Choose the information to protect' (selected), 'Name your policy', 'Locations to apply the policy', 'Policy settings', 'Test or turn on the policy', and 'Review your settings'. The main area is titled 'Start with a template or create a custom policy'. It includes a search bar ('Search for specific templates') and a dropdown ('All countries or regions'). Below is a table with three columns: 'Categories' (Financial, Medical and health, Privacy, Custom), 'Templates' (Custom policy, highlighted with a red box), and 'Custom policy' (description: 'Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.'). At the bottom are 'Next' and 'Cancel' buttons.

When done, select **Next**.

4. Name the policy and provide a meaningful description.

The screenshot shows the Microsoft 365 compliance 'Create policy' wizard. The left pane shows the 'Name your policy' step is selected. The main area is titled 'Name your DLP policy' with the sub-instruction 'Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.' It has fields for 'Name *' (containing 'Name your policy') and 'Description' (containing 'Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.'). At the bottom are 'Back', 'Next' (highlighted in blue), and 'Cancel' buttons.

When done, select **Next**.

5. Enable Power BI as a location for the DLP policy. **Disable all other locations.**

Currently, DLP policies for Power BI must specify Power BI as the sole location.

The screenshot shows the Microsoft 365 compliance 'Create policy' wizard. On the left, a vertical navigation pane lists steps: 'Choose the information to protect' (done), 'Name your policy' (done), 'Locations to apply the policy' (selected), 'Policy settings' (not done), 'Test or turn on the policy' (not done), and 'Review your settings' (not done). The main area is titled 'Choose locations to apply the policy' and contains a note: 'We'll apply the policy to data that's stored in the locations you choose.' Below this is a table with four columns: Status, Location, Included, and Excluded. The table shows four locations: Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages. All four are currently set to 'Off'. A red box highlights the 'On' toggle switch for 'Power BI', which is set to 'On'. To the right of the table are buttons for 'All' (Choose workspaces) and 'None' (Exclude workspaces). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

By default the policy will apply to all workspaces. Alternatively, you can specify particular workspaces to include in the policy as well as workspaces to exclude from the policy.

➊ Note

DLP actions are supported only for workspaces hosted in Premium Gen2 capacities.

If you select **Choose workspaces** or **Exclude workspaces**, a dialog will allow you to select workspaces to be included (or excluded).

You can search for workspaces by workspace name or by user email address. When you search by a user's email address, that user's My Workspace will be listed as *personalWorkspace - <email address>*, and you can then select it.



Power BI workspaces



Search by workspace name or user email

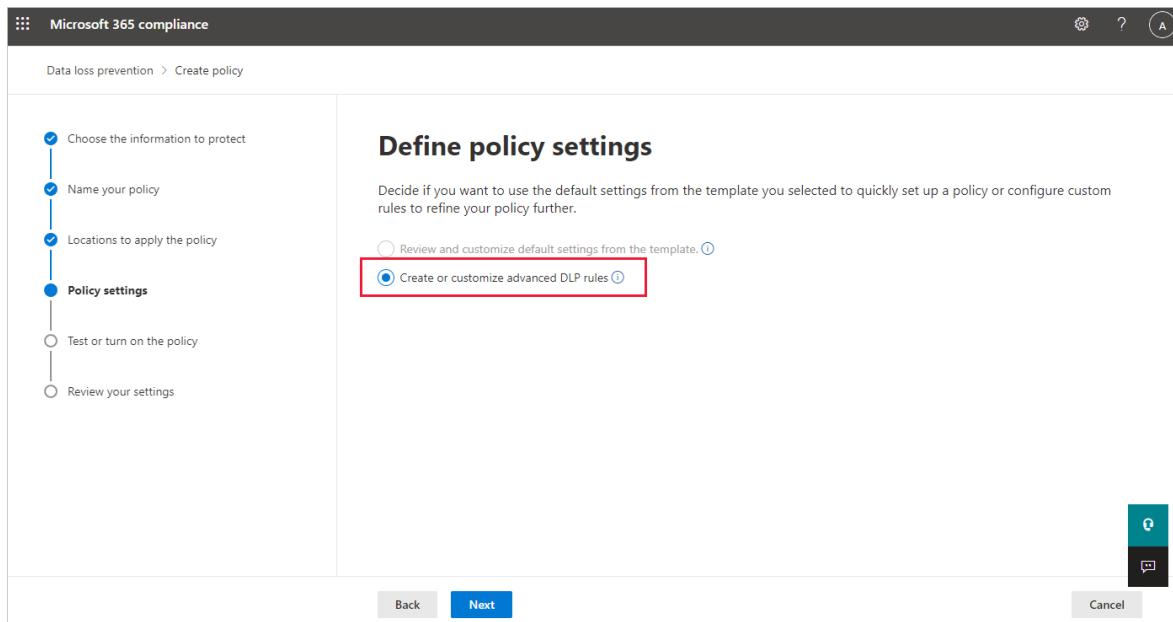
0 items

Done

Cancel

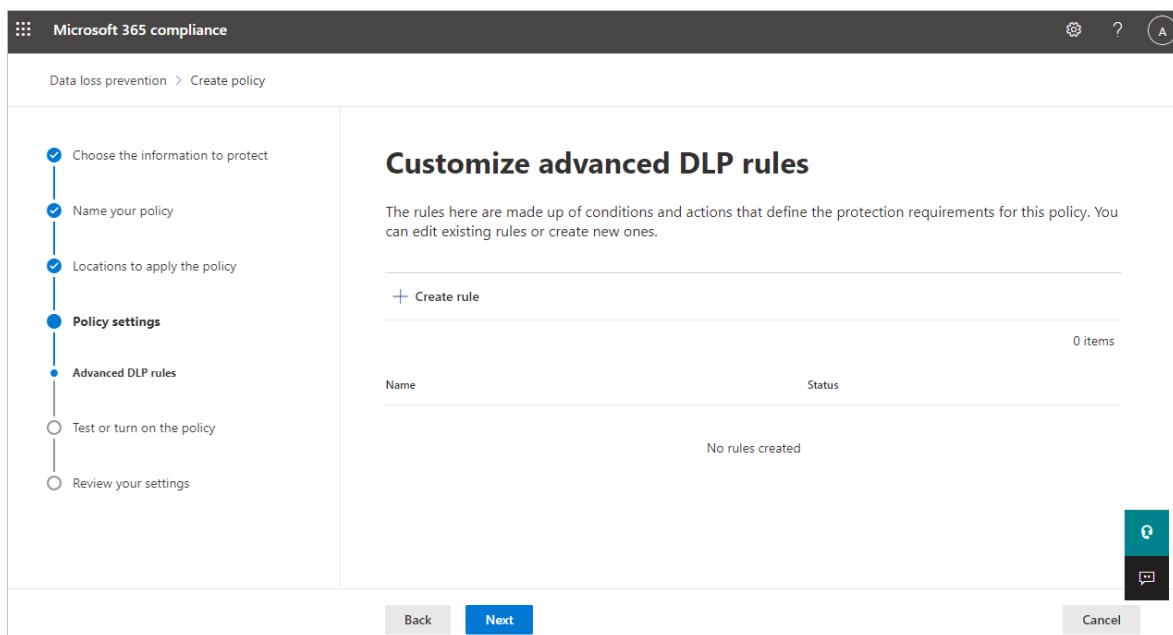
After enabling Power BI as a DLP location for the policy and choosing which workspaces the policy will apply to, select **Next**.

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.

Create rule

Name *

Description

Conditions
Exceptions
Actions
User notifications
User overrides
Incident reports
Additional options

Save **Cancel**

Conditions

In the condition section, you define the conditions under which the policy will apply to a dataset. Conditions are created in groups. Groups make it possible to construct complex conditions.

1. Open the conditions section, choose **Add condition** and then **Content contains**.

Conditions

We'll apply this policy to content that matches these conditions.

+ Add condition

Content contains

Exceptions

This opens the first group (named Default – you can change this).

2. Choose **Add**, and then chose either **Sensitive info types** or **Sensitivity labels**.

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Default	Any of these
Add	
Sensitive info types	
Sensitivity labels	
+ Add condition	

! Note

Currently, DLP policies for Power BI don't support scanning for sensitive info types in data stored in the Southeast Asia region. See [How to find the default region for your organization](#) to learn how to find your organization's default data region.

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.

The screenshot shows two side-by-side lists of sensitive info types and sensitivity labels. Both lists include a search bar at the top and a table with columns for Name and Publisher.

Sensitivity labels:

Name	Publisher
Non-Business	Non-Business
Public	Public
General	General
Confidential	Confidential
<input checked="" type="checkbox"/> Highly Confidential	Highly Confidential

Sensitive info types:

Name	Publisher
U.S. Physical Addresses	Microsoft Corporation
U.K. Unique Taxpayer Reference Number	Microsoft Corporation
U.S. / U.K. Passport Number	Microsoft Corporation
U.S. Bank Account Number	Microsoft Corporation
U.S. Driver's License Number	Microsoft Corporation
U.S. Individual Taxpayer Identification N...	Microsoft Corporation
U.S. Physical Addresses	Microsoft Corporation
<input checked="" type="checkbox"/> U.S. Social Security Number (SSN)	Microsoft Corporation
Ukraine Passport Number (Domestic)	Microsoft Corporation
Ukraine Passport Number (International)	Microsoft Corporation

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.

A screenshot showing the configuration of a condition. It includes a dropdown for 'Medium confidence' with an info icon, and input fields for 'Instance count' set to '1' and 'to Any' with another info icon.

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 datasets 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.

The screenshot shows the 'Content contains' section of a policy configuration. A red box highlights the 'Default' group under 'Sensitivity labels'. Another red box highlights the 'Any of these' dropdown menu. The 'Sensitive info types' section is also visible at the bottom.

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.

The screenshot shows the 'Content contains' section of a policy configuration. A red box highlights the 'OR' dropdown menu. The 'Sensitive info types' section is also visible at the bottom.

Exceptions

If the dataset has a sensitivity label or sensitive info type that matches any of the defined exceptions, the rule won't be applied to the dataset.

Exceptions are configured in the same way as conditions, described above.

Exceptions

We won't apply this rule to content that matches any of these exceptions.

 Add exception 

Actions

Protection actions are currently unavailable for Power BI DLP policies.

Actions

Use actions to protect content when the conditions are met.

 Add an action 

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** and **Policy tips** checkboxes, and write your policy tip in the text box.

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

 On

 Support and behavior for policy tips varies across apps and platforms. [Learn where policy tips are supported](#)

Microsoft 365 services

Notify users in Office 365 service with a policy tip

Policy tips

Customize the policy tip text

Write your policy tip here

User overrides

User overrides are currently unavailable for Power BI DLP policies.

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

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.

[^ Incident reports](#)

Use this severity level in admin alerts and reports:

Select an option ▼

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

[Add or remove users or groups](#)

Send alert every time an activity matches the rule

Send alert when the volume of matched activities reaches a threshold

Instances more than or equal to matched activities

Volume more than or equal to MB

During the last minutes

For [All users](#) ▼

Additional options

[^ Additional options](#)

If there's a match for this rule, stop processing additional DLP policies and rules.

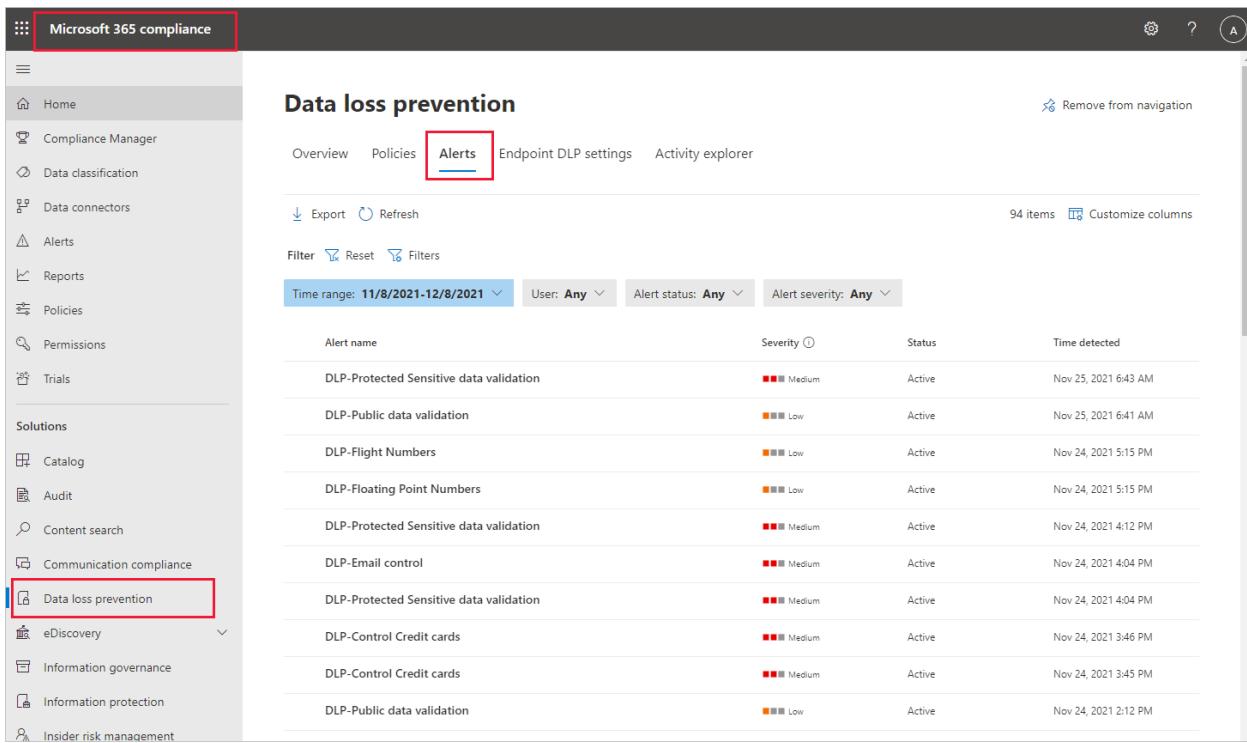
Set the order in which this rule will be selected for evaluation

Priority:

▼

Monitor and manage policy alerts

Log into the [Microsoft Purview compliance portal](#)  and navigate to **Data loss prevention > Alerts**.



