Microsoft Fabric End-to-End Security Whitepaper

Technical reviewers: Kasper de Jonge, Sergei Gundorov, Vengatesh Parasuraman

Version: November, 2024

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Introduction

Security is a top priority for any organization that wants to succeed in the digital age. You need to safeguard your assets from threats and follow your organization's security policies. This whitepaper serves as an end-to-end security overview for Microsoft Fabric. It covers details on how Microsoft secures your data by default as a SaaS service and how you can secure, manage, and govern the data stored in Microsoft Fabric as an organization.

The contents of this whitepaper is created by combining several security related online documents into a single whitepaper for reading convenience. This whitepaper will be updated regularly, but the online documentation will always be up to date. You can find the online documentation here: Microsoft Fabric security - Microsoft Fabric | Microsoft Learn

Table of contents:

End to end Security

Microsoft Fabric is a software as a service (SaaS) platform that lets users get, create, share, and visualize data.

As a SaaS service, Fabric offers a complete security package for the entire platform. Fabric removes the cost and responsibility of maintaining your security solution, and transfers it to the cloud. With Fabric, you can use the expertise and resources of Microsoft to keep your data secure, patch vulnerabilities, monitor threats, and comply with regulations. Fabric also allows you to manage, control and audit your security settings, in line with your changing needs and demands.

As you bring your data to the cloud and use it with various analytic experiences such as Power BI, Data Factory, and the next generation of Synapse, Microsoft ensures that built-in security and reliability features secure your data at rest and in transit. Microsoft also makes sure that your data is recoverable in cases of infrastructure failures or disasters.

Fabric security is:

- **Always on** - Every interaction with Fabric is encrypted by default and authenticated using Microsoft Entra ID. All communication between Fabric experiences travels through the Microsoft backbone internet. Data at rest is automatically stored encrypted. To regulate access to Fabric, you can add extra security features such as Private Links or Entra Conditional Access . Fabric can also connect to data protected by a firewall or a private network using trusted access.
- **Compliant** – Fabric has data sovereignty out of the box with multi geo capacities. Fabric also supports a wide range of compliance standards.
- **Governable** - Fabric comes with a set of governance tools such data lineage, information protection labels, data loss prevention and purview integration.
- **Configurable** - You can configure Fabric security in accordance with your organizational policies.
- **Evolving** - Microsoft is constantly improving Fabric security, by adding new features and controls.

Fabric platform

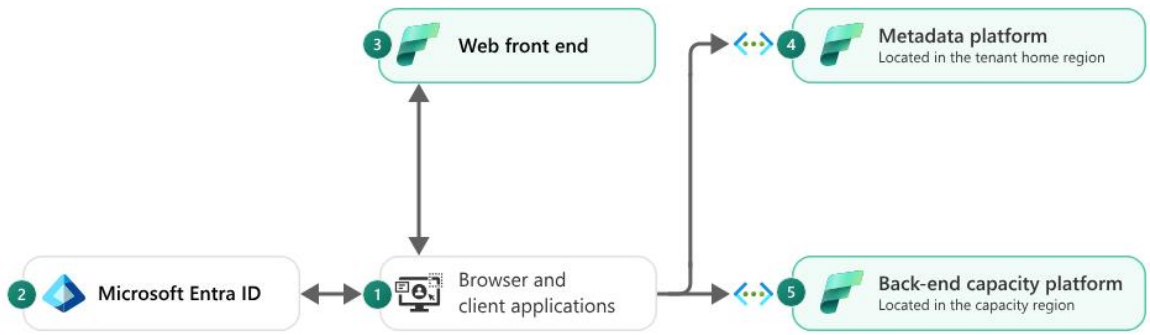
The Fabric platform comprises a series of services and infrastructure components that support the common functionality for all Fabric experiences. Collectively, they offer a comprehensive set of analytics experiences designed to work together

seamlessly. Experiences include Lakehouse, Data Factory, Synapse Data Engineering, Synapse Data Warehouse, Power BI, and others.

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

Architectural diagram

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



The architectural diagram depicts the following concepts.

1. A user uses a browser or a client application, like Power BI Desktop, to connect to the Fabric service.
2. Authentication is handled by Microsoft Entra ID, previously known as Azure Active Directory, which is the cloud-based identity and access management service that authenticates the user or service principal and manages access to Fabric.
3. The web front end receives user requests and facilitates login. It also routes requests and serves front-end content to the user.
4. The metadata platform stores tenant metadata, which can include customer data. Fabric services query this platform on demand in order to retrieve authorization information and to authorize and validate user requests. It's located in the tenant home region.
5. The back-end capacity platform is responsible for compute operations and for storing customer data, and it's located in the capacity region. It

leverages Azure core services in that region as necessary for specific Fabric experiences.

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

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

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

Authenticate

Microsoft Fabric is a SaaS platform, like many other Microsoft services such as Azure, Microsoft Office, OneDrive, and Dynamics. All these Microsoft SaaS services including Fabric, use Microsoft Entra ID as their cloud-based identity provider. Microsoft Entra ID helps users connect to these services quickly and easily from any device and any network. Every request to connect to Fabric is authenticated with Microsoft Entra ID, allowing users to safely connect to Fabric from their corporate office, when working at home, or from a remote location.

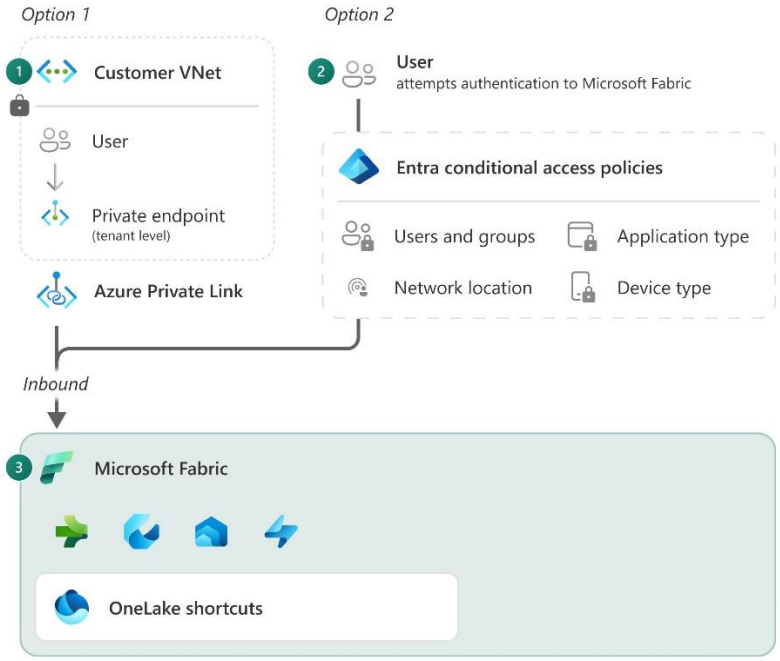
When authenticated, users receive access tokens from Microsoft Entra ID. Fabric uses these tokens to perform operations in the context of the user.

Network security

Fabric is SaaS service that runs in the Microsoft cloud. Some scenarios involve connecting to data that's outside of the Fabric platform. For example, viewing a report from your own network or connecting to data that's in another service. Interactions within Fabric use the internal Microsoft network and traffic outside of the service is protected by default.

Inbound network security

Inbound traffic is traffic coming into Fabric from the internet. This article explains the differences between the two ways to protect inbound traffic in Microsoft Fabric. Use this article to decide which method is best for your organization.



1. **Entra Conditional Access** - When a user authenticates access is determined based on a set of policies that might include IP address, location, and managed devices.
2. **Private links** - Fabric uses a private IP address from your virtual network. The endpoint allows users in your network to communicate with Fabric over the private IP address using private links.
3. **Access to Fabric** is additionally secured, either through connecting through a private network or adhering to the additional Entra policies

Once traffic enters Fabric, it gets authenticated by Microsoft Entra ID, which is the same authentication method used by Microsoft 365, OneDrive, and Dynamics 365. Microsoft Entra ID authentication allows users to securely connect to cloud applications from any device and any network, whether they're at home, remote, or in their corporate office.

The Fabric backend platform is protected by a virtual network and isn't directly accessible from the public internet other than through secure endpoints.

By default, Fabric communicates between experiences using the internal Microsoft backbone network. When a Power BI report loads data from OneLake, the data goes through the internal Microsoft network. This configuration is different from having to set up multiple Platform as a Service (PaaS) services to connect to each other over a private network. Inbound communication between clients such as your browser or SQL Server Management Studio (SSMS) and Fabric, uses the TLS 1.2 protocol and negotiates to TLS 1.3 when possible.

Fabric's default security settings include:

- Microsoft Entra ID which is used to authenticate every request.
- Upon successful authentication, requests are routed to the appropriate backend service through secure Microsoft managed endpoints.
- Internal traffic between experiences in Fabric is routed over the Microsoft backbone.
- Traffic between clients and Fabric is encrypted using at least the Transport Layer Security (TLS) 1.2 protocol.

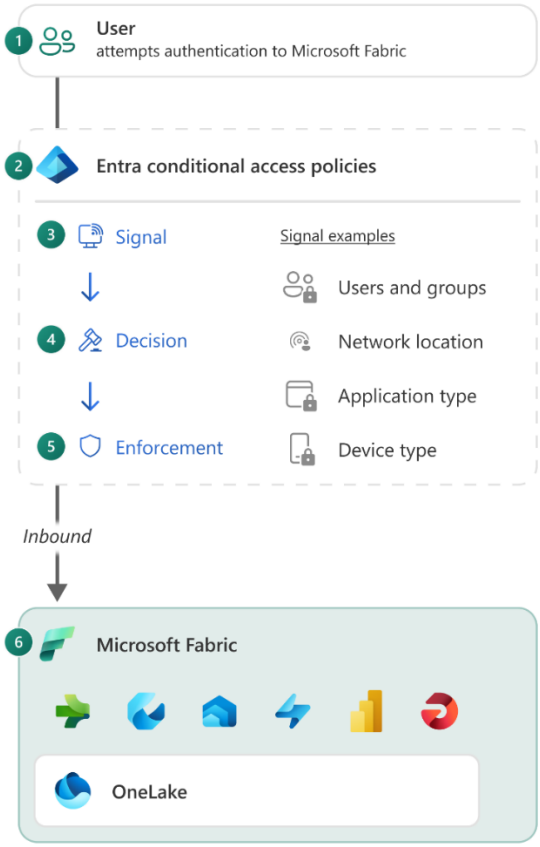
Entra Conditional Access

Every interaction with Fabric is authenticated with Microsoft Entra ID. Microsoft Entra ID is based upon the Zero Trust security model, which assumes that you're not fully protected within your organization's network perimeter. Instead of looking at your network as a security boundary, Zero Trust looks at identity as the primary perimeter for security.

To determine access at the time of authentication you can define and enforce conditional access policies based on your users' identity, device context, location, network, and application sensitivity. For example, you can require multifactor authentication, device compliance, or approved apps for accessing your data and resources in Fabric. You can also block or limit access from risky locations, devices, or networks.

Conditional access policies help you protect your data and applications without compromising user productivity and experience. Here are a few examples of access restrictions you can enforce using conditional access.

- Define a list of IPs for inbound connectivity to Fabric.
- Use Multifactor Authentication (MFA).
- Restrict traffic based on parameters such as country of origin or device type.



The architectural diagram depicts the following concepts.

1. The user attempts to connect to Fabric by for example opening the web browser or using SSMS to connect to a SQL Endpoint
2. The organization defines a policy as Entra conditional access to determine who is allowed access to Microsoft Fabric.
3. When authenticating Entra collects signals from the user like its account, network location, which application it connects to and which device they are connecting from.
4. Based on the policy defined in step 2 and the signals in step 3 Entra makes a decision to authenticate or not.

5. The decision gets enforced for each authentication attempt.
6. When the authentication is successful access to Microsoft Fabric is granted.

Fabric doesn't support other authentication methods such as account keys or SQL authentication, which rely on usernames and passwords.

Configure conditional access

To configure conditional access in Fabric, you need to select several Fabric related Azure services such as Power BI, Azure Data Explorer, Azure SQL Database, and Azure Storage. This overlap of services can be considered too broad for some customers as any policy will be applied to Fabric and the related Azure services.

Licensing

Conditional access requires Microsoft Entra ID P1 licenses. Often these licenses are already available in your organization because they're shared with other Microsoft products such as Microsoft 365. To find the right license for your requirements, see License requirements.

Trusted access to data

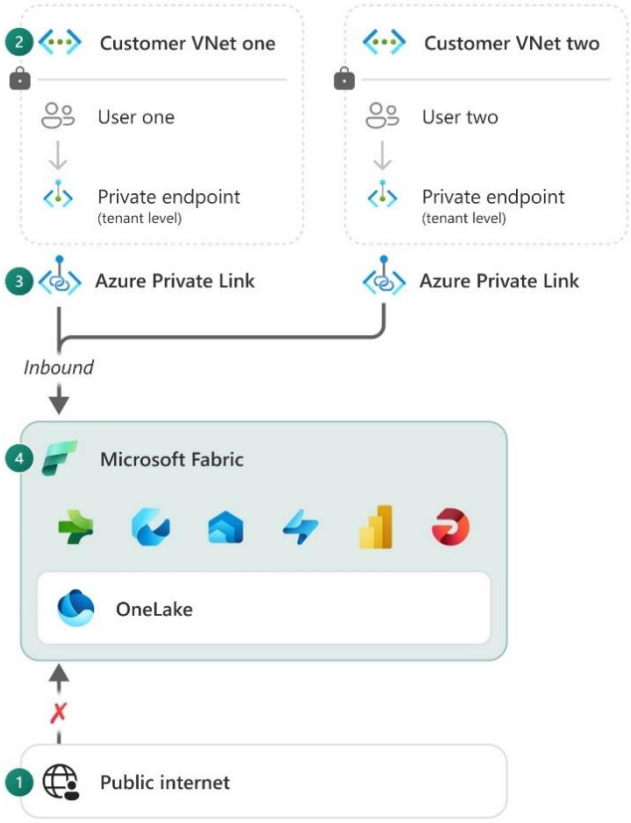
Fabric doesn't need to reside in your private network, even when you have your data stored inside one. With PaaS services, it's common to put the compute in the same private network as the storage account. However, with Fabric this isn't needed. To enable trusted access into Fabric, you can use features such as on-premises Data gateways, Trusted workspace access and managed private endpoints. For more information, see Security in Microsoft Fabric.

Private links

With private endpoints your service is assigned a private IP address from your virtual network. The endpoint allows other resources in the network to communicate with the service over the private IP address.

Using Private links, a tunnel from the service into one of your subnets creates a private channel. Communication from external devices travels from their IP address, to a private endpoint in that subnet, through the tunnel and into the service.

When implementing private links, Fabric is no longer accessible through the public internet. To access Fabric, all users have to connect through the private network. The private network is required for all communications with Fabric, including viewing a Power BI report in the browser and using SQL Server Management Studio (SSMS) to connect to an SQL endpoint.



The architectural diagram depicts the following concepts.

1. Microsoft Fabric is configured to not be accessible to the public internet.
2. The user is connecting from a private network (Expresseroute or Vnet).
3. A private link is set up from the private network to Microsoft Fabric.
4. Now that the user has access to the private network, he can access Microsoft Fabric.

On-premises networks

If you're using on-premises networks, you can extend them to the Azure Virtual Network (VNet) using an ExpressRoute circuit, or a site-to-site VPN, to access Fabric using private connections.

Bandwidth

With private links, all traffic to Fabric travels through the private endpoint, causing potential bandwidth issues. Users are no longer able to load global distributed nondata related resources such as images .css and .html files used by Fabric, from their region. These resources are loaded from the location of the private endpoint.

For example, for Australian users with a US private endpoint, traffic travels to the US first. This increases load times and might reduce performance.

Cost

The cost of private links and the increase of the ExpressRoute bandwidth to allow private connectivity from your network, might add costs to your organization.

Considerations and limitations

With private links you're closing off Fabric to the public internet. As a result, there are considerations and limitations you need to take into account.

Add Fabric URLs to your allowlist

The URLs are divided into two categories: required and optional. The required URLs are necessary for the service to work correctly. The optional URLs are used for specific features that you might not use. To use Fabric, you must be able to connect to the endpoints marked required in the tables in this article, and to any endpoints marked required on the linked sites. If the link to an external site refers to a specific section, you only need to review the endpoints in that section. You can also add endpoints that are marked optional to allowlists for specific functionality to work.

Fabric requires only TCP Port 443 to be opened for the listed endpoints.

The tables in this article use the following conventions:

- Wildcards (*) represent all levels under the root domain.
- N/A is used when information isn't available.

The **Endpoint** column lists domain names and links to external sites, which contain further endpoint information.

Fabric Platform Endpoints

Purpose	Endpoint	Port
Required: Portal	*.fabric.microsoft.com	TCP 443

OneLake

Purpose	Endpoint	Port
For OneLake access for DFS APIs (default Onelake endpoint)	*.onelake.dfs.fabric.microsoft.com	Port 1443

Onelake endpoint for calling Blob APIs	*.onelake.blob.fabric.microsoft.com	TCP 443
Optional: Regional Endpoints for DFS APIs	*<region>-onelake.dfs.fabric.microsoft.com	TCP 443
Optional: Regional Endpoints for Blob APIs	*<region>-onelake.blob.fabric.microsoft.com	TCP 443

Pipeline

Purpose	**Endpoint**	**Port**
For outbound connections		
Required: Portal	*.powerbi.com	TCP 443
Required: Backend APIs for Portal	*.pbidedicated.windows.net	TCP 443
Required: Cloud pipelines	No specific endpoint is required	N/A
Optional: On-premises data gateway login	*.login.windows.net login.live.com aadcdn.msauth.net login.microsoftonline.com *.microsoftonline-p.com See the documentation for Adjust communication settings for the on-premises data gateway	TCP 443
Optional: On-premises data gateway communication	*.servicebus.windows.net	TCP 443 TCP 5671-5672 TCP 9350-9354
Optional: On-premises data gateway pipelines	*.frontend.clouddatahub.net (User can use service tag DataFactory or DataFactoryManagement)	TCP 443
For inbound connections	No specific endpoints other than the customer's data store endpoints required in pipelines and behinds the firewall. (User can use service tag DataFactory, regional tag is supported, like DataFactory.WestUs)	

Lakehouse

Purpose	**Endpoint**	**Port**
Inbound connections	https://cdn.jsdelivr.net/npm/monaco-editor*	N/A

Notebook

Purpose	**Endpoint**	**Port**
Inbound connections (icons)	http://res.cdn.office.net/	N/A

Required: Notebook backend	https://*.pbidedicated.windows.net wss://*.pbidedicated.windows.net (HTTP/WebSocket)	N/A
Required: Lakehouse backend	https://onelake.dfs.fabric.microsoft.com	N/A
Required: Shared backend	https://*.analysis.windows.net	N/A
Required: DE/DS extension UX	https://pbides.powerbi.com	N/A
Required: Notebooks UX	https://aznb-ame-prod.azureedge.net	N/A
Required: Notebooks UX	https://*.notebooks.azuresandbox.ms	N/A
Required: Notebooks UX	https://content.powerapps.com	N/A
Required: Notebooks UX	https://aznbcdn.notebooks.azure.net	N/A

Spark

Purpose	**Endpoint**	**Port**
Inbound connections (icons)	http://res.cdn.office.net/	N/A
Inbound connections (library management for PyPI)	https://pypi.org/*	N/A
Inbound connections (library management for Conda)	local static endpoints for condaPackages	N/A

Data Warehouse

Purpose	**Endpoint**	**Port**
Required: Datamart SQL	datamart.fabric.microsoft.com	1433
Required: Datamart SQL	datamart.pbidedicated.microsoft.com	1433
Required: Fabric DW SQL	datawarehouse.fabric.microsoft.com	1433
Required: Fabric SQL	datawarehouse.pbidedicated.microsoft.com	1433

Data Science

Purpose	**Endpoint**	**Port**
Inbound connections (library management for PyPI)	https://pypi.org/*	N/A
Inbound connections (library management for Conda)	local static endpoints for condaPackages	N/A

KQL Database

Purpose	Endpoint	Port
	https://*.z[0-9].kusto.fabric.microsoft.com	

Eventstream

Purpose	Endpoint	Port
Customers can send/read events from Event stream in their custom app	sb://*.servicebus.windows.net	http: 443 amqp: 5672/5673 kafka: 9093

Add Power BI URLs to your allowlist

The Power BI service requires internet connectivity. The endpoints listed in the following tables should be reachable for customers who use the Power BI service. All endpoints in the Power BI service support HTTP/2.