The screenshot shows the Microsoft 365 compliance interface. The left sidebar has a 'Data loss prevention' link highlighted with a red box. The main content area is titled 'Data loss prevention' and shows a table of alerts. The 'Alerts' tab is selected at the top. The table columns are 'Alert name', 'Severity', 'Status', and 'Time detected'. The data in the table is as follows:

Alert name	Severity	Status	Time detected
DLP-Protected Sensitive data validation	Medium	Active	Nov 25, 2021 6:43 AM
DLP-Public data validation	Low	Active	Nov 25, 2021 6:41 AM
DLP-Flight Numbers	Low	Active	Nov 24, 2021 5:15 PM
DLP-Floating Point Numbers	Low	Active	Nov 24, 2021 5:15 PM
DLP-Protected Sensitive data validation	Medium	Active	Nov 24, 2021 4:12 PM
DLP-Email control	Medium	Active	Nov 24, 2021 4:04 PM
DLP-Protected Sensitive data validation	Medium	Active	Nov 24, 2021 4:04 PM
DLP-Control Credit cards	Medium	Active	Nov 24, 2021 3:46 PM
DLP-Control Credit cards	Medium	Active	Nov 24, 2021 3:45 PM
DLP-Public data validation	Low	Active	Nov 24, 2021 2:12 PM

Select an alert to start drilling down to its details and to see management options.

Next steps

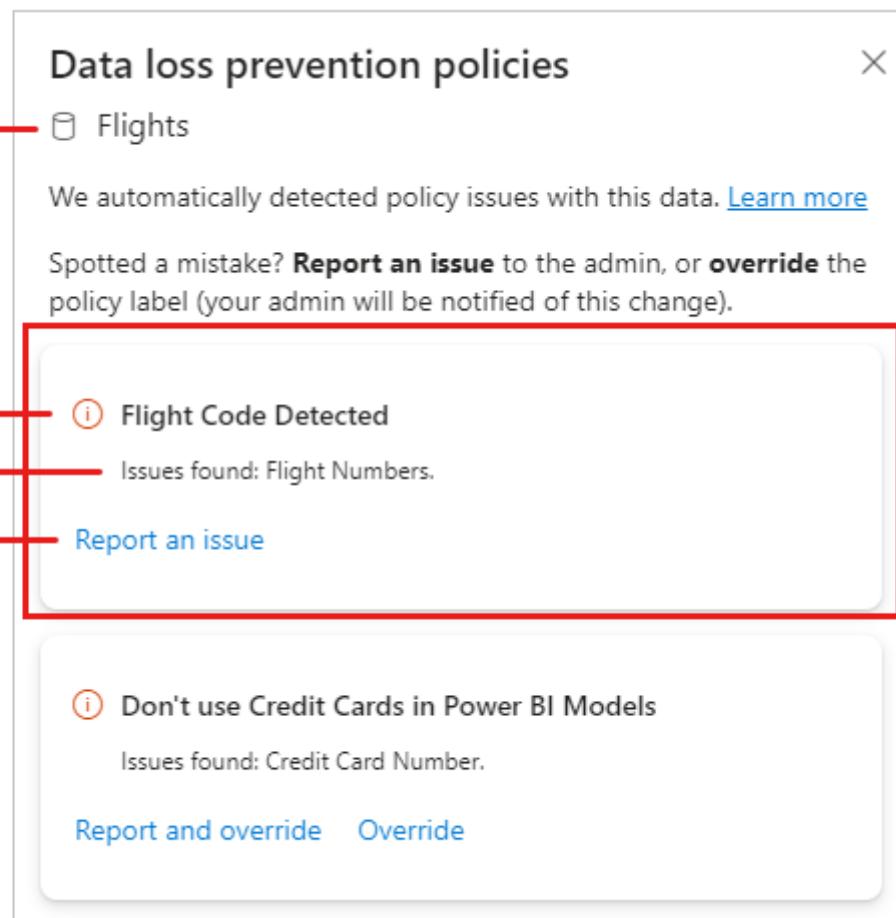
- [Learn about data loss prevention](#)
- [Get started with Data loss prevention policies for Power BI](#)
- [Sensitivity labels in Power BI](#)
- [Audit schema for sensitivity labels in Power BI](#)
- [Power BI implementation planning: Data loss prevention for Power BI](#)

Overriding data loss prevention policies (preview)

Article • 12/29/2022 • 2 minutes to read

The data loss prevention side pane lists all the DLP policy issues detected by a content scan of the dataset.

Each DLP policy issue is shown on a card. The card shows 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.



The action or combination of actions you see may vary depending on the policy configuration. The possible actions are described below.

- **Report an issue:** Report the issue as a false positive (that is, report that the policy has mistakenly identified non-sensitive data as sensitive).
- **Override:** Override the policy. Overriding a policy means that this policy will no longer check this dataset for sensitive data. Depending on the policy configuration, you may 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.

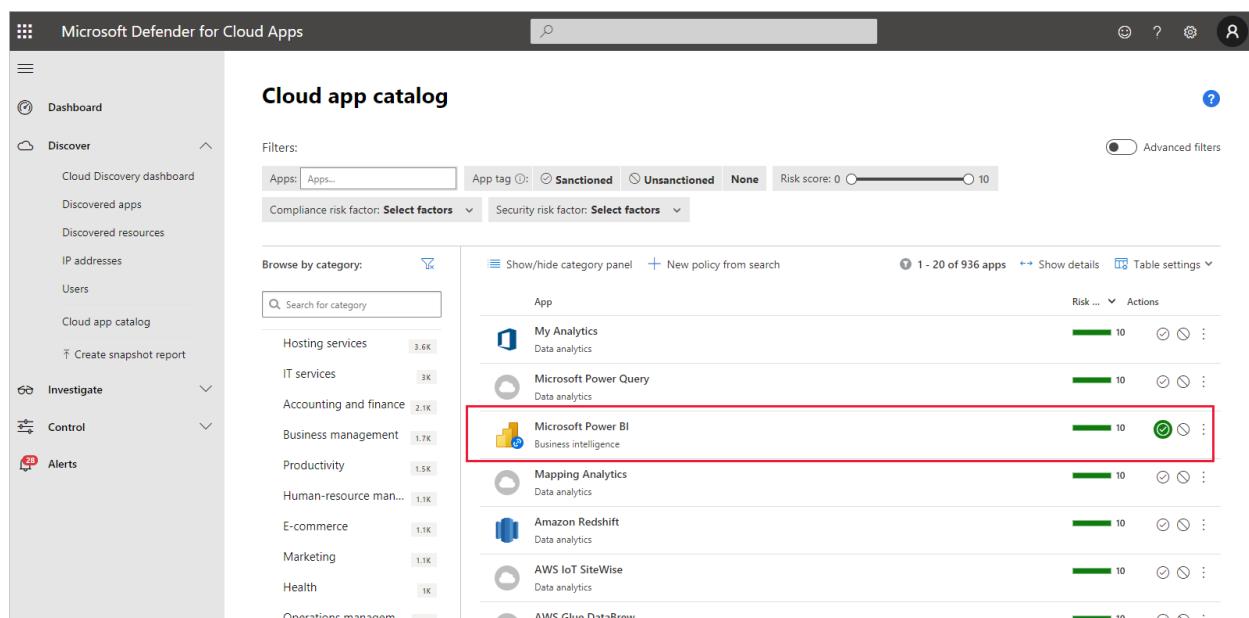
Next steps

- [Learn about data loss prevention](#)
- [Data loss prevention policies for Power BI](#)
- [Get started with Data loss prevention policies for Power BI](#)
- [Sensitivity labels in Power BI](#)
- [Audit schema for sensitivity labels in Power BI](#)
- [Power BI implementation planning: Data loss prevention for Power BI](#)

Using Microsoft Defender for Cloud Apps controls in Power BI

Article • 12/29/2022 • 7 minutes to read

Using Defender for Cloud Apps with Power BI, you can help protect your Power BI reports, data, and services from unintended leaks or breaches. With Defender for Cloud Apps, you can create conditional access policies for your organization's data, using real-time session controls in Azure Active Directory (Azure AD), that help to ensure your Power BI analytics are secure. Once these policies have been set, administrators can monitor user access and activity, perform real-time risk analysis, and set label-specific controls.



The screenshot shows the Microsoft Defender for Cloud Apps interface. On the left is a navigation sidebar with options like Dashboard, Discover, Investigate, Control, and Alerts. The main area is titled 'Cloud app catalog' and displays a list of apps. A search bar at the top allows filtering by app name ('Apps...'), app tag ('Sanctioned', 'Unsanctioned', 'None'), and risk score (0 to 10). Below the search bar are dropdowns for 'Compliance risk factor' and 'Security risk factor'. The app list includes 'My Analytics', 'Microsoft Power Query', 'Microsoft Power BI' (which is highlighted with a red box), 'Mapping Analytics', 'Amazon Redshift', 'AWS IoT SiteWise', and 'AWS Glue DataBrew'. Each app entry shows its category, risk score (10), and three action icons: a green circle, a blue circle, and a grey circle. The 'Microsoft Power BI' row has a red box around it, indicating it is the focus of the example.

You can configure Defender for Cloud Apps for all sorts of apps and services, not only Power BI. You'll need to configure Defender for Cloud Apps to work with Power BI to benefit from Defender for Cloud Apps protections for your Power BI data and analytics. For more information about Defender for Cloud Apps, including an overview of how it works, the dashboard, and app risk scores, see the [Defender for Cloud Apps documentation](#).

Defender for Cloud Apps licensing

To use Defender for Cloud Apps with Power BI, you must use and configure relevant Microsoft security services, some of which are set outside Power BI. In order to have Defender for Cloud Apps in your tenant, you must have one of the following [licenses](#):

- Microsoft Defender for Cloud Apps: Provides Defender for Cloud Apps capabilities for all supported apps, part of the EMS E5 and Microsoft 365 E5 suites.
- Office 365 Cloud App Security: Provides Defender for Cloud Apps capabilities only for Office 365, part of the Office 365 E5 suite.

Configure real-time controls for Power BI with Defender for Cloud Apps

Note

An Azure Active Directory Premium P1 license is required in order to benefit from Defender for Cloud Apps real-time controls.

The sections below describe the steps for configuring real-time controls for Power BI with Defender for Cloud Apps.

Set session policies in Azure AD (required)

The steps necessary to set session controls are completed in the Azure AD and Defender for Cloud Apps portals. In the Azure AD portal, you create a conditional access policy for Power BI, and route sessions used in Power BI through the Defender for Cloud Apps service.

Defender for Cloud Apps operates using a reverse-proxy architecture, and is integrated with Azure AD conditional access to monitor Power BI user activity in real-time. The following steps are provided here to help you understand the process, and detailed step-by-step instructions are provided in the linked content in each of the following steps. You can also read this [Defender for Cloud Apps article](#) that describes the process in whole.

1. [Create an Azure AD conditional access test policy](#)
2. [Sign into each app using a user scoped to the policy](#)
3. [Verify the apps are configured to use access and session controls](#)
4. [Enable the app for use in your organization](#)
5. [Test the deployment](#)

The process for setting session policies is described in detail in the [Session policies](#) article.

Set anomaly detection policies to monitor Power BI activities (recommended)

You can define anomaly Power BI detection policies that can be independently scoped, so that they apply to only the users and groups you want to include and exclude in the policy. [Learn more](#).

Defender for Cloud Apps also has two dedicated, built-in detections for Power BI. [See the section later on in this document for detail](#).

Use sensitivity labels from Microsoft Purview Information Protection (recommended)

Sensitivity labels enable you to classify and help protect sensitive content, so that people in your organization can collaborate with partners outside your organization, yet still be careful and aware of sensitive content and data.

You can read the article on [sensitivity labels in Power BI](#), which goes into detail about the process of using sensitivity labels for Power BI. See below for an [example of a Power BI policy based on sensitivity labels](#).

Custom policies to alert on suspicious user activity in Power BI

Defender for Cloud Apps activity policies enable administrators to define their own custom rules to help detect user behavior that deviates from the norm, and even possibly act upon it automatically, if it seems too dangerous. For example:

- **Massive sensitivity label removal.** For example: alert me when sensitivity labels are removed by a single user from 20 different reports in a time window shorter than 5 minutes.
- **Encrypting sensitivity label downgrade.** For example: alert me when a report that had a 'Highly confidential' sensitivity label is now classified as 'Public'.

Note

The unique identifiers (IDs) of Power BI artifacts and sensitivity labels can be found using [Power BI REST APIs](#). See [Get datasets](#) or [Get reports](#).

Custom activity policies are configured in the Defender for Cloud Apps portal. [Learn more.](#)

Built-in Defender for Cloud Apps detections for Power BI

Defender for Cloud Apps detections enable administrators to monitor specific activities of a monitored app. For Power BI, there are currently two dedicated, built-in Defender for Cloud Apps detections:

- **Suspicious share** – detects when a user shares a sensitive report with an unfamiliar (external to the organization) email. A sensitive report is a report whose sensitivity label is set to **INTERNAL-ONLY** or higher.
- **Mass share of reports** – detects when a user shares a massive number of reports in a single session.

Settings for these detections are configured in the Defender for Cloud Apps portal. [Learn more.](#)

Power BI admin role in Defender for Cloud Apps

A new role is created for Power BI admins when using Defender for Cloud Apps with Power BI. When you log in as a Power BI admin to the [Defender for Cloud Apps portal](#), you have limited access to data, alerts, users at risk, activity logs, and other information relevant to Power BI.