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

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

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

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

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

Authentication

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

Purpose	Destination	Port

Required: Authentication and identity	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

General site usage

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

Expand table

Purpose	Destination	Port
Required: Backend APIs	api.powerbi.com	TCP 443
Required: Backend APIs	*.analysis.windows.net	TCP 443
Required: Backend APIs	*.pbidedicated.windows.net	TCP 443
Required: Content Delivery Network (CDN)	content.powerapps.com	TCP 443
Required: Datamart SQL	One of the following: • datamart.fabric.microsoft.com • datamart.pbidedicated.windows.net	1433
Required: Microsoft 365 integration	See the documentation for Microsoft 365 Common and Office Online URLs	N/A
Required: Portal	*.powerbi.com	TCP 443
Required: Manage gateways, connections and data policies (preview)	gatewayadminportal.azure.com	TCP 443
Required: Service telemetry	dc.services.visualstudio.com	TCP 443
Optional: Informational messages	arc.msn.com	TCP 443
Optional: NPS surveys	nps.onyx.azure.net	TCP 443

Administration

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

Purpose	Destination	Port

Required: For managing users and viewing audit logs	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

Getting data

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

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

Dashboard and report integration

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

Purpose	Destination	Port
Required: Excel integration	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

Power BI visuals

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

Purpose	Destination	Port
Required: Import a custom visual from the Marketplace interface or from a file	*.powerbi.com *.osi.office.net *.msecnd.net store.office.com store-images.s-microsoft.com visuals.azureedge.net	TCP 443
Optional: Azure Maps	https://atlas.microsoft.com https://us.atlas.microsoft.com https://eu.atlas.microsoft.com	N/A
Optional: Bing Maps	bing.com platform.bing.com r.bing.com *.virtualearth.net	TCP 443
Optional: Esri Maps	*.esri.com *.arcgis.com	TCP 443
Optional: PowerApps	See the Required services section from the PowerApps system requirements site	N/A
Optional: Visio	See the documentation for Microsoft 365 Common and Office Online URLs, as well as SharePoint Online and OneDrive for work or school	N/A

Power BI OneDrive and SharePoint integration

Power BI depends on certain endpoints to support integration with OneDrive for Business and SharePoint Online. You must be able to connect to the endpoints and linked sites in the following table.

Purpose	Destination	Port

Required: OneDrive and SharePoint integration	See the documentation for SharePoint Online and OneDrive for Business URLs	N/A

Related external sites

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

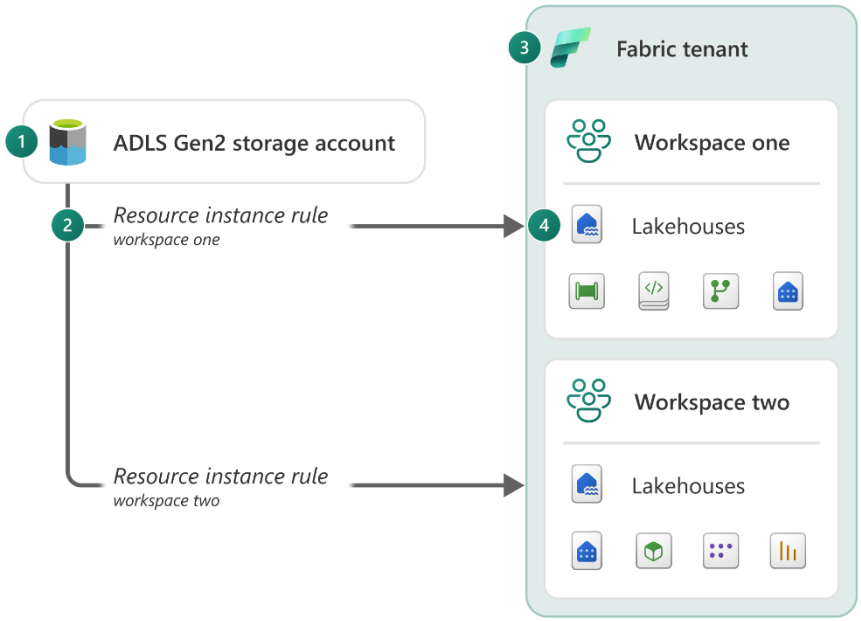
Purpose	Destination	Port
Optional: Community site	community.powerbi.com oxcrx34285.i.lithium.com	TCP 443
Optional: Documentation site	learn.microsoft.com img-prod-cms-rt-microsoft-com.akamaized.net statics-uhf-eas.akamaized.net cdnssl.clicktale.net ing-district.clicktale.net	TCP 443
Optional: Download site (for Power BI Desktop and other products)	download.microsoft.com	TCP 443
Optional: External redirects	aka.ms go.microsoft.com	TCP 443
Optional: Ideas feedback site	ideas.powerbi.com powerbi.uservoice.com	TCP 443
Optional: Power BI site - landing page, learn more links, support site, download links, partner showcase, and so on.	powerbi.microsoft.com	TCP 443
Optional: Power BI Developer Center	dev.powerbi.com	TCP 443
Optional: Support site	support.powerbi.com s3.amazonaws.com *.olark.com logx.optimizely.com mscom.demdex.net tags.tiqcdn.com	TCP

Outbound network security

Fabric has a set of tools that allow you to connect to external data sources and bring that data into Fabric in a secure way. This section lists different ways to import and connect to data from a secure network into fabric.

Trusted workspace access

With Fabric you can access firewall enabled Azure Data Lake Gen 2 accounts securely. Fabric workspaces that have a workspace identity can securely access Azure Data Lake Gen 2 accounts with public network access enabled, from selected virtual networks and IP addresses. You can limit ADLS gen 2 access to specific Fabric workspaces. For more information, see Trusted workspace access.



The architectural diagram depicts the following concepts.

1. The Azure Data Lake Gen 2 account has network access enabled from selected virtual networks and IP addresses. This means it is closed off from the public internet.
2. A resource instance rule can be set up in the Azure portal to allow access from specific Fabric workspaces.
3. Only the workspace configured in the Fabric to have access to the Azure Data Lake Gen 2 account will have access.
4. The workspace can now create a shortcut to the ADLS account or you can create a data pipeline to access the data directly in Fabric.

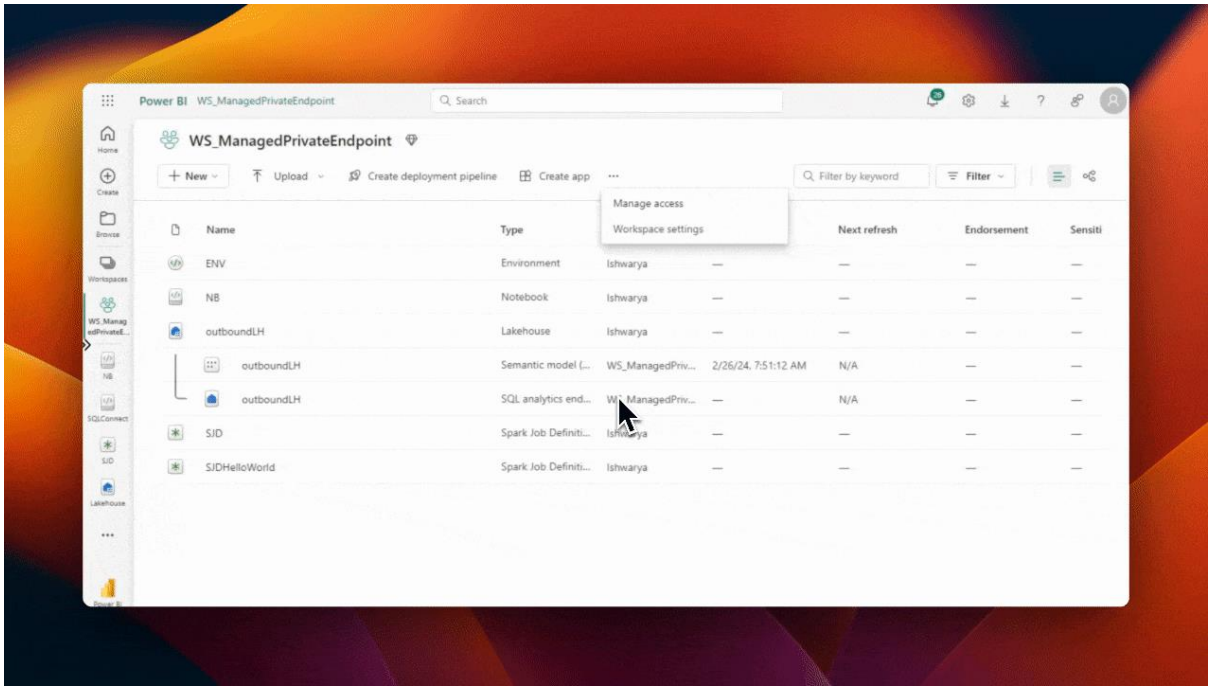
Managed Private Endpoints

Managed private endpoints allow secure connections to data sources such as ADLS Gen 2 or Azure SQL databases without exposing them to the public network or requiring complex network configurations.

Managed private endpoints are feature that allows secure and private access to data sources from certain Fabric workloads.

What are Managed Private Endpoints?

- Managed private endpoints are connections that workspace admins can create to access data sources that are behind a firewall or that are blocked from public internet access.
- Managed private endpoints allow Fabric workloads to securely access data sources without exposing them to the public network or requiring complex network configurations.
- Microsoft Fabric creates and manages managed private endpoints based on the inputs from the workspace admin. Workspace admins can set up managed private endpoints from the workspace settings by specifying the resource ID of the data source, identifying the target subresource, and providing a justification for the private endpoint request.
- Managed private endpoints support various data sources, such as Azure Storage, Azure SQL Database and many more.



Note

Managed private endpoints are supported for Fabric trial capacity and all Fabric F SKU capacities.

For more information about supported data sources for managed private endpoints in Fabric, see [Supported data sources](#).

Supported item types

- Fabric Spark workloads: This includes notebooks, lakehouses, and Spark job definitions. For more information, see Create and use managed private endpoints.
- Eventstream: For more information, see Connect to Azure resources securely using managed private endpoints (Preview).

Limitations and considerations

- **Tenant Region Compatibility**: Managed private endpoints function only in regions where Fabric Data Engineering workloads are available. Creating them in unsupported Fabric Tenant home regions results in errors. These unsupported Tenant home regions include:

Expand table

Region
Singapore
Israel Central
Switzerland West
Italy North
West India
Mexico Central
Qatar Central
Spain Central
Brazil South

- **Capacity Region Compatibility**: Creating managed private endpoints in unsupported capacity regions results in errors. These unsupported regions include:

Region
West Central US
Switzerland West
Italy North
Qatar Central
West India
France South
Germany North
Japan West
Korea South

Region
South Africa West
UAE Central
Brazil South
Singapore
Central US

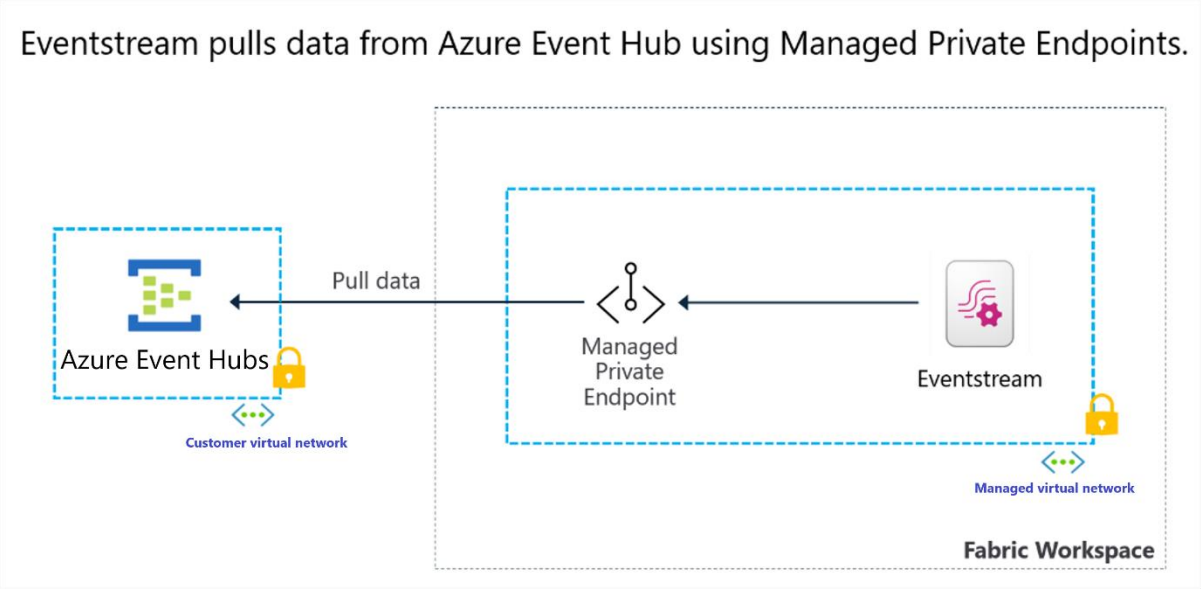
- **Limitations for specific workloads**:
  - Spark: See Create and use managed private endpoints.
  - Eventstream: Connect to Azure resources securely using managed private endpoints (Preview).
- **Workspace migration**: Workspace migration across capacities in different regions is unsupported.
- **OneLake shortcuts** do not yet support connections to ADLS Gen2 storage accounts using managed private endpoints.
- Creating a managed private endpoint with a fully qualified domain name (FQDN) is not supported.

These limitations and considerations might affect your use cases and workflows. Take them into account before enabling the Azure Private Link tenant setting for your tenant.

Connect to Azure resources securely using managed private endpoints

Managed Private Endpoint is a network security feature of the Fabric platform that allows Fabric items to securely access data sources behind a firewall or not accessible from the public internet. By integrating Eventstream with the Managed Private Endpoint, a managed VNet is automatically created for Eventstream, allowing you to securely connect to your Azure resources within a private network. This ensures that your data is securely transmitted over a private network.

The following diagram shows a sample architecture for connecting Eventstream to Azure event hub within a virtual network:



Supported regions and data sources

- **Supported regions for Eventstream managed VNet**: Only selected Fabric tenant regions are supported for Eventstream managed VNet. These regions include:
    - Australia Southeast
    - East US
    - Canada Central
    - East US 2
    - North Central US
    - North Europe
    - West Europe
    - West US
- **Supported data sources**: In alignment with the Managed Private Endpoints in Fabric, Eventstream only supports private connections for the following Azure resources:
    - **Azure Event Hubs**
    - **Azure IoT Hub**

To learn more about the Managed Private Endpoints and supported data sources, visit Managed Private Endpoints for Fabric.

Connect to Azure Event Hubs using a managed private endpoint

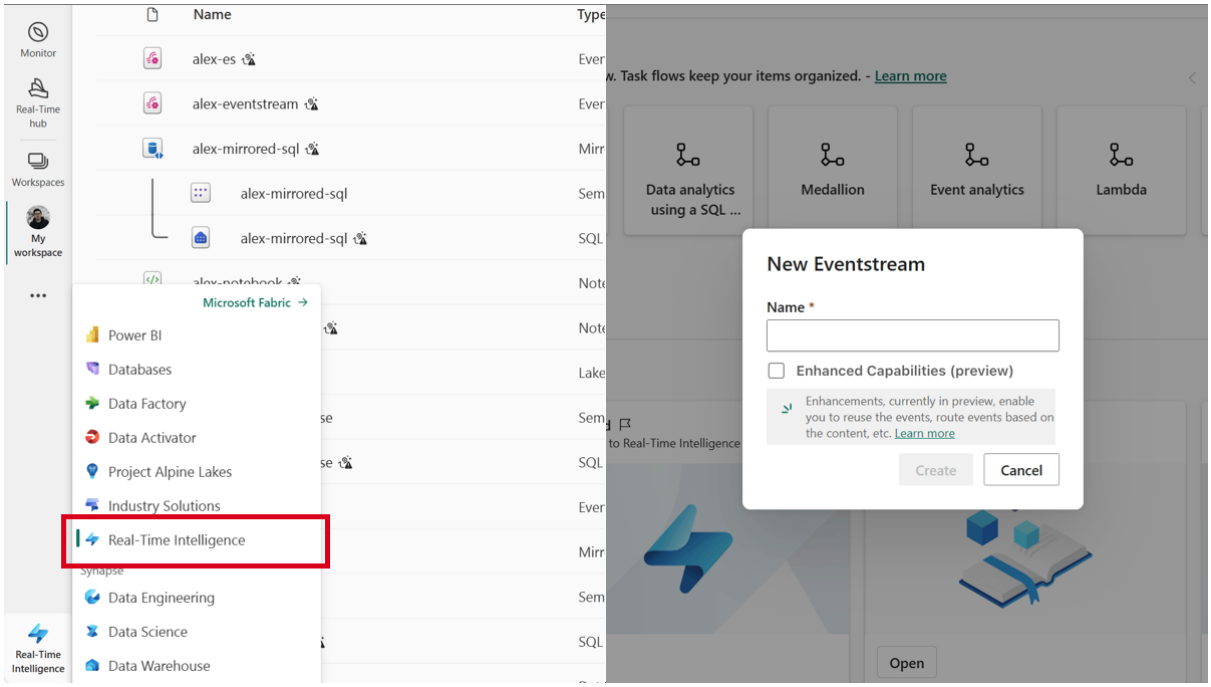
Setting up a private connection in Eventstream is straightforward. Follow these steps to create a managed private endpoint for an Azure event hub and stream data to Eventstream over private network.

Prerequisites

- Managed private endpoints are supported for **Fabric trial** and **all Fabric F SKU** capacities.
- Only users with **Workspace Admin** permissions can create Managed Private Endpoints
- An Azure event hub with public access disabled, and its **Resource ID** ready for creating a private endpoint.
- A Fabric tenant region that supports managed VNet for Eventstream.

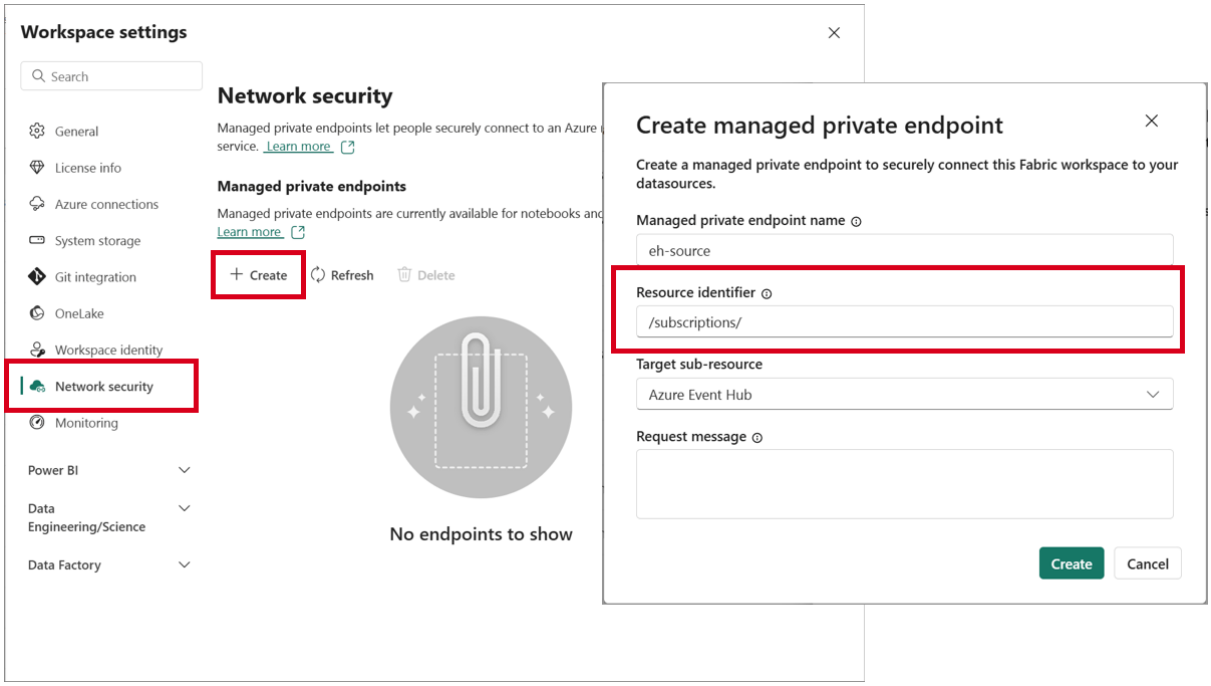
Step 1: Create an eventstream

- Switch your Power BI experience to **Real-time Intelligence**.
- Navigate to the **Eventstream** section and select **Create**. Name your Eventstream such as "eventstream-1."