Considerations and limitations

Using Defender for Cloud Apps with Power BI is designed to help secure your organization's content and data, with detections that monitor user sessions and their activities. When using Defender for Cloud Apps with Power BI, there are a few considerations and limitations you should keep in mind:

- Defender for Cloud Apps can only operate on Excel, PowerPoint, and PDF files.
- If you want to use sensitivity labels capabilities in your session policies for Power BI, you need to have an Azure Information Protection Premium P1 or Premium P2 license. Microsoft Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See [Azure Information Protection](#).

[Protection pricing](#) for detail. In addition, sensitivity labels must have been applied on your Power BI assets.

- Session control is available for any browser on any major platform on any operating system. We recommend using Internet Explorer 11, Microsoft Edge (latest), Google Chrome (latest), Mozilla Firefox (latest), or Apple Safari (latest). Power BI public API calls and other non-browser-based sessions aren't supported as part of Defender for Cloud Apps session control. [See more detail](#).
- If you experience login difficulties, such as having to login more than once, it could be related to the way some apps handle authentication. See [Slow login in the Defender for Cloud Apps documentation](#) for more information and remediation steps.

 **Caution**

In the session policy, in the "Action" part, the "protect" capability works only if no label exists on the item. If a label already exists, the "protect" action won't apply; you can't override an existing label that has already been applied to an item in Power BI.

Example

The following example shows you how to create a new session policy using Defender for Cloud Apps with Power BI.

First, create a new session policy. In the **Defender for Cloud Apps** portal, select **Policies** on the navigation pane. Then on the policies page, click **Create policy** and choose **Session policy**.

The screenshot shows the Microsoft Defender for Cloud Apps interface. On the left sidebar, under the 'Control' section, the 'Policies' option is selected and highlighted with a red box. The main content area is titled 'Policies' and contains a navigation bar with tabs: Threat detection, Information protection, Conditional access, Shadow IT, and All policies (which is currently selected). Below the navigation bar are filters for Name, Type, Status (with options ACTIVE, DISABLED, and SCHEDULED), and Severity. A 'Create policy' button and an 'Export' button are also present. A list of policy types is shown, with 'Session policy' highlighted by a red box. A tooltip for the session policy states: 'This policy is automatically enabled to alert you when anomalous behavior is detected in discovered users.' At the bottom of the list, there is a note: 'Malware detection [Disabled]'. The right side of the screen has some descriptive text about user actions and OAuth apps.

In the window that appears, create the session policy. The numbered steps describe settings for the following image.

1. In the **Policy template** drop-down, choose *No template*.
2. For the **Policy name** box, provide a relevant name for your session policy.
3. For **Session control type**, select *Control file download (with inspection)* (for DLP).

For the **Activity source** section, choose relevant blocking policies. We recommend blocking unmanaged and non-compliant devices. Choose to block downloads when the session is in Power BI.

Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template *

Policy name *

Policy severity *



Category *

Description

Block download of highly confidential reports in Power BI

Session control type *

Select the type of control you want to enable:

Activity source

Add activity filters to the policy

Activities matching all of the following

Edit and preview results

Device	▼	Tag	▼	does not equal	▼	Intune compliant, Hybrid Azure AD joined	▼	
App	▼	equals	▼	Microsoft Power BI	▼			

When you scroll down you see more options. The following image shows those options, with additional examples.

4. Create a filter on **Sensitivity label** and choose *Highly confidential* or whatever best fits your organization.
5. Change the **Inspection method** to *none*.
6. Choose the **Block** option that fits your needs.
7. Make sure you create an alert for such an action.

Add file filters to the policy

files matching all of the following

Filters:

Sensitivity label equals Highly confidential

Add a filter

Inspection method

None

Actions

Select an action to be applied when user activity matches the policy.

Test

Monitor login activities

Block

A default block message is displayed when possible

Also notify user by email

Customize block message (i)

Protect

Apply sensitivity label to downloads & monitor all activities

Require step-up authentication PREVIEW (i)

Re-evaluate Azure AD Conditional Access policies based on the authentication context.

Unpublished authentication context will not be enforced

[Configure authentication context](#) (i)

(i) No authentication context configured

Always apply the selected action even if data cannot be scanned (i)

Alerts

Create an alert for each matching event with the policy's severity

[Save as default settings](#) | [Restore default settings](#)

Send alert as email (i)

Send alert as text message (i)

Daily alert limit per policy 5

Send alerts to Power Automate

[Create a playbook in Power Automate](#)

Session control applies to browser-based apps.

To block access from mobile and desktop apps, [create an Access policy](#)

8. Finally, select the **Create** button to create the session policy.



We'd love to hear about your experience

Tell us about your experience (optional). Do not include personally identifiable information as part of this feedback.



It's OK to contact me

admin@EimDataProtection02Dxt.onmicrosoft.com

Submit

It may take several minutes for these changes to take effect.

We secure your data as described in our [privacy statement](#) and [online service terms](#).

Create

Cancel

Next steps

This article described how Defender for Cloud Apps can provide data and content protections for Power BI. You might also be interested in the following articles, which describe Data Protection for Power BI and supporting content for the Azure services that enable it.

- [Overview of sensitivity labels in Power BI](#)
- [Enable sensitivity labels in Power BI](#)
- [How to apply sensitivity labels in Power BI](#)

You might also be interested in the following Azure and security articles:

- [Protect apps with Microsoft Defender for Cloud Apps Conditional Access App Control](#)
- [Deploy Conditional Access App Control for featured apps](#)
- [Session policies](#)
- [Overview of sensitivity labels](#)
- [Data protection metrics report](#)
- [Power BI implementation planning: Defender for Cloud Apps for Power BI](#)

Power BI Security

Article • 12/29/2022 • 4 minutes to read

For detailed information about Power BI security, see the [Power BI Security white paper](#).

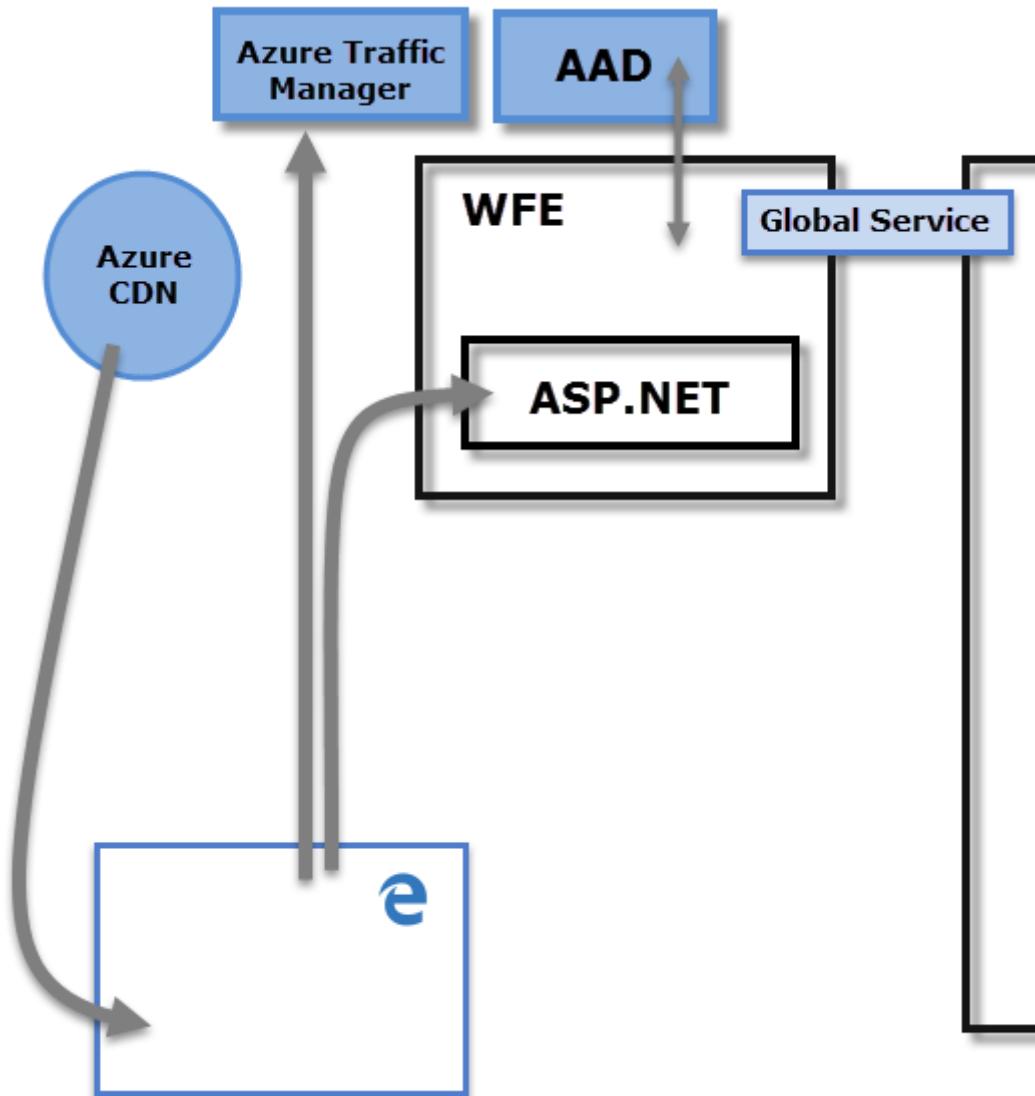
To plan for Power BI security, see the Power BI implementation planning [security series of articles](#). It expands upon the content in the Power BI Security white paper. While the Power BI security white paper focuses on key technical topics such as authentication, data residency, and network isolation, 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:

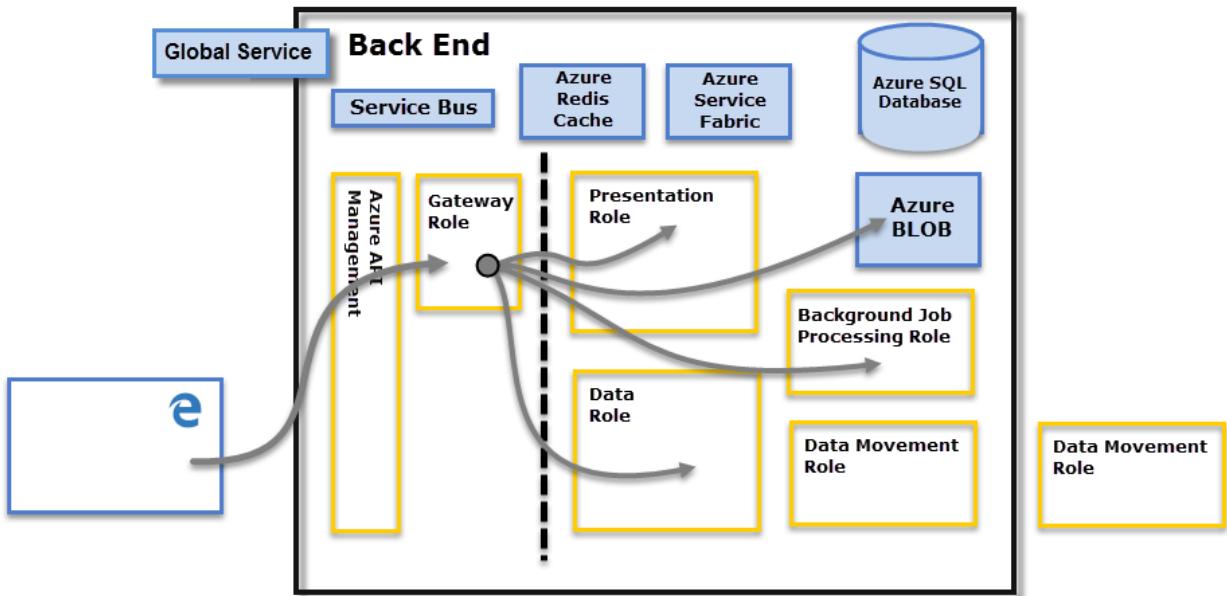
- The **Web Front End (WFE)** cluster. The **WFE** cluster manages the initial connection and authentication to the Power BI service.
- The **Back-End** cluster. Once authenticated, the **Back-End** handles all subsequent user interactions. Power BI uses Azure Active Directory (Azure AD) to store and manage user identities. Azure AD also manages data storage and metadata using Azure BLOB and Azure SQL Database, respectively.

Power BI Architecture

The **WFE** cluster uses Azure AD 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, datasets, 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**.



(i) 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 [Azure Active Directory](#) 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 Azure AD and on-premises credentials requires [directory synchronization](#) to work properly.

Platform security for Power BI also includes multi-tenant environment security, networking security, and the ability to add other Azure AD-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 datasets 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 datasets initiates authentication for each user that attempts to access the report or dataset. 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 respects the registry key settings described in those articles, and only creates connections using the version 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](#).

Row-level security (RLS) with Power BI

Article • 12/29/2022 • 8 minutes to read

Row-level security (RLS) with Power BI can be used to restrict data access for given users. Filters restrict data access at the row level, and you can define filters within roles. In the Power BI service, members of a workspace have access to datasets in the workspace. RLS doesn't restrict this data access.

You can configure RLS for data models imported into Power BI with Power BI Desktop. You can also configure RLS on datasets that are using DirectQuery, such as SQL Server. For Analysis Services or Azure Analysis Services lives connections, you configure Row-level security in the model, not in Power BI Desktop. The security option will not show up for live connection datasets.

Define roles and rules in Power BI Desktop

You can define roles and rules within Power BI Desktop. When you publish to Power BI, you also publish the role definitions.

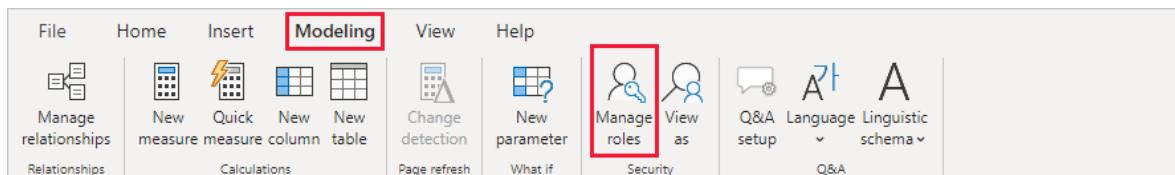
To define security roles:

1. Import data into your Power BI Desktop report, or configure a DirectQuery connection.

ⓘ Note

You can't define roles within Power BI Desktop for Analysis Services live connections. You need to do that within the Analysis Services model.