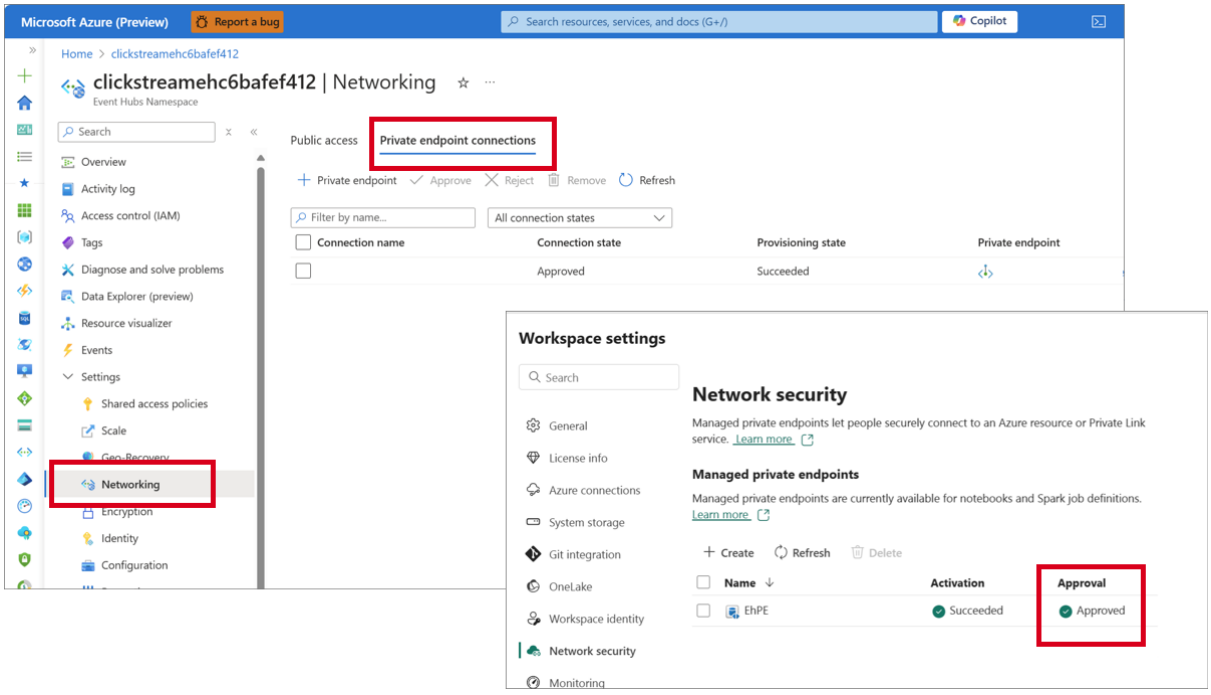
Step 2: Create a private endpoint

- In the Fabric workspace, go to the **Workspace settings** and navigate to the **Network security** section.
- Select **Create** to add a new private endpoint.
- Enter the resource ID of your Azure Event Hubs.



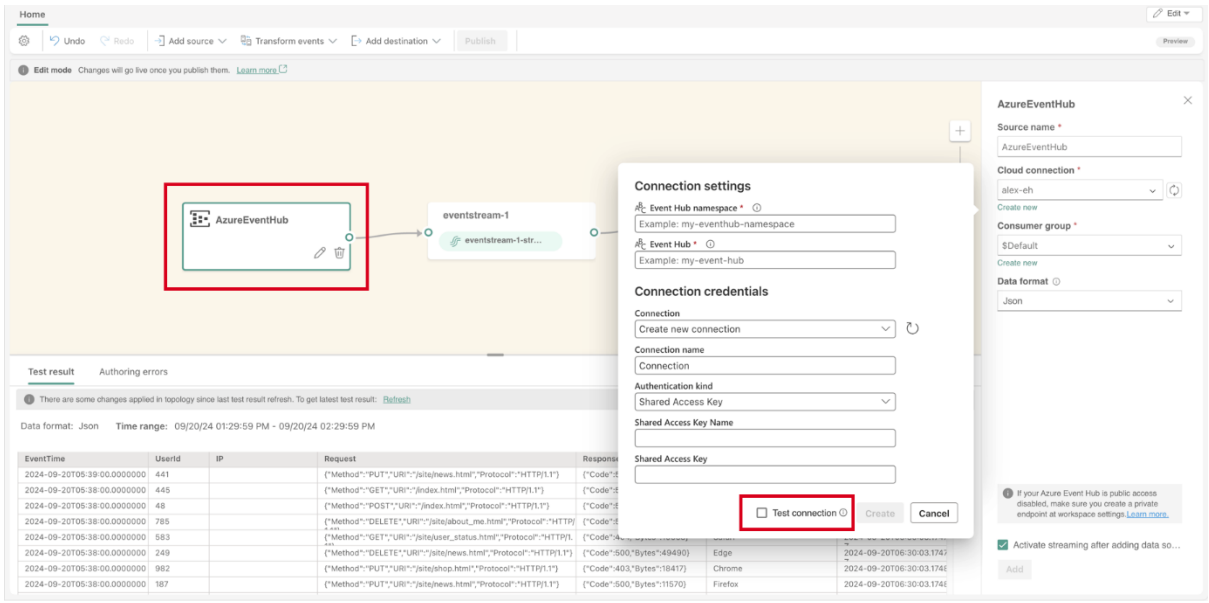
Step 3: Approve the private endpoint in Azure Event Hubs

- Go to the Azure portal and open your Azure event hub.
- In the **Networking** section, navigate to the **Private endpoint connections** tab.
- Locate the private endpoint request from your Fabric workspace and approve it.
- Once approved, the managed private endpoint status updates to **Approved**.

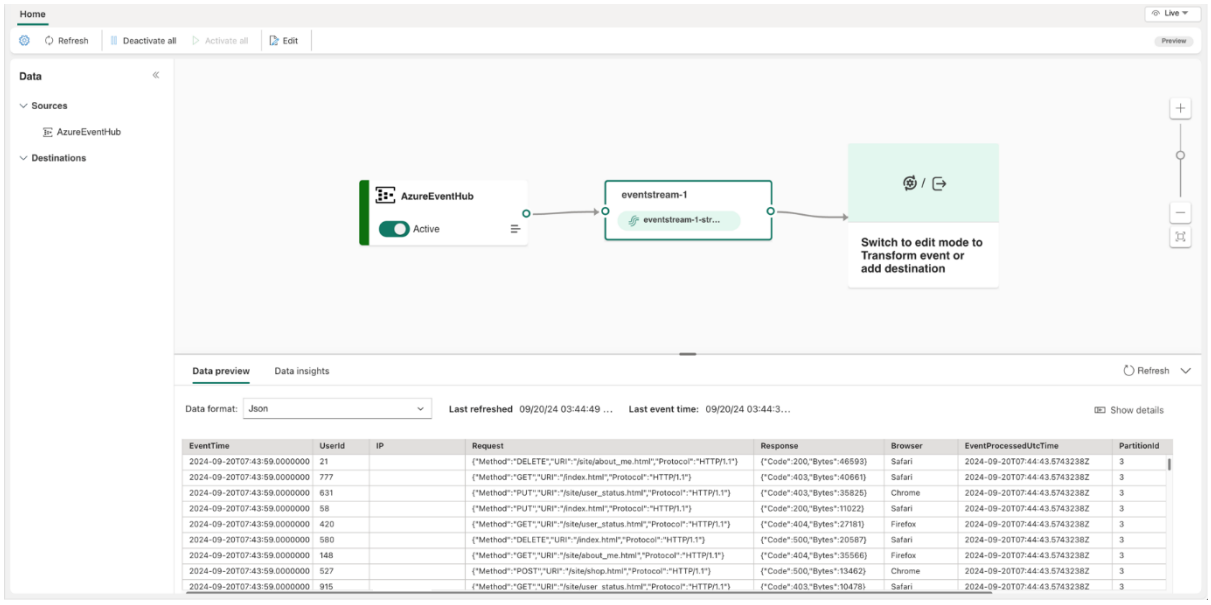


Step 4: Add an Azure Event Hubs source to Eventstream

- Go back to the eventstream you created in Fabric.
- Select **Azure Event Hubs** and add it as a source to your Eventstream.
- When creating a new connection to your Azure event hub, uncheck the **Test connection** option if your event hub is not publicly accessible.
- Manually enter the **Consumer group**.



Once added, Eventstream starts pulling data from your Azure event hub over the private network.

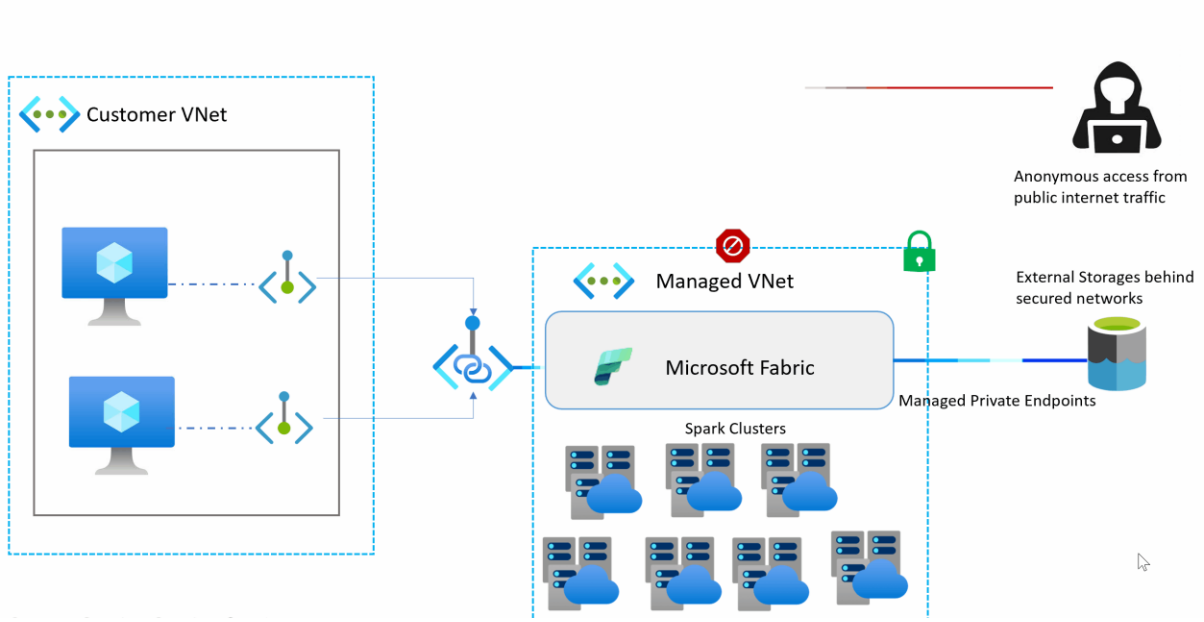


By following these steps, you have a fully operational Eventstream running over a secure private network, using the managed private endpoint to ensure secure data streaming.

Managed virtual networks

Managed virtual networks are virtual networks that are created and managed by Microsoft Fabric for each Fabric workspace. Managed virtual networks provide network isolation for Fabric Spark workloads, meaning that the compute clusters are deployed in a dedicated network and are no longer part of the shared virtual network.

Managed virtual networks also enable network security features such as managed private endpoints, and private link support for Data Engineering and Data Science items in Microsoft Fabric that use Apache Spark.



Fabric workspaces that are provisioned with a dedicated virtual network provide you with value in three ways:

- With a managed virtual network you get complete network isolation for the Spark clusters running your Spark jobs (which allow users to run arbitrary user code) while offloading the burden of managing the virtual network to Microsoft Fabric.
- You don't need to create a subnet for the Spark clusters based on peak load, as this is managed for you by Microsoft Fabric.
- A managed virtual network for your workspace, along with managed private endpoints, allows you to access data sources that are behind firewalls or otherwise blocked from public access.

Data gateway

To connect to on-premises data sources or a data source that might be protected by a firewall or a virtual network, you can use one of these options:

- On-premises data gateway - The gateway acts as a bridge between your on-premises data sources and Fabric. The gateway is installed on a server within your network, and it allows Fabric to connect to your data sources through a secure channel without the need to open ports or make changes to your network.
- Virtual network (VNet) data gateway - The VNet gateway allows you to connect from Microsoft Cloud services to your Azure data services within a VNet, without the need of an on-premises data gateway.

Connect to OneLake from an existing service

You can connect to Fabric using your existing Azure Platform as a Service (PaaS) service. For Synapse and Azure Data Factory (ADF) you can use Azure Integration Runtime (IR) or Azure Data Factory managed virtual network. You can also connect to these services and other services such as Mapping data flows, Synapse Spark clusters, Databricks Spark clusters and Azure HDInsight using OneLake APIs.

Azure service tags

Use service Tags to ingest data without the use of data gateways, from data sources deployed in an Azure virtual network, such as Azure SQL Virtual Machines (VMs), Azure SQL Managed Instance (MI) and EST APIs. You can also use service tags to get traffic from a virtual network or an Azure firewall. For example, service tags can allow outbound traffic to Fabric so that a user on a VM can connect to Fabric SQL endpoints from SSMS, while blocked from accessing other public internet resources.

IP allowlists

If you have data that doesn't reside in Azure, you can enable an IP allowlist on your organization's network to allow traffic to and from Fabric. An IP allowlist is useful if you need to get data from data sources that don't support service tags, such as on-premises data sources. With these shortcuts, you can get data without copying it into OneLake using a Lakehouse SQL endpoint or Direct Lake.

You can get the list of Fabric IPs from Service tags on-premises. The list is available as a JSON file, or programmatically with REST APIs, PowerShell, and Azure Command-Line Interface (CLI).

Workspace identity

A Fabric workspace identity is an automatically managed service principal that can be associated with a Fabric workspace. Fabric workspaces with a workspace identity can securely read or write to firewall-enabled Azure Data Lake Storage Gen2 accounts through trusted workspace access for OneLake shortcuts. Fabric items can use the identity when connecting to resources that support Microsoft Entra authentication. Fabric uses workspace identities to obtain Microsoft Entra tokens without the customer having to manage any credentials.

Workspace identities can be created in the workspace settings of any workspace except My workspaces. A workspace identity is automatically assigned the workspace contributor role and has access to workspace items.

When you create a workspace identity, Fabric creates a service principal in Microsoft Entra ID to represent the identity. An accompanying app registration is also created. Fabric automatically manages the credentials associated with workspace identities, thereby preventing credential leaks and downtime due to improper credential handling.

Note

> Fabric workspace identity is **generally available**. You can create a workspace identity in any workspace except **My workspace**.

While Fabric workspace identities share some similarities with Azure managed identities, their lifecycle, administration, and governance are different. A workspace identity has an independent lifecycle that is managed entirely in Fabric. A Fabric workspace can optionally be associated with an identity. When the workspace is deleted, the identity gets deleted. The name of the workspace identity is always the same as the name of the workspace it's associated with.

Authenticate with workspace identity

A Fabric workspace identity is an automatically managed service principal that can be associated with a Fabric workspace. You can use the workspace identity as an authentication method when connecting Fabric items in the workspace to resources that support Microsoft Entra authentication. Workspace identity is a secure authentication method as there is no need to manage keys, secrets, and certificates. When you grant the workspace identity with permissions on target resources such as ADLS gen 2, Fabric can use the identity to obtain Microsoft Entra tokens to access the resource.

Trusted access to Storage accounts and authentication with workspace identity can be combined together. You can use workspace identity as the authentication method to access storage accounts that have public access restricted to selected virtual networks and IP addresses.

This article describes how to use the workspace identity to authenticate when connecting OneLake shortcuts and data pipelines to data sources. The target audience is data engineers and anyone interested in establishing a secure connection between Fabric items and data sources.

Step 1: Create the workspace identity

You must be a workspace admin to be able to create and manage a workspace identity.

1. Navigate to the workspace and open the workspace settings.
2. Select the **Workspace identity** tab.
3. Select the **+ Workspace identity** button.

When the workspace identity has been created, the tab displays the workspace identity details and the list of authorized users.

Workspace identity can be created and deleted by workspace admins. The workspace identity has the workspace contributor role on the workspace. Admins, members, and contributors in the workspace can configure the identity as the authentication method in Azure Data Lake Storage (ADLS) Gen2 connections that are used in data pipelines and shortcuts.

For more detail, see Create and manage a workspace identity.

Step 2: Grant the identity permissions on the storage account

1. Sign in to the Azure portal and navigate to the storage account you want to access from OneLake.
2. Select the Access control (IAM) tab on the left sidebar and select **Role assignments**.
3. Select the **Add** button and select **Add role assignment**.
4. Select the role you want to assign to the identity, such as *Storage Blob Data Reader* or *Storage Blob Data Contributor*.

Note

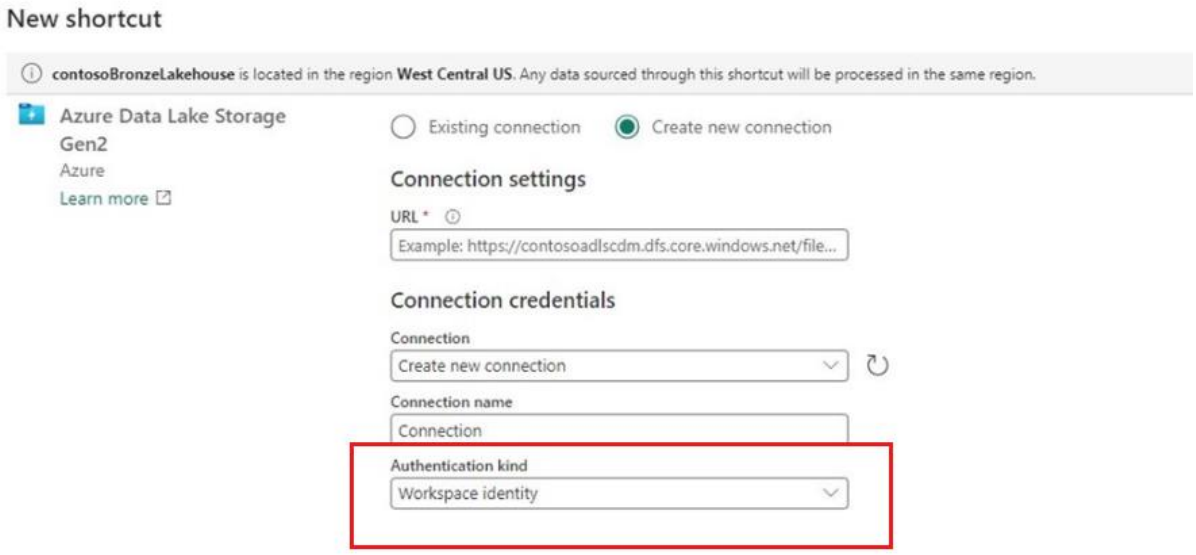
The role must be provided at the Storage account level.

5. Select **Assign access to User, group, or service principal**.
6. Select **+ Select members**, and search by name or app ID of the workspace identity. Select the identity associated with your workspace.
7. Select **Review + assign** and wait for the role assignment to be completed.

Step 3: Create the Fabric item

OneLake shortcut

Follow the steps listed in Create an Azure Data Lake Storage Gen2 shortcut. Select workspace identity as the authentication method (supported only for ADLS Gen2).



Data pipelines with Copy, Lookup, and GetMetadata activities

Follow the steps listed in Module 1 - Create a pipeline with Data Factory to create the data pipeline. Select workspace identity as the authentication method (supported only for ADLS Gen2 and for Copy, Lookup, and GetMetadata activities).

Note

The user creating the shortcut with workspace identity must have an admin, member or contributor role in the workspace. Users accessing the shortcuts only need permissions on the lakehouse.

Known issues

Write to shortcut destination fails when using workspace identity as the authentication method.

Considerations and limitations

- Workspace identity can be created in workspaces associated with any capacity (except for My workspaces).
- Workspace identity can be used for authentication in any capacity that supports OneLake shortcuts and data pipelines.
- Trusted workspace access to firewall-enabled Storage accounts is supported in any F capacity.
- You can create ADLS Gen 2 connections with workspace-identity-based authentication in the Manage Gateways and Connections experience.
- Connections with workspace-identity-authentication can only be used in Onelake shortcuts and data pipelines.
- Checking the status of a connection that has workspace identity as the authentication method isn't supported.