2. From the **Modeling** tab, select **Manage Roles**.



3. From the **Manage roles** window, select **Create**.

Manage roles

Roles

Tables

Create

Delete

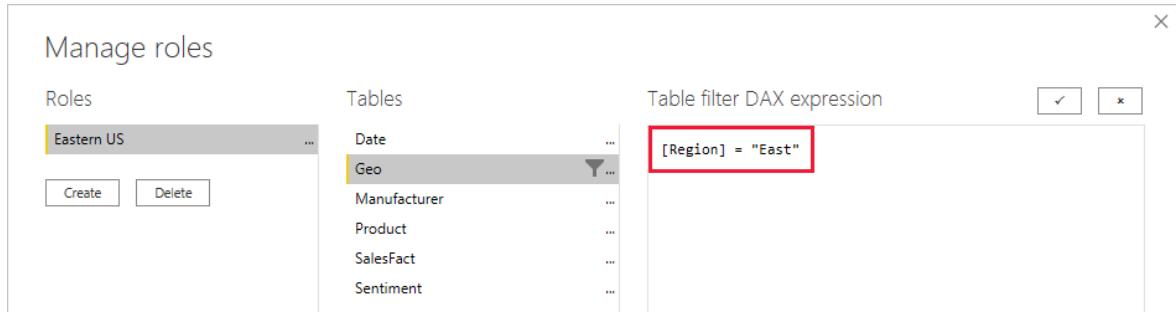
4. Under **Roles**, provide a name for the role.

 Note

You can't define a role with a comma, for example `London,ParisRole`.

5. Under **Tables**, select the table to which you want to apply a DAX (Data Analysis Expression) rule.

6. In the **Table filter DAX expression** box, enter the DAX expressions. This expression returns a value of true or false. For example: `[Entity ID] = "Value"`.



 Note

You can use `username()` within this expression. Be aware that `username()` has the format of `DOMAIN\username` within Power BI Desktop. Within the Power BI service and Power BI Report Server, it's in the format of the user's User Principal Name (UPN). Alternatively, you can use `userprincipalname()`, which always returns the user in the format of their user principal name, `username@contoso.com`.

7. After you've created the DAX expression, select the checkmark above the expression box to validate the expression.



! Note

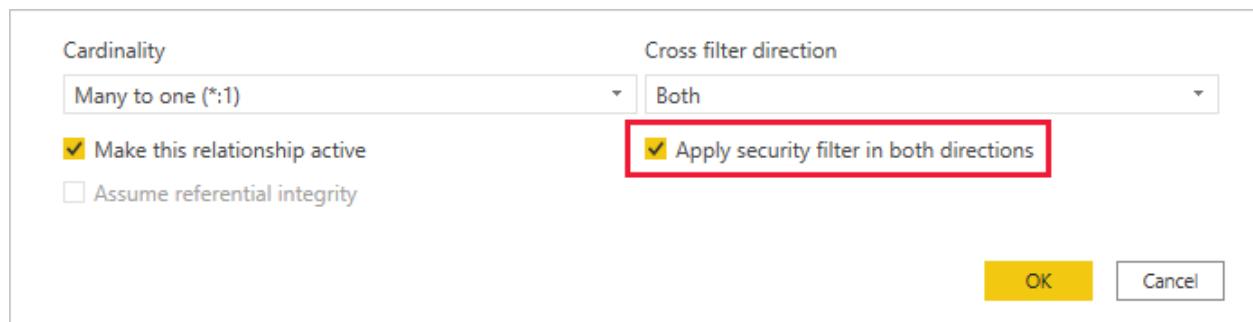
In this expression box, use commas to separate DAX function arguments even if you're using a locale that normally uses semicolon separators (e.g. French or German).

8. Select Save.

You can't assign users to a role within Power BI Desktop. You assign them in the Power BI service. You can enable dynamic security within Power BI Desktop by making use of the `username()` or `userprincipalname()` DAX functions and having the proper relationships configured.

By default, row-level security filtering uses single-directional filters, whether the relationships are set to single direction or bi-directional. You can manually enable bi-directional cross-filtering with row-level security by selecting the relationship and checking the **Apply security filter in both directions** checkbox. Note that if a table takes part in multiple bi-directional relationships you can only select this option for one of those relationships. Select this option when you've also implemented dynamic row-level security at the server level, where row-level security is based on username or login ID.

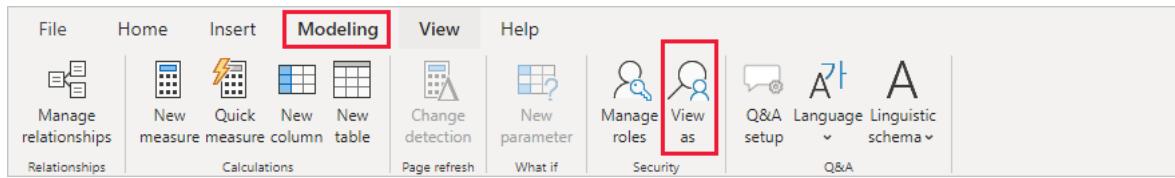
For more information, see [Bidirectional cross-filtering using DirectQuery in Power BI Desktop](#) and the [Securing the Tabular BI Semantic Model](#) technical article.



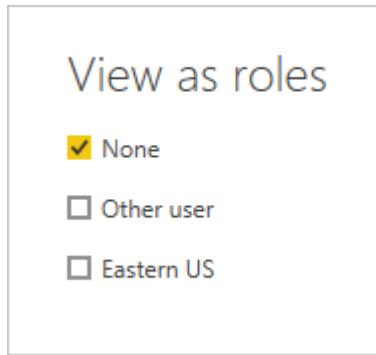
Validate the roles within Power BI Desktop

After you've created your roles, test the results of the roles within Power BI Desktop.

1. From the **Modeling** tab, select **View as**.



The **View as roles** window appears, where you see the roles you've created.



2. Select a role you created. Then choose **OK** to apply that role.

The report renders the data relevant for that role.

3. You can also select **Other user** and supply a given user.



It's best to supply the User Principal Name (UPN) because that's what the Power BI service and Power BI Report Server use.

Within Power BI Desktop, **Other user** displays different results only if you're using dynamic security based on your DAX expressions.

4. Select **OK**.

The report renders based on what the RLS filters allow the user to see.

➊ Note

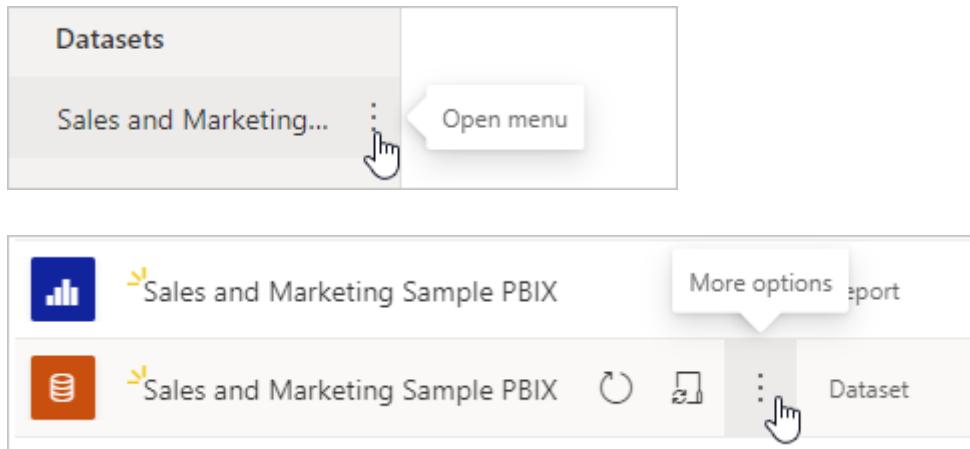
The **View as roles** feature doesn't work for DirectQuery models with Single Sign-On (SSO) enabled.

Now that you're done validating the roles in Power BI Desktop, go ahead and publish your report to the Power BI service.

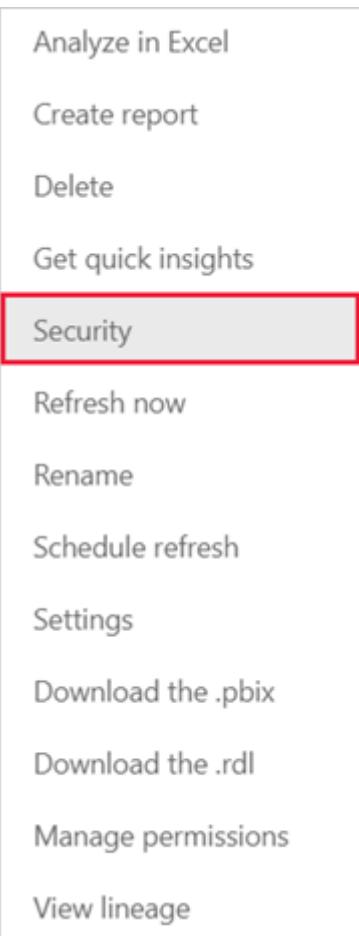
Manage security on your model

To manage security on your data model, open the workspace where you saved your report in the Power BI service and do the following steps:

1. In the Power BI service, select the **More options** menu for a dataset. This menu appears when you hover on a dataset name, whether you select it from the navigation menu or the workspace page.



2. Select **Security**.



Security will take you to the Role-Level Security page where you add members to a role you created in Power BI Desktop. Contributor (and higher workspace roles) will see **Security** and can assign users to a role.

You can only create or modify roles within Power BI Desktop.

Working with members

Add members

In the Power BI service, you can add a member to the role by typing in the email address or name of the user or security group. You can't add Groups created in Power BI. You can add members [external to your organization](#).

You can use the following groups to set up row level security.

- Distribution Group
- Mail-enabled Group
- Security Group

Note, however, that Office 365 groups are not supported and cannot be added to any roles.

Row-Level Security

Eastern US (0)

Members (0)

People or groups who belong to this role

Enter email addresses

Add

You can also see how many members are part of the role by the number in parentheses next to the role name, or next to Members.

Row-Level Security

Eastern US (1)

Members (1)

Remove members

You can remove members by selecting the X next to their name.

Members (1)

People or groups who belong to this role

Enter email addresses

Add

Adele Vance

Validating the role within the Power BI service

You can validate that the role you defined is working correctly in the Power BI service by testing the role.

1. Select **More options (...)** next to the role.
2. Select **Test data as role**.

Row-Level Security

Eastern US (1)

Members (1)

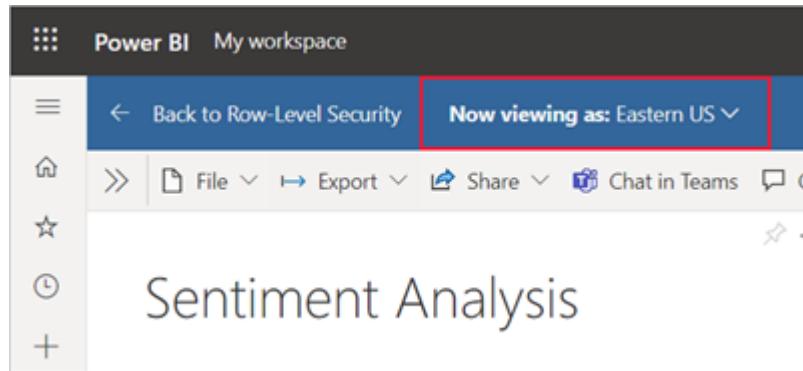
Test as role

People or groups who belong to this role

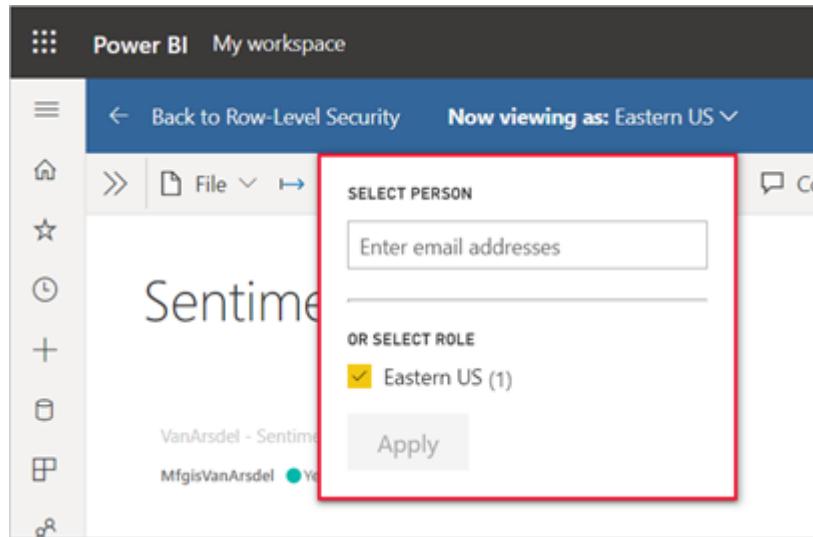
Enter email addresses

You'll be redirected to the report that was published from Power BI Desktop with this dataset, if it exists. Dashboards are not available for testing using the **Test as role** option.

In the page header, the role being applied is shown.



Test other roles, or a combination of roles, by selecting **Now viewing as**.



You can choose to view data as a specific person or you can select a combination of available roles to validate they're working.

To return to normal viewing, select **Back to Row-Level Security**.

ⓘ Note

The Test as role feature doesn't work for DirectQuery models with Single Sign-On (SSO) enabled.

Using the `username()` or `userprincipalname()` DAX function

You can take advantage of the DAX functions `username()` or `userprincipalname()` within your dataset. You can use them within expressions in Power BI Desktop. When you publish your model, it will be used within the Power BI service.

Within Power BI Desktop, `username()` will return a user in the format of `DOMAIN\User` and `userprincipalname()` will return a user in the format of `user@contoso.com`.

Within the Power BI service, `username()` and `userprincipalname()` will both return the user's User Principal Name (UPN). This looks similar to an email address.

Using RLS with workspaces in Power BI

If you publish your Power BI Desktop report to a [workspace](#) in the Power BI service, the RLS roles are applied to members who are assigned to the **Viewer** role in the workspace. Even if **Viewers** are given Build permissions to the dataset, RLS still applies. For example, if Viewers with Build permissions use [Analyze in Excel](#), their view of the data will be protected by RLS. Workspace members assigned **Admin**, **Member**, or **Contributor** have edit permission for the dataset and, therefore, RLS doesn't apply to them. If you want RLS to apply to people in a workspace, you can only assign them the **Viewer** role. Read more about [roles in workspaces](#).

Considerations and limitations

You can see the current limitations for row-level security on cloud models here:

- If you previously defined roles and rules in the Power BI service, you must re-create them in Power BI Desktop.
- You can define RLS only on the datasets created with Power BI Desktop. If you want to enable RLS for datasets created with Excel, you must convert your files into Power BI Desktop (PBIX) files first. [Learn more](#).
- Service principals can't be added to an RLS role. Accordingly, RLS won't be applied for apps using a service principal as the final effective identity.
- Only Import and DirectQuery connections are supported. Live connections to Analysis Services are handled in the on-premises model.
- The Test as role/View as role feature doesn't work for DirectQuery models with single sign-on (SSO) enabled.

FAQ

Question: What if I had previously created roles and rules for a dataset in the Power BI service? Will they still work if I do nothing?

Answer: No, visuals won't render properly. You'll have to re-create the roles and rules within Power BI Desktop and then publish to the Power BI service.

Question: Can I create these roles for Analysis Services data sources?

Answer: Yes, if you imported the data into Power BI Desktop. If you're using a live connection, you can't configure RLS within the Power BI service. This is defined within the Analysis Services model on-premises.

Question: Can I use RLS to limit the columns or measures accessible by my users?

Answer: No, if a user has access to a particular row of data, they can see all the columns of data for that row.

Question: Does RLS let me hide detailed data but give access to data summarized in visuals?

Answer: No, you secure individual rows of data, but users can always see either the details or the summarized data.

Question: My data source already has security roles defined (for example SQL Server roles or SAP BW roles). What's the relationship between these and RLS?

Answer: The answer depends on whether you're importing data or using DirectQuery. If you're importing data into your Power BI dataset, the security roles in your data source aren't used. In this case, you should define RLS to enforce security rules for users who connect in Power BI. If you're using DirectQuery, the security roles in your data source are used. When a user opens a report, Power BI sends a query to the underlying data source, which applies security rules to the data based on the user's credentials.

Next steps

- Restrict data access with row-level security (RLS) for Power BI Desktop
- Row-level security (RLS) guidance in Power BI Desktop
- Power BI implementation planning: Report consumer security planning
- Questions? Try asking the Power BI Community ↗
- Suggestions? Contribute ideas to improve Power BI ↗

Object level security (OLS)

Article • 01/02/2023 • 2 minutes to read

Object-level security (OLS) enables model authors to secure specific tables or columns from report viewers. For example, a column that includes personal data can be restricted so that only certain viewers can see and interact with it. In addition, you can also restrict object names and metadata. This added layer of security prevents users without the appropriate access levels from discovering business critical or sensitive personal information like employee or financial records. For viewers that don't have the required permission, it's as if the secured tables or columns don't exist.

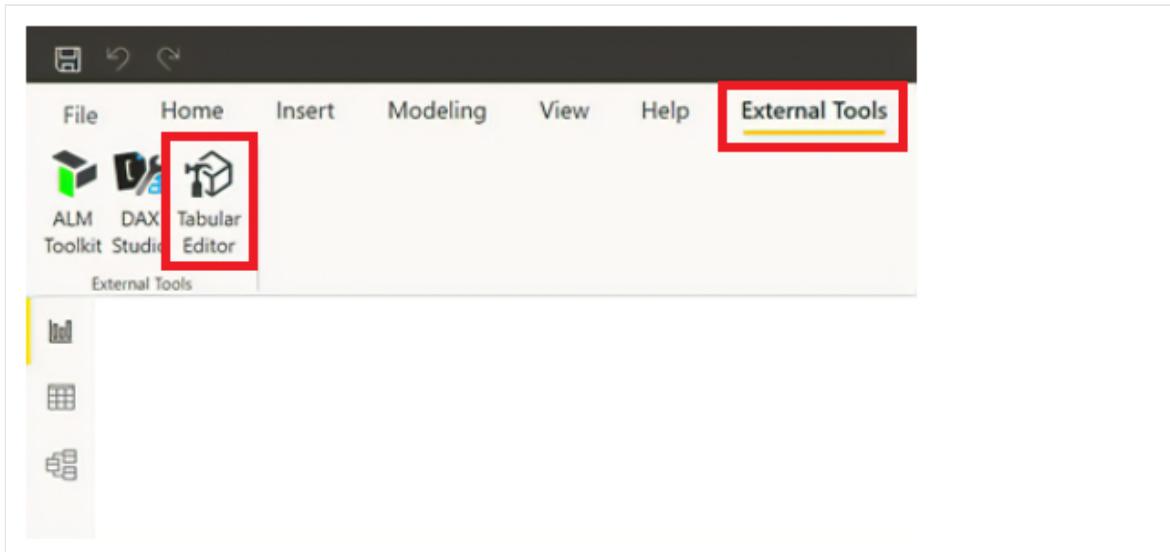
Create a report that uses OLS

Like RLS, OLS is also defined within model roles. Currently, you can't create OLS definitions natively in Power BI Desktop.

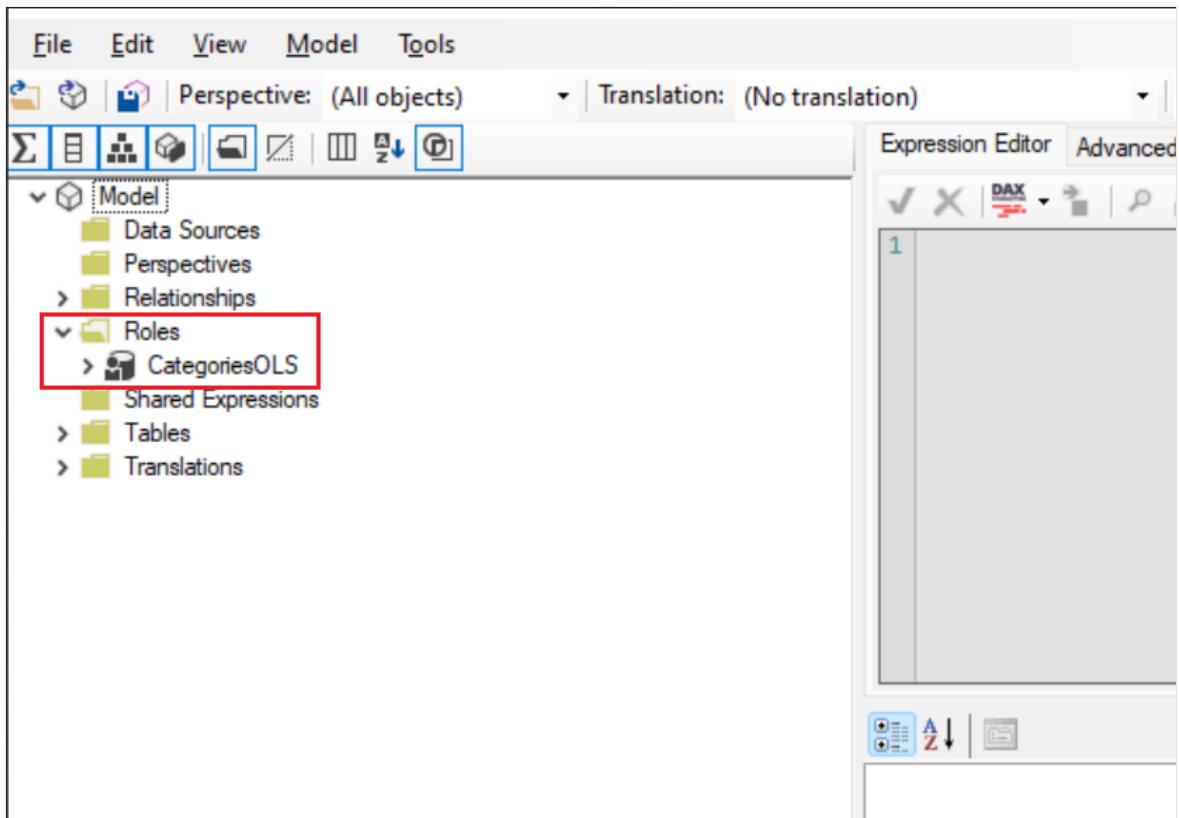
To create roles on **Power BI Desktop** datasets, use [external tools](#) such as [Tabular Editor](#).

Configure object level security using tabular editor

1. In Power BI Desktop, [create the model](#) that will define your OLS rules.
2. On the **External Tools** ribbon, select **Tabular Editor**. If you don't see the Tabular Editor button, install the [program](#). When open, Tabular Editor will automatically connect to your model.



3. In the **Model** view, select the drop-down menu under **Roles**. The roles you created in step one will appear.



4. Select the role you want to enable an OLS definition for, and expand the **Table Permissions**.

Setting	Value
Basic	Description: Finance Name: Finance
Metadata	Annotations: 1 annotation ErrorMessage: 0 extended properties Object Type: Role
Security	Row Level Security: RLS enabled on 0 out of 22 tables Table Permissions: OLS enabled on 3 out of 22 tables
Translations, Perspectives, Security	Members: 0 model role members Model Permission: Read

5. Set the permissions for the table or column to *None* or *Read*.

None: OLS is enforced and the table or column will be hidden from that role

Read: The table or column will be visible to that role

To secure the **whole table**

Set categories under *Table permissions* to *None*.

The screenshot shows the Power BI Model view. On the left, there's a tree view with nodes like 'Basic', 'Metadata', 'Security', 'Table Permissions', and 'Translations, Perspectives, Security'. Under 'Table Permissions', 'Categories' is expanded, showing tables like 'Customers', 'DateTableTemplate...', 'LocalDateTable...', etc., each with a 'Role' column set to 'None'. The 'Translations, Perspectives, Security' node shows 'Members' and 'Model Permission' with 'Read' roles.

6. After you define object-level security for the roles, save your changes.

The screenshot shows the Power BI Model view. The ribbon at the top has 'File', 'Edit', 'View', 'Model' (which is selected), and 'Tools'. The 'Model' tab has a blue save icon highlighted with a red box. The main area shows the model structure with 'Model' selected, containing 'Data Sources', 'Relationships', 'Roles', 'Tables', and 'Translations'. The 'Tables' node contains 'CategoriesOLS'. The right side features an 'Expression Editor' window with a DAX formula bar and a large empty workspace.

7. In Power BI Desktop, publish your dataset to the Power BI Service.

8. In the Power BI Service, navigate to the **Security** page by selecting the **more options** menu on the dataset, and assign members or groups to their appropriate roles.

The OLS rules are now defined. Users without the required permission will receive a message that the field can't be found for all report visuals using that field.

The screenshot shows the Power BI Data Explorer interface. A DAX query is being run:

```
//Run as OLS Test
EVALUATE
SELECTCOLUMNS (
    DimCustomer,
    "Last Name", DimCustomer[LastName],
    "Birth Date", DimCustomer[BirthDate]
)
```

The query runs successfully, as indicated by the message "Run complete". However, there is an error message in the "Messages" pane:

Executing the query
Query (6, 19) Column 'BirthDate' in table 'DimCustomer' cannot be found or may not be used in this expression.

Considerations and limitations

- OLS only applies to *Viewers* in a workspace. Workspace members assigned *Admin*, *Member*, or *Contributor* have edit permission for the dataset and, therefore, OLS doesn't apply to them. Read more about [roles in workspaces](#).
- Datasets with OLS configured for one or more table or column objects aren't supported with these Power BI features:
 - Q&A visualizations
 - Quick insights visualizations
 - Smart narrative visualizations
 - Excel Data Types gallery
- See other OLS restrictions

Next steps

- [Object-level security in Azure Analysis Services](#)
- [Power BI implementation planning: Report consumer security planning](#)
- Questions? [Try asking the Power BI Community](#)
- Suggestions? [Contribute ideas to improve Power BI](#)