Workload specific security.

As we have mentioned before the Fabric platform comprises a series of services and infrastructure components that support the common functionality for all Fabric experiences. Collectively, they offer a comprehensive set of analytics experiences designed to work together seamlessly. Experiences include Lakehouse, Data Factory, Synapse Data Engineering, Synapse Data Warehouse, Power BI, and others.

This section discusses individual experiences and how they are secured by Microsoft.

Power BI

Power BI platform

Power BI is an online software service (*SaaS*, or Software as a Service) offering as part of Microsoft Fabric that lets you easily and quickly create self-service Business Intelligence dashboards, reports, semantic models, and visualizations. With Power BI, you can connect to many different data sources, combine and shape data from those connections, then create reports and dashboards that can be shared with others.

This section outlines Power BI data handling practices when it comes to storing, processing, and transferring customer data.

Data at rest

Power BI uses two primary data storage resource types:

- Azure Storage
- Azure SQL Databases

In most scenarios, Azure Storage is utilized to persist the data of Power BI artifacts, while Azure SQL Databases are used to persist artifact metadata.

All data persisted by Power BI is encrypted by default using Microsoft-managed keys. Customer data stored in Azure SQL Databases is fully encrypted using Azure SQL's Transparent Data Encryption (TDE) technology. Customer data stored in Azure storage is encrypted using Azure Storage Encryption.

Optionally, organizations can utilize Power BI Premium to use their own keys to encrypt data at rest that is imported into a semantic model. This approach is often described as bring your own key (BYOK). Utilizing BYOK helps ensure that even in case of a service operator error, customer data won't be exposed – something that

can't easily be achieved using transparent service-side encryption. See Bring your own encryption keys for Power BI for more information.

Power BI semantic models allow for various data source connection modes that determine whether the data source data is persisted in the service or not.

Expand table

Semantic Model Mode (Kind)	Data Persisted in Power BI
Import	Yes
DirectQuery	No
Live Connect	No
DirectLake	No (stored in Onelake)
Composite	If contains an Import data source
Streaming	If configured to persist

Regardless of the semantic model mode utilized, Power BI may temporarily cache any retrieved data to optimize query and report load performance.

Data in processing

Data is in processing when it's either actively being used by one or more users as part of an interactive scenario, or when a background process, such as refresh, touches this data. Power BI loads actively processed data into the memory space of one or more service workloads. To facilitate the functionality required by the workload, the processed data in memory isn't encrypted.

Power BI embedded analytics

Independent Software Vendors (ISVs) and solution providers have two main modes of embedding Power BI artifacts in their web applications and portals: embed for your organization and embed for your customers. The artifact is embedded into an IFrame in the application or portal. An IFrame is not allowed to read or write data from the external web application or portal, and the communication with the IFrame is done by using the Power BI Client SDK using POST messages.

In an embed for your organization scenario, Microsoft Entra or through customized portals.ITs. All Power BI policies and capabilities described in this paper such as Row Level Security (RLS) and object-level security (OLS) are automatically applied to all users independently of whether they access Power BI through the Power BI portal or through customized portals.

In an embed for your customers scenario, ISVs typically own Power BI tenants and Power BI items (dashboards, reports, semantic models, and others). It's the

responsibility of an ISV back-end service to authenticate its end users and decide which artifacts and which access level is appropriate for that end user. ISV policy decisions are encrypted in an embed token generated by Power BI and passed to the ISV back-end for further distribution to the end users according to the business logic of the ISV. End users using a browser or other client applications aren't able to automatically append the encrypted embed token to Power BI requests as an *Authorization: EmbedToken* header. Based on this header, Power BI will enforce all policies (such as access or RLS) precisely as was specified by the ISV during generation.Power BI Client APIs automatically append the encrypted embed token to Power BI requests as an *Authorization: EmbedToken* header. Based on this header, Power BI will enforce all policies (such as access or RLS) precisely as was specified by the ISV during generation.

To enable embedding and automation, and to generate the embed tokens described above, Power BI exposes a rich set of REST APIs. These Power BI REST APIs support both user delegated and service principal Microsoft Entra methods of authentication and authorization.

Power BI embedded analytics and its REST APIs support all Power BI network isolation capabilities described in this article: For example, Service Tags and Private Links.

Paginated reports

Paginated reports are designed to be printed or shared. They're called paginated because they're formatted to fit well on a page. They display all the data in a table, even if the table spans multiple pages. You can control their report page layout exactly.

Paginated reports support rich and powerful expressions written in Microsoft Visual Basic .NET. Expressions are widely used throughout Power BI Report Builder paginated reports to retrieve, calculate, display, group, sort, filter, parameterize, and format data.

Expressions are created by the author of the report with access to the broad range of features of the .NET framework. The processing and execution of paginated reports is performed inside a sandbox.

Paginated report definitions (.rdl section.Authentication to the Power BI Service section.

The Microsoft Entra token obtained during the authentication is used to communicate directly from the browser to the Power BI Premium cluster.

In Power BI Premium, the Power BI service runtime provides an appropriately isolated execution environment for each report render.

A paginated report can access a wide set of data sources as part of the rendering of the report. The sandbox doesn't communicate directly with any of the data sources but instead communicates with the trusted process to request data, and then the trusted process appends the required credentials to the connection. In this way, the sandbox never has access to any credential or secret.

In order to support features such as Bing maps, or calls to Azure Functions, the sandbox does have access to the internet.

Power BI Mobile

Power BI Mobile is a collection of apps designed for the primary mobile platforms: Android, iOS. Security considerations for the Power BI Mobile apps fall into two categories:

- Device communication
- The application and data on the device

For device communication, all Power BI Mobile applications communicate with the Power BI service, and use the same connection and authentication sequences used by browsers, which are described in detail earlier in this white paper. The Power BI mobile applications for iOS and Android bring up a browser session within the application itself.

Power BI Mobile supports certificate-based authentication (CBA) when authenticating with Power BI (sign in to service), SSRS ADFS on-premises (connect to SSRS server) and SSRS App Proxy on either iOs or Android.

Power BI Mobile apps actively communicate with the Power BI service. Telemetry is used to gather mobile app usage statistics and similar data, which is transmitted to services that are used to monitor usage and activity; no customer data is sent with telemetry.

The Power BI application stores data on the device that facilitates use of the app:

- Microsoft Entra ID and refresh tokens are stored in a secure mechanism on the device, using industry-standard security measures.
- Data and settings (key-value pairs for user configuration) is cached in storage on the device and can be encrypted by the OS. In iOS this is automatically done when the user sets a passcode. In Android this can be configured in the settings. T data and settings (key-value pairs for

user configuration) are cached in storage on the device in a sandbox and internal storage that is accessible only to the app.
- Geolocation is enabled or disabled explicitly by the user. If enabled, geolocation data isn't saved on the device and isn't shared with Microsoft.
- Notifications are enabled or disabled explicitly by the user. If enabled, Android and iOS don't support geographic data residency requirements for notifications.

Data encryption can be enhanced by applying file-level encryption via Microsoft Intune, a software service that provides mobile device and application management. Both platforms for which Power BI Mobile is available support Intune. With Intune enabled and configured, data on the mobile device is encrypted, and the Power BI application itself can't be installed on an SD card. Learn more about Microsoft Intune.

In order to implement SSO, some secured storage values related to the token-based authentication are available for other Microsoft first party apps (such as Microsoft Authenticator) and are managed by the Microsoft Authentication Library (MSAL).

Power BI Mobile cached data is deleted when the app is removed, when the user signs out of Power BI Mobile, or when the user fails to sign in (such as after a token expiration event or password change). The data cache includes dashboards and reports previously accessed from the Power BI Mobile app.

Power BI Mobile doesn't access other application folders or files on the device.

The Power BI apps for iOS and Android let you protect your data by configuring additional identification, such as providing Face ID, Touch ID, or a passcode for iOS, and biometric ID (Fingerprint ID) for Android. Learn more about additional identification. Users can also configure their app to require identification each time the app is brought to the foreground using Face Id, touch id or passcode.

On-premises data gateway

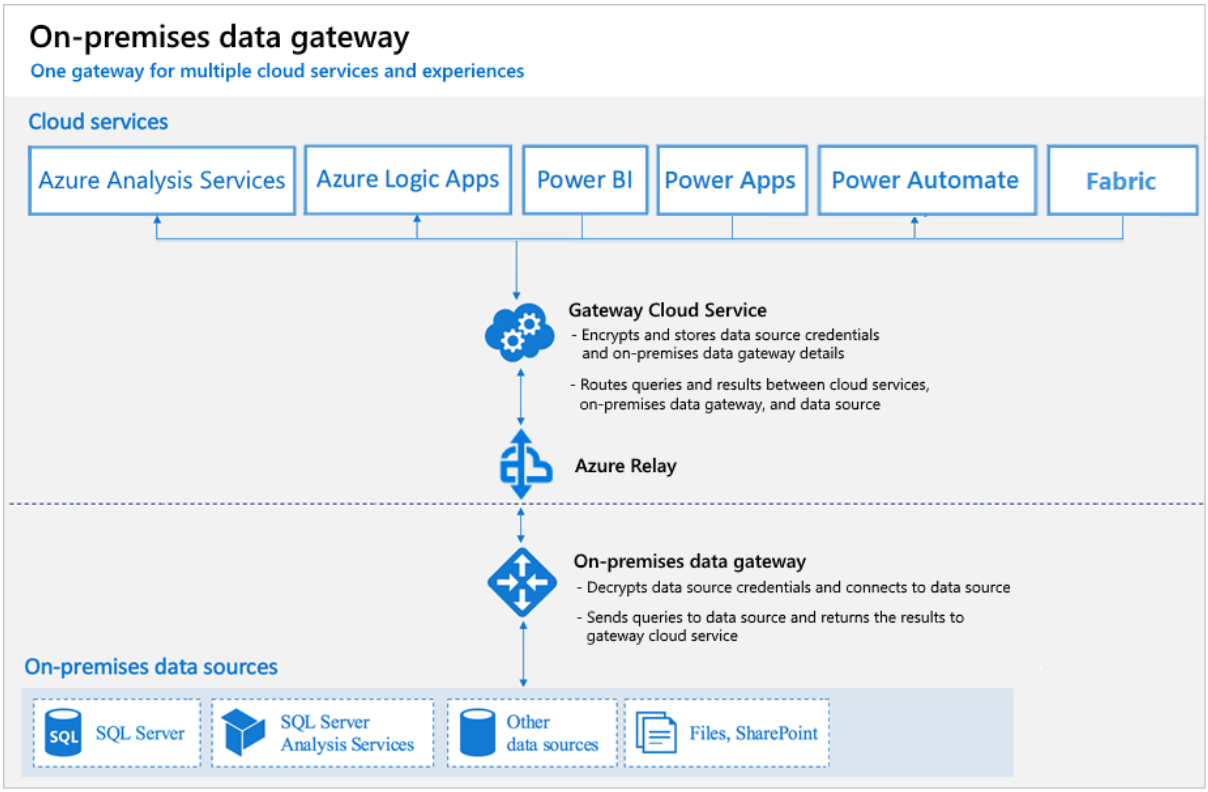
Users in your organization can access on-premises data to which they already have access authorization from services in the cloud like Power BI, Power Platform, and Microsoft Fabric. But before those users can connect the cloud service to your on-premises data source, an on-premises data gateway needs to be installed and configured.