Power BI Desktop privacy levels

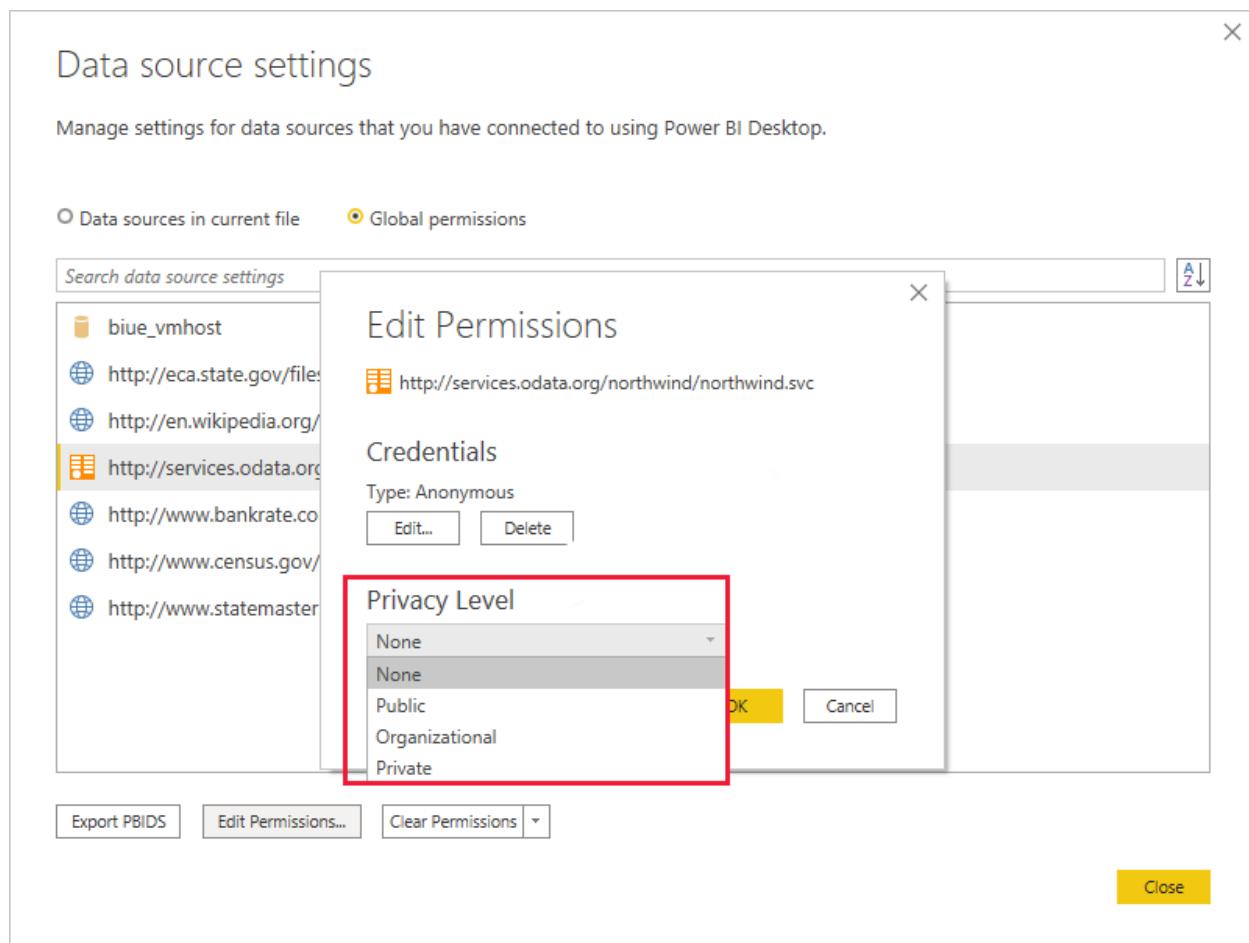
Article • 12/29/2022 • 2 minutes to read

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:

Setting	Description	Example data sources
---------	-------------	----------------------

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.

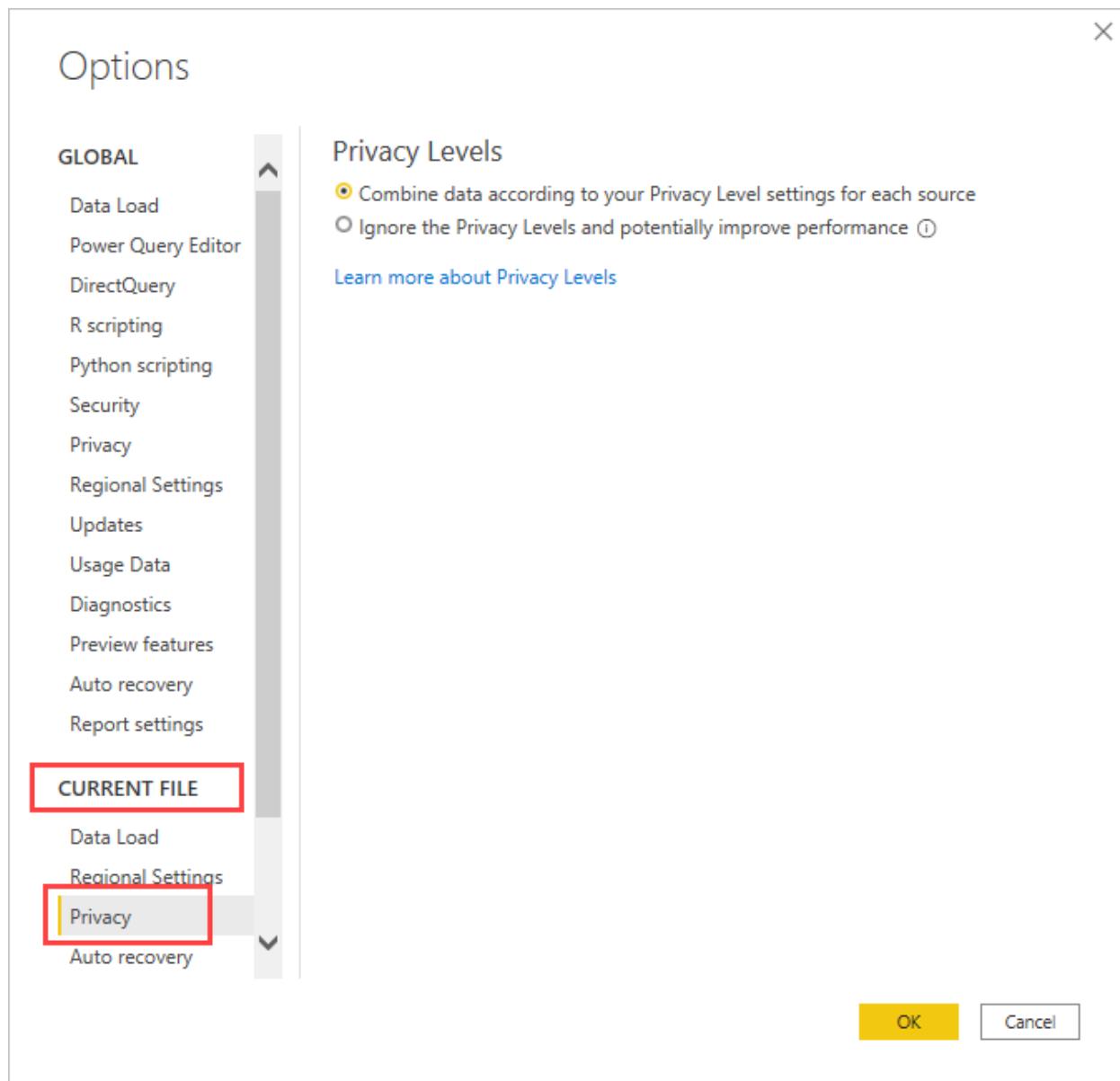
 **Caution**

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:

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.

Next steps

- [Power BI implementation planning: Content creator security planning](#)
- Questions? [Try asking the Power BI Community](#)
- Suggestions? [Contribute ideas to improve Power BI](#)

Using service tags with Power BI

Article • 12/15/2022 • 4 minutes to read

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:

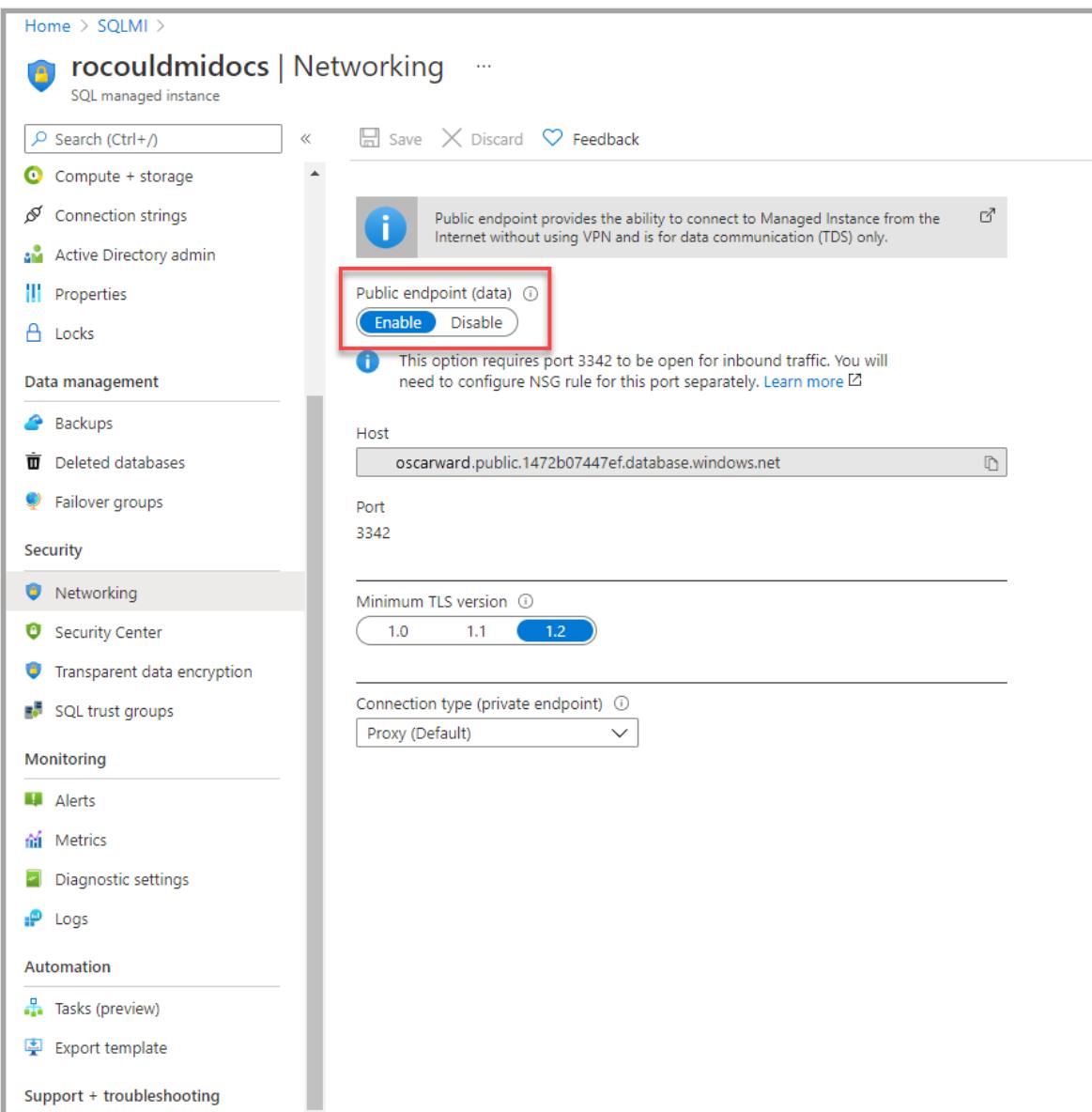
1. Enable a public endpoint in the SQL Managed Instance
2. Create a Network Security Group rule to allow inbound traffic
3. Enter the credentials in Power BI

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. Navigate to your SQL Managed Instance in the Azure portal.
2. On the left side of the page select **Networking**, slide the **Public endpoint (data)** to **Enable**. The following image shows the screen in the Azure portal.



3. Set the **Minimum TLS version** to 1.2

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. Currently this action can't be completed in the Azure portal, and rather, must be accomplished using either the *Command Line Interface (CLI)* or by using *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 may 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
#specify 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 Network Security Group (NSG) rule. For more information, see [Add a network security group rule in PowerShell](#). You may 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 the Power BI service

The last part of the process is entering the credentials in the Power BI service. Log into Power BI 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*. Take the following steps to complete the process:

1. Navigate to **Dataset settings**.

2. Expand the **Data source credentials** section, as shown in the following image.

The screenshot shows the 'Datasets' tab selected in the top navigation bar. On the left, a list of datasets includes 'ASAdataset', 'Contoso SQL MI Demo' (which is selected and highlighted in grey), 'Customer Profitability Sample PBIX', and 'datasourceParameter'. The main content area is titled 'Settings for Contoso SQL MI Demo' and shows the dataset was configured by 'oscarward@contoso.com'. A red box highlights the 'Data source credentials' section, which contains the connection string 'contoso-oscarward242 .public.1472b07447ef.database.windows.net;3342'. Below this, there are links for 'Edit credentials' and 'Show in lineage view'. Other sections listed include 'Gateway connection', 'Sensitivity label', 'Parameters', 'Query Caching', 'Scheduled refresh', 'Server settings', 'Q&A', 'Featured Q&A questions', 'Endorsement', 'Large dataset storage format', and 'Dataset Image'.

3. Select the **edit credentials** link. In the dialog 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.

Next steps

- [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 endpoints for accessing Power BI

Article • 09/29/2022 • 11 minutes to read

You can use the Azure Private Link feature to provide secure access for data traffic in Power BI. Azure networking provides the Azure Private Link feature. In this configuration, Azure Private Link and Azure Networking private endpoints are used to send data traffic privately using Microsoft's backbone network infrastructure. The data travels the Microsoft private network backbone instead of going across the Internet.

When private link connections are used, those connections go through the Microsoft private network backbone when Power BI users access resources in the Power BI service.

See [What is Azure Private Link](#) to learn more about Azure Private Link.

Understanding private endpoints

Private endpoints guarantee that traffic going *into* your organization's Power BI items (such as reports, or workspaces) always follow your organization's configured private link network path. User traffic to your Power BI items must come from the established private link. You can configure Power BI to deny all requests that don't come from the configured network path.

Private endpoints *do not* guarantee that traffic from Power BI 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.

Power BI and private endpoint integration

Azure Private Endpoint for Power BI is a network interface that connects you privately and securely to the Power BI service, powered by Azure Private Link.

Private Endpoints integration enables Platform as a Service (PaaS) services to be deployed and accessed privately from customer's virtual and on-premises networks, while the service is still running outside of the customer's network. Private Endpoints is a single, directional technology that lets clients initiate connections to a given service, but it 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 multi-tenant services, this Private Endpoint model provides link identifiers to prevent access to other customers' resources hosted within the same service. When using Private Endpoints,

only a limited set of other PaaS service resources can be accessed from services using the integration.

The Power BI service implements Private Endpoints, and not Service Endpoints.

Using private endpoints with Power BI provide the following benefits:

1. Private endpoints ensure that traffic will flow over the Azure backbone to a private endpoint for Azure cloud-based resources.
2. Network traffic isolation from non-Azure based infrastructure, such as on-premises access, would require customers to have ExpressRoute or a Virtual Private Network (VPN) configured.