The gateway facilitates quick and secure behind-the-scenes communication. This communication flows from a user in the cloud to your on-premises data source and then back to the cloud.

An admin is usually the one who installs and configures a gateway. These actions might require special knowledge of your on-premises servers or Server Administrator permissions.

This article doesn't provide step-by-step guidance on how to install and configure the gateway. For that guidance, go to Install an on-premises data gateway. This article does provide in-depth understanding of how the gateway works.

How the gateway works



Let's first look at what happens when you interact with an element that is connected to an on-premises data source.

Note: Depending on the cloud service, you might need to configure a data source for the gateway.

1. The cloud service creates a query and the encrypted credentials for the on-premises data source. The query and credentials are sent to the gateway queue for processing when the gateway polls the service

periodically. For more information about credential encryption in Power BI, go to Power BI security whitepaper.

2. The gateway cloud service analyzes the query and pushes the request to Azure Relay.
3. Azure Relay sends the pending requests to the gateway when it polls periodically. Both the gateway and Power BI service are implemented to only accept TLS 1.2 traffic.
4. The gateway gets the query, decrypts the credentials, and connects to one or more data sources with those credentials.
5. The gateway sends the query to the data source to be run.
6. The results are sent from the data source back to the gateway and then to the cloud service. The service then uses the results.

In step 6, queries like Power BI and Azure Analysis Services refreshes can return large amounts of data. For such queries, data is temporarily stored on the gateway machine. This data storage continues until all data is received from the data source. The data is then sent back to the cloud service. This process is called spooling. We recommend you use a solid-state drive (SSD) as the spooling storage.

Authentication to on-premises data sources

A stored credential is used to connect from the gateway to on-premises data sources. Regardless of the user, the gateway uses the stored credential to connect. But there might be authentication exceptions like DirectQuery and LiveConnect for Analysis Services in Power BI. For more information about credential encryption in Power BI, go to Power BI security whitepaper.

Sign-in account

You sign in with either a work account or a school account. This account is your organization account. If you signed up for an Office 365 offering and didn't supply your actual work email address, your account name might look like nancy@contoso.onmicrosoft.com. A cloud service stores your account within a tenant in Microsoft Entra ID. In most cases, the User Principal Name (UPN) of your Microsoft Entra ID account matches your email address.

Network traffic security

Traffic goes from the gateway to Azure Relay to the Power BI backend cluster. This traffic doesn't traverse the public internet. All Azure internal traffic goes over the Azure backbone.

Microsoft Entra ID

Microsoft cloud services use Microsoft Entra ID to authenticate users. Microsoft Entra ID is the tenant that contains usernames and security groups. Typically, the email address that you use for sign-in is the same as the UPN of your account. For more information about authentication in Power BI, go to Power BI security whitepaper.

Keys and credential management

During gateway installation and configuration, the administrator types in a gateway **Recovery Key**. That **Recovery Key** is used to generate a strong AES symmetric key. An RSA asymmetric key is also created at the same time.

Those generated keys (RSA and AES) are stored in a file located on the local machine. That file is also encrypted. The contents of the file can only be decrypted by that particular Windows machine, and only by that particular gateway service account.

When a user enters data source credentials in the Power BI service UI, the credentials are encrypted with the public key in the browser. The gateway decrypts the credentials using the RSA private key and re-encrypts them with an AES symmetric key before the data is stored in the Power BI service. With this process, the Power BI service never has access to the unencrypted data.

Virtual network data gateway

The virtual network (VNet) data gateway facilitates secure connectivity to data sources associated with your VNet.

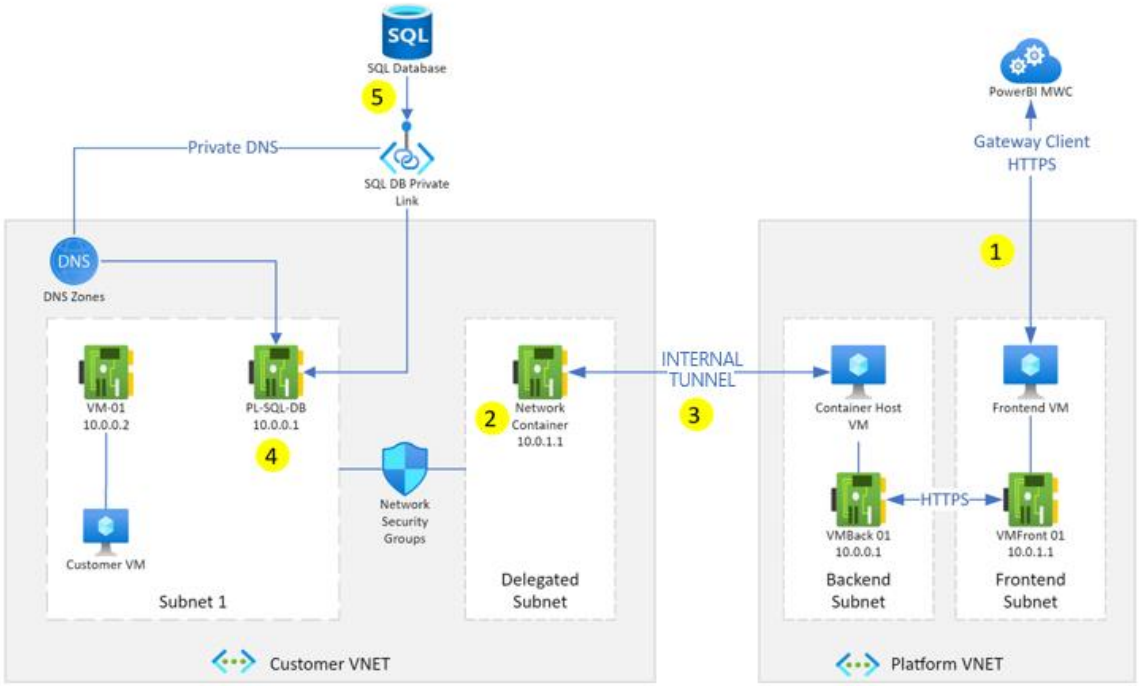
Users in your organization can access data secured by a VNet to which they already have access. But before these users can connect to these data sources from Microsoft Cloud services, a VNet gateway needs to be registered and configured.

Let's first look at what happens when you interact with a Power BI report that's connected to a data source within a VNet.

1. Power BI cloud service (or one of the other supported cloud services) kicks off a query and sends the query, data source details, and credentials to the Microsoft Power Platform VNet service.
2. The Microsoft Power Platform VNet then securely injects a container running the VNet data gateway into the subnet. This VNet data gateway can now connect to data services accessible from within this subnet.
3. The Microsoft Power Platform VNet service then sends the query, data source details, and credentials to the VNet data gateway.

4. The VNet data gateway gets the query and connects to the data sources with those credentials.
5. The query is then sent to the data source for execution.
6. After execution, the results are sent to the VNet data gateway and the Microsoft Power Platform VNet service securely pushes the data from the container to the cloud service.

Here's a network diagram illustrating the data pathway between Power BI cluster and a SQL database data source:



When the workload starts up, the VNet data gateway leases an IP from the delegated subnet, which means it's obeying the network security group (NSG) and network address translation (NAT) rules on the target VNet. Traffic going through this IP address obeys all NSG rules that are applied to the subnet.

The VNet gateway doesn't require any Service Endpoint or open ports back to Power BI. Data from the VNet is returned to Power BI by an internal Microsoft tunnel that doesn't reach the public internet, which uses Automatic Private IP Addressing (APIPA) and exists on the infrastructure virtual machine.

Note: All traffic uses the Azure backbone, including the internal Microsoft tunnel.

Hardware

Each instance of the VNet data gateway has a maximum capacity of:

- 2 cores
- 8 GB of RAM each

At this time, this is the only available hardware configuration and it can't be scaled or changed.

VNet region and data transfer

The VNet data gateway must be created in the home region of the tenant to work with Power BI. However, when creating it, you can choose an Azure VNet and subnet from any region. Your data will go to this subnet and only metadata is ever moved to the home region.

Privacy, security, and responsible use for Copilot

With Copilot and other generative AI features in preview, Microsoft Fabric brings a new way to transform and analyze data, generate insights, and create visualizations and reports.

Before your business starts using Copilot in Fabric, you may have questions about how it works, how it keeps your business data secure and adheres to privacy requirements, and how to use generative AI responsibly.

Note

- Your administrator needs to enable the tenant switch before you start using Copilot. See the article **Copilot tenant settings** for details.
- Your F64 or P1 capacity needs to be in one of the regions listed in this article, **Fabric region availability**.
- If your tenant or capacity is outside the US or France, Copilot is disabled by default unless your Fabric tenant admin enables the **Data sent to Azure OpenAI can be processed outside your tenant's geographic region, compliance boundary, or national cloud instance** tenant setting in the Fabric Admin portal.
- Copilot in Microsoft Fabric isn't supported on trial SKUs. Only paid SKUs (F64 or higher, or P1 or higher) are supported.
- Copilot in Fabric is currently rolling out in public preview and is expected to be available for all customers by end of March 2024.
- See the article **Overview of Copilot in Fabric and Power BI** for more information.

Overview

Your business data is secure