Using secure private endpoints to access Power BI

In Power BI, you can configure and use an endpoint that enables your organization to access Power BI privately. To configure private endpoints, you must be a Power BI administrator and have permissions in Azure to create and configure resources such as Virtual Machines (VMs) and Virtual Networks (V-Net).

The steps that enable you to securely access Power BI from private endpoints are:

1. [Enable private endpoints for Power BI](#)
2. [Create a Power BI resource in the Azure portal](#)
3. [Create a virtual network](#)
4. [Create a virtual machine \(VM\)](#)
5. [Create a private endpoint](#)
6. [Connect to a VM using Remote Desktop \(RDP\)](#)
7. [Access Power BI privately from the virtual machine](#)
8. [Disable public access for Power BI](#)

The following sections provide additional information for each step.

Enable private endpoints for Power BI

To get started, sign in to the [Power BI](#) service as an administrator, then perform the following steps:

1. From the page header, select **Settings > Admin portal**.

2. Select **Tenant settings** and scroll to **Advanced Networking**. Toggle the radio button to turn on **Azure Private Link**.

The screenshot shows the 'Advanced networking' section of the Azure Power BI tenant settings. It contains two main configuration items:

- Azure Private Link**: Described as *Enabled for the entire organization*. A note says: "Increase security by allowing people to use a Private Link to access your Power BI tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email. [Learn more](#) | [Set-up instructions](#)". A toggle switch is set to **Enabled**.
- Block Public Internet Access**: Described as *Disabled for the entire organization*. A note says: "For extra security, block access to your Power BI tenant via the public internet. This means people who don't have access to the Private Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect". A toggle switch is set to **Disabled**.

Each configuration item has an **Apply** and **Cancel** button below it.

It takes about 15 minutes to configure a private link for your tenant, which includes configuring a separate FQDN for the tenant in order to communicate privately with Power BI services.

After this process is finished, you can move on to the next step.

Create a Power BI resource in the Azure portal

Next, sign into the [Azure portal](#) and create a Power BI resource, using an **Azure Template**. Replace the parameters in the ARM template example, shown in the following table, to create a Power BI resource.

Parameter	Value
<resource-name>	myPowerBIResource
<tenant-object-id>	Find your tenant ID in the Azure portal

Create the ARM template

```
{  
    "$schema": "http://schema.management.azure.com/schemas/2015-01-  
01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {},  
    "resources": [  
        {  
            "type": "Microsoft.PowerBI/privateLinkServicesForPowerBI",  
            "apiVersion": "2020-06-01",  
            "name": "<resource-name>",  
            "location": "global",  
            "properties":  
            {  
                "tenantId": "<tenant-object-id>"  
            }  
        }  
    ]  
}
```

In the dialog that appears, select the checkbox to agree to the terms and conditions, and then select **Purchase**.

Custom deployment
Deploy from a custom template

TEMPLATE

1 resource  

BASICS

Subscription *

Resource group * [Create new](#)

Location

TERMS AND CONDITIONS

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

I agree to the terms and conditions stated above

Create a virtual network

The next step is to create a virtual network and subnet. Replace the sample parameters in the table below with your own to create a virtual network and subnet.

Parameter	Value
<resource-group-name>	myResourceGroup
<virtual-network-name>	myVirtualNetwork
<region-name>	Central US
<IPv4-address-space>	10.5.0.0/16
<subnet-name>	mySubnet
<subnet-address-range>	10.5.0.0/24

1. On the upper-left side of the screen, select **Create a resource > Networking > Virtual network** or search for **Virtual network** in the search box.
2. In **Create virtual network** enter or select the following information in the **Basics** tab:

Settings	Value
Project details	
Subscription	Select your Azure Subscription
Resource Group	Select Create new , enter <resource-group-name>, then select OK , or select an existing <resource-group-name> based on parameters.
Instance details	
Name	Enter <virtual-network-name>
Region	Select <region-name>

The following image shows the **Basics** tab.

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *	PrivateLinkTesting
Resource group *	myResourceGroup
	Create new

Instance details

Name *	myVirtualNetwork
Region *	(US) Central US

3. Next, select the **IP Addresses** tab or select the **Next: IP Addresses** button at the bottom of the form. In the IP Addresses tab, enter the following information:

Settings	Value
IPv4 address space	Enter <IPv4-address-space>

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.5.0.0/16 10.5.0.0 - 10.5.255.255 (65536 addresses)



Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+ Add subnet](#) [Remove subnet](#)

Subnet name

Subnet address range

default

10.5.0.0/24

4. In **Subnet name** select the word *default*, and in **Edit subnet**, enter the following information:

Settings	Value

Settings	Value
Subnet name	Enter <subnet-name>
Subnet address range	Enter <subnet-address-range>

Edit subnet X

Subnet name *
mySubnet ✓

Subnet address range * ⓘ
10.5.0.0/24
10.5.0.0 - 10.5.0.255 (251 + 5 Azure reserved addresses)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ
0 selected ▼

5. Then select **Save**, and then select the **Review + create** tab, or select the **Review + create** button.

6. Then, select **Create**.

Once you've completed these steps, you can create a virtual machine (VM), as described in the next section.

Create a virtual machine (VM)

The next step is to create virtual network, and the subnet to host the virtual machine (VM).

1. On the upper-left side of the screen in your Azure portal, select **Create a resource** > **Compute** > **Virtual Machine**.
2. In **Create a virtual machine - Basics** enter or select the following information:

Settings	Value
Project details	
Subscription	Select your Azure Subscription
Resource Group	Select myResourceGroup which you created in the previous section.
Instance details	
Name	Enter myVm
Region	Select Central US
Availability options	Leave the default No infrastructure redundancy required
Image	Select Windows 10 Pro
Size	Leave the default Standard DS1 v2
ADMINISTRATOR ACCOUNT	
Username	Enter a username of your choosing
Password	Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements
Confirm Password	Reenter password
INBOUND PORT RULES	
Public inbound ports	Leave the default None
SAVE MONEY	
Already have a Windows license?	Leave the default No

3. Then select **Next: Disks**

4. In **Create a virtual machine - Disks**, leave the defaults and select **Next: Networking**.

5. In **Create a virtual machine - Networking**, select the following information:

Settings	Value
Virtual network	Leave the default MyVirtualNetwork
Address space	Leave the default 10.5.0.0/24
Subnet	Leave the default mySubnet (10.5.0.0/24)
Public IP	Leave the default (new) myVm-ip
Public inbound ports	Select **Allow selected **
Select inbound ports	Select RDP

6. Select **Review + create**. You're taken to the **Review + create** page where Azure validates your configuration.
7. When you see the **Validation passed** message, select **Create**.

Create a private endpoint

The next step, is to create a private endpoint for Power BI.

1. On the upper-left side of the Azure portal screen **Create a resource > Networking > Private Link Center (Preview)**.
2. In **Private Link Center - Overview**, on the option to **Build a private connection to a service**, select **Create private endpoint**.
3. In **Create a private endpoint (Preview) - Basics** enter or select the following information:

Settings	Value
Project details	
Subscription	Select your Azure Subscription
Resource Group	Select myResourceGroup . You created this in the previous section
Instance details	
Name	Enter <i>myPrivateEndpoint</i> . If this name is taken, create a unique name
Region	Select Central US

The following image shows the **Create a private endpoint - Basics** window.

Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription *

Resource group *
[Create new](#)

Instance details

Name *

Region *

- Once that information is complete, select **Next: Resource** and in the **Create a private endpoint - Resource** page, enter or select the following information:

Settings	Value
Connection method	Select connect to an Azure resource in my directory
Subscription	Select your subscription
Resource type	Select Microsoft.PowerBI/privateLinkServicesForPowerBI
Resource	myPowerBIResource
Target sub-resource	Tenant

The following image shows the **Create a private endpoint - Resource** window.

✓ Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method Connect to an Azure resource in my directory.
 Connect to an Azure resource by resource ID or alias.

Subscription *

Resource type *

Resource *

Target sub-resource *

5. Once that information is properly input, select **Next: Configuration** and in the **Create a private endpoint (Preview) - Configuration** and enter or select the following information:

Settings	Value
NETWORKING	
Virtual network	Select <i>myVirtualNetwork</i>
Subnet	Select <i>mySubnet</i>
PRIVATE DNS INTEGRATION	
Integrate with private DNS zone	Select Yes
Private DNS Zone	Select <i>(New)privatelink.analysis.windows.net</i> <i>(New)privatelink.pbidedicated.windows.net</i> <i>(New)privatelink.tip1.powerquery.microsoft.com</i>

The following image shows the **Create a private endpoint - Configuration** window.

The screenshot shows the 'Create a private endpoint' configuration page. The top navigation bar has five tabs: Basics (checkmark), Resource (checkmark), Configuration (selected, highlighted in blue), Tags (number 4), and Review + create (number 5). The main area is divided into two sections: Networking and Private DNS integration.

Networking: Under 'Virtual network *', the dropdown shows 'myVirtualNetwork'. Under 'Subnet *', the dropdown shows 'mySubnet (10.5.0.0/24)'. A note below states: 'If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.'

Private DNS integration: Under 'Integrate with private DNS zone', there is a radio button for 'Yes' (selected) and one for 'No'. Below this, a table lists three configuration names with their corresponding subscription and private DNS zones:

Configuration name	Subscription	Private DNS zones
privatelink-analysis-wi...	PrivateLinkTesting	(New) privatelink.analysis.windows.net
privatelink-pbidedicat...	PrivateLinkTesting	(New) privatelink.pbidedicated.windows.net
privatelink-tip1-power...	PrivateLinkTesting	(New) privatelink.tip1.powerquery.microsoft.c...

Next select **Review + create**, which displays the **Review + create** page where Azure validates your configuration. When you see the **Validation passed** message, select **Create**.

Connect to a VM using Remote Desktop (RDP)

Once you've created your virtual machine, called **myVM**, connected to it from the Internet using the following steps:

1. In the portal's search bar, enter *myVm*.
2. Select the **Connect** button. Once you select the **Connect** button, **Connect to virtual machine** opens.
3. Select **Download RDP File**. Azure creates a Remote Desktop Protocol (.rdp) file and downloads it to your computer.
4. Open the .rdp file.
5. If prompted, select **Connect**.
6. Enter the username and password you specified when creating the VM in the previous step.
7. Select **OK**.
8. You may receive a certificate warning during the sign-in process. If you receive a certificate warning, select **Yes** or **Continue**.

Access Power BI privately from the VM

The next step is to access Power BI privately, from the virtual machine you created in the previous step, using the following steps:

1. In the Remote Desktop of myVM, open PowerShell.
2. Enter nslookup *tenant-object-id-without-hyphens-api.privatelink.analysis.windows.net*.
3. You'll receive a response similar to the message shown below:

```
Server: UnKnown
Address: 168.63.129.16

Non-authoritative answer:
Name: 52d40f65ad6d48c3906f1ccf598612d4-
      api.privatelink.analysis.windows.net
Address: 10.5.0.4
```

4. Open the browser and go to app.powerbi.com to access Power BI privately.

Disable public access for Power BI

Lastly, you need to disable public access for Power BI.

Sign to the [Power BI](#) service as an administrator, and navigate to the **Admin portal**. Select **Tenant settings** and scroll to the **Advanced networking** section. Enable the toggle button in the **Block Public Internet Access** section, as shown in the following image. It takes approximately 15 minutes for the system to disable your organization's access to Power BI from the public Internet.

And that's it - after following these steps, Power BI for your organizations is only accessible from private endpoints, and not accessible from the public Internet.

Considerations and limitations

There are a few considerations to keep in mind while working with private endpoints in Power BI:

- Any uses of external images or themes aren't available when using a private link environment.
- If Internet access is disabled, and if the dataset or dataflow is connecting to a Power BI dataset or dataflow as a data source, the connection will fail.
- Each private endpoint can be connected to one tenant only.
- Datamarts don't support private links using SSMS. Even with a configured private link, connections to datamarts using SSMS are only supported through public Internet access.
- If your organization is using **Azure Private Link** in Power BI, modern usage metrics reports will contain partial data (only Report Open events). A current limitation when transferring client information over private links prevents Power BI from capturing Report Page Views and performance data over Private Links. If your organization is using **Azure Private Link** and **Block Public Internet Access** in Power BI, the refresh for the dataset will fail and the usage metrics report will not show any data.
- The Power BI Premium Capacity Metrics app doesn't work when private links are enabled.

- Publish to Web is not supported when you enable **Azure Private Link** in Power BI.
- Exporting a report as PDF or PowerPoint is not supported when you enable **Azure Private Link** in Power BI.
- Email subscriptions are not supported when you enable **Block Public Internet Access** in Power BI.
- [Microsoft Purview Information Protection](#) doesn't currently support Private Links. This means that in [Power BI Desktop](#) running in an isolated network, the Sensitivity button will be grayed out, label information will not appear, and decryption of .pbix files will fail.

To enable these capabilities in Power BI Desktop, admins can configure [Service Tags](#) for the underlying services that support MIP, [EOP](#), and AIP. Make sure you understand the implications of using Service Tags in a Private Links isolated network.

- Gateways enabled for Power BI private endpoints will not work properly with non-Power BI scenarios. For some scenarios, a potential workaround is to turn off Private Links, configure the gateway in a 'remote' region (a region other than the Recommended region), and then reenable the Private Links. After the Private Link is re-enabled, the Gateway in the remote region won't be using Private Link.
- When private links are enabled for Power BI, an on-premises data gateway (personal mode) will fail to register.
- Private Links resource REST APIs don't support tags.
- You can't set up a private link to be used by more than one tenant.

Next steps

- [Administering Power BI in your Organization](#)
- [Understanding the Power BI admin role](#)
- [Auditing Power BI in your organization](#)
- [How to find your Azure Active Directory tenant ID](#)

The following video shows how to connect a mobile device to Power BI, using private endpoints:

 **Note**

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

<https://www.youtube-nocookie.com/embed/-3yFtIZBpqS>

More questions? Try asking the Power BI Community [↗](#)

Configure mobile apps with Microsoft Intune

Article • 03/09/2022 • 3 minutes to read

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 is not 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 device 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. The article is not meant as a full configuration guide for Microsoft Intune. For more information on 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 can use the Power BI app on their devices, an Intune admin must add the app to Intune and also 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 enter the app.

Step 1: Add the Power BI app to Intune

To add the Power BI app to Intune, use the steps provided in the following topics:

- [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, you can 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, use the steps provided 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 inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. 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, use the steps provided in [How to create and assign app protection policies](#).

Step 4: Use the application on a device

Managed apps are apps that your company support can set up to help protect company data that you can access in that app. When you access company data in a managed app on your device, you may 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 provided in the following articles:

- [Use managed apps on your iOS device](#)
- [Use managed apps on your Android device](#)

Next steps

[How to create and assign app protection policies](#)

[Power BI apps for mobile devices](#)

More questions? [Try asking the Power BI Community](#) ↗

Customer Lockbox for Power BI

Article • 11/02/2022 • 3 minutes to read

APPLIES TO: ✗ Power BI Desktop ✓ Power BI service

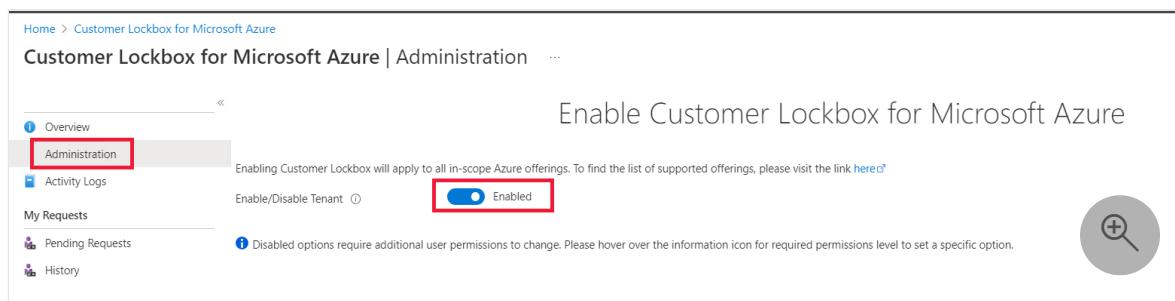
Use [Customer Lockbox for Microsoft Azure](#) to control how Microsoft engineers access your data. In this article you'll learn how Customer Lockbox requests are initiated, tracked, and stored for later reviews and audits.

Typically, Customer Lockbox is used to help Microsoft engineers troubleshoot a Power BI service support request. Customer Lockbox can also be used when Microsoft identifies a problem, and a Microsoft-initiated event is opened to investigate the issue.

Enable Customer Lockbox for Power BI

To enable Customer Lockbox for Power BI, you must be an Azure AD Global Administrator. To assign roles in Azure AD, see [Assign Azure AD roles to users](#).

1. Open the Azure portal.
2. Go to [Customer Lockbox for Microsoft Azure](#).
3. In the Administration tab, select **Enabled**.



Microsoft access request

In cases where the Microsoft engineer can't troubleshoot your issue by using standard tools, elevated permissions are requested using the [Just-In-Time](#) (JIT) access service. The request can come from the original support engineer, or from a different engineer.

After the access request is submitted, the JIT service evaluates the request, considering factors such as:

- The scope of the resource

- Whether the requester is an isolated identity or using multi-factor authentication
- Permissions levels

Based on the JIT role, the request may also include an approval from internal Microsoft approvers. For example, the approver might be the customer support lead or the DevOps Manager.

When the request requires direct access to customer data, a Customer Lockbox request is initiated. For example, in cases where remote desktop access to a customer's virtual machine is needed. Once the Customer Lockbox request is made, it awaits customer's approval before access is granted.

These steps describe a Microsoft initiated Customer Lockbox request, for Power BI service.

1. The Azure AD Global Administrator receives a pending access request notification email from Microsoft. The admin who received the email, becomes the designated approver.

Microsoft Azure

Customer Lockbox for Microsoft Azure

A customer Lockbox request is pending your approval.

Please [sign in](#) to the Azure portal and go to the "Customer Lockbox for Microsoft Azure" service blade to approve this request.

Request Information

Support request #	342918742
Requestor	Microsoft Support Engineer
Resource ID	Power BI
Resource type	ACIS
Justification	Microsoft Support Team is requesting access to your resource temporarily for troubleshooting.
Request start time	October 19, 2022
Duration of access	08:00:00
Request end time	October 23, 2022
Client Request ID	ee7c304f-3747-45b4-9433-ecb182af4f37

By approving this request, the Microsoft support organization will be given direct access to your resource for the purpose of troubleshooting and/or resolving the technical issue described in the Microsoft support case.



2. The email provides a link to Customer Lockbox in the Azure Administration module. Using the link, the designated approver signs in to the Azure portal to view any pending Customer Lockbox requests. The request remains in the customer queue for four days. After that, the access request automatically expires and no access is granted to Microsoft engineers.
3. To get the details of the pending request, the designated approver can select the Customer Lockbox request from the **Pending Requests** menu option.
4. After reviewing the request, the designated approver enters a justification and selects one of the options below. For auditing purposes, the actions are logged in the Customer Lockbox [logs](#).
 - **Approve** - Access is granted to the Microsoft engineer for a default period of eight hours.
 - **Deny** - The access request by the Microsoft engineer is rejected and no further action is taken.

X

 Microsoft Support Engineer
lockboxnotify@microsoft.com

Created Time 10/19/2022, 5:08 PM

Requestor Microsoft Support Engineer

Service Request Id 342918742

Reason Microsoft Support Team is requesting access to your resource temporarily for troubleshooting.

Resource Type ACIS

Resource Name Power BI

Subscription Name N/A

Expires on 10/23/2022, 5:08 PM

Requested Duration 08:00:00

Client Request Id ee7c304f-3747-45b4-9433-ecb182af4f37

Justification * ⓘ

Approve Deny 

Logs

Customer Lockbox has two type of logs:

- **Activity logs** - Available from the [Azure Monitor activity log](#).

The following activity logs are available for Customer Lockbox:

- Deny Lockbox Request

- Create Lockbox Request
- Approve Lockbox Request
- Lockbox Request Expiry

To access the activity logs, in the Azure portal, select *Activity Log*. You can filter the results for specific actions.

- **Audit logs** - Available from the Microsoft Purview compliance portal. You can see the audit logs in the Power BI [admin portal](#).

Customer Lockbox for Power BI has four [Power BI audit logs](#):

Audit log	Friendly name
GetRefreshHistoryViaLockbox	Get refresh history via lockbox
DeleteAdminUsageDashboardsViaLockbox	Delete admin usage dashboards via lockbox
DeleteUsageMetricsv2PackageViaLockbox	Delete usage metrics v2 package via lockbox
DeleteAdminMonitoringFolderViaLockbox	Delete admin monitoring folder via lockbox

Exclusions

Customer Lockbox requests aren't triggered in the following engineering support scenarios:

- Emergency scenarios that fall outside of standard operating procedures. For example, a major service outage requires immediate attention to recover or restore

services in an unexpected scenario. These events are rare and usually don't require access to customer data.

- A Microsoft engineer accesses the Azure platform as part of troubleshooting, and is accidentally exposed to customer data. For example, during troubleshooting the Azure Network Team captures a packet on a network device. Such scenarios don't usually result in access to meaningful customer data.
- External legal demands for data. For details, see [government requests for data](#) on the Microsoft Trust Center.

Next steps

[Microsoft Purview Customer Lockbox](#)

[Microsoft 365 guidance for security & compliance](#)

[Power BI Security](#)

Enable service principal authentication for read-only admin APIs

Article • 11/24/2022 • 3 minutes to read

Service principal is an authentication method that can be used to let an Azure Active Directory (Azure AD) application access Power BI service content and APIs. When you create an Azure AD app, a [service principal object](#) is created. The service principal object, also known simply as the service principal, allows Azure AD to authenticate your app. Once authenticated, the app can access Azure AD tenant resources.

Method

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

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

Important

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

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

New Group

Group type * ⓘ

 ▼

Group name * ⓘ

 ✓

Group description ⓘ

Azure AD roles can be assigned to the group (Preview) ⓘ

 Yes No

Membership type * ⓘ

 ▼

Owners

No owners selected

Members

No members selected

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

ⓘ **Important**

Make sure the app doesn't have any admin-consent required permissions for Power BI set on it in the Azure portal. [See how to check whether your app has any such permissions.](#)

4. Enable the Power BI service admin settings:

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

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

Unapplied changes

Web apps registered in Azure Active Directory (Azure AD) will use an assigned service principal to access read-only Power BI Admin APIs without a signed in user. To allow an app to use service principal authentication, its service principal must be included in an allowed security group. By including the service principal in the allowed security group, you're giving the service principal read-only access to all the information available through Power BI admin APIs (current and future). For example, Power BI user names and emails, dataset and report detailed metadata. [Learn more](#)

 Enabled

Apply to:

The entire organization

Specific security groups

Enter security groups

 Apply  Cancel

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

 **Important**

An app using service principal authentication that calls read-only admin APIs **must not** have any admin-consent required permissions for Power BI set on it in the Azure portal. [See how to check whether your app has any such permissions.](#)

Supported APIs

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

- [GetGroupsAsAdmin](#) with \$expand for dashboards, datasets, reports, and dataflows
- [GetGroupUsersAsAdmin](#)
- [GetDashboardsAsAdmin](#) with \$expand tiles
- [GetDashboardUsersAsAdmin](#)
- [GetAppsAsAdmin](#)
- [GetAppUsersAsAdmin](#)
- [GetDatasourcesAsAdmin](#)
- [GetDatasetToDataflowsLinksAsAdmin](#)
- [GetDataflowDatasourcesAsAdmin](#)
- [GetDataflowUpstreamDataflowsAsAdmin](#)

- [GetCapacitiesAsAdmin](#)
- [GetCapacityUsersAsAdmin](#)
- [GetActivityLog](#)
- [GetModifiedWorkspaces](#)
- [WorkspaceGetInfo](#)
- [WorkspaceScanStatus](#)
- [WorkspaceScanResult](#)
- [GetDashboardsInGroupAsAdmin](#)
- [GetTilesAsAdmin](#)
- [ExportDataflowAsAdmin](#)
- [GetDataflowsAsAdmin](#)
- [GetDataflowUsersAsAdmin](#)
- [GetDataflowsInGroupAsAdmin](#)
- [GetDatasetsAsAdmin](#)
- [GetDatasetUsersAsAdmin](#)
- [GetDatasetsInGroupAsAdmin](#)
- [Get Power BI Encryption Keys](#)
- [Get Refreshable For Capacity](#)
- [Get Refreshables](#)
- [Get Refreshables For Capacity](#)
- [GetImportsAsAdmin](#)
- [GetReportsAsAdmin](#)
- [GetReportUsersAsAdmin](#)
- [GetReportsInGroupAsAdmin](#)

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

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

1. Sign into the **Azure portal** as a Global Administrator, an Application Administrator, or a Cloud Application Administrator.
2. Select **Azure Active Directory**, then **Enterprise applications**.
3. Select the application you want to grant access to Power BI.
4. Select **Permissions**. There must be no admin-consent required permissions of type Application registered for the app.

Considerations and limitations

- You can't sign into the Power BI portal using service principal.
- Power BI admin rights are required to enable service principal in the Admin API settings in the Power BI admin portal.

PowerShell cmdlets, REST APIs, and .NET Client library for Power BI administration

Article • 03/09/2022 • 2 minutes to read

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
<code>Get-PowerBIDatasource</code>	N/A	<code>Datasets_GetDataSourcesAsAdmin</code>	<code>/v1.0/myorg/admin/datasets/{datasetkey}/datasources</code>	Gets the data sources for a given dataset.
<code>Get-PowerBI Dataset</code>	N/A	<code>Datasets_GetDatasetsAsAdmin</code>	<code>/v1.0/myorg/admin/datasets</code>	Gets the full list of datasets in a Power BI tenant.
<code>Get-PowerBIWorkspace</code>	<code>Get-PowerBIGroup</code>	<code>Groups_GetGroupsAsAdmin</code>	<code>/v1.0/myorg/admin/groups</code>	Gets the full list of workspaces in a Power BI tenant.
<code>Add-PowerBIworkspaceUser</code>	<code>Add-PowerBIGroupUser</code>	<code>Groups_AddUserAsAdmin</code>	<code>/v1.0/myorg/admin/groups/{groupId}/users</code>	Adds a user as a member to a given workspace.
<code>Remove-PowerBIworkspaceUser</code>	<code>Remove-PowerBIGroupUser</code>	<code>Groups_DeleteUserAsAdmin</code>	<code>/v1.0/myorg/admin/groups/{groupId}/users/{user}</code>	Removes a user from the membership list of a given workspace.
<code>Restore-PowerBIworkspace</code>	<code>Restore-PowerBIGroup</code>	<code>Groups_RestoreDeletedGroupAsAdmin</code>	<code>/v1.0/myorg/admin/groups/{groupId}/restore</code>	Restores a deleted workspace.
<code>Set-PowerBIworkspace</code>	<code>Set-PowerBIGroup</code>	<code>Groups_UpdateGroupAsAdmin</code>	<code>/v1.0/myorg/admin/groups/{groupId}</code>	Updates the properties of a given workspace.
<code>Get-PowerBIDataset - WorkspaceId</code>	N/A	<code>Groups_GetDatasetsAsAdmin</code>	<code>/v1.0/myorg/admin/groups/{group_id}/datasets</code>	Gets the datasets within a given workspace.
<code>Get-PowerBIReport</code>	N/A	<code>Reports_GetReportsAsAdmin</code>	<code>/v1.0/myorg/admin/reports</code>	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 • 4 minutes to read

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.

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 038f9a64-1fcf-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 `-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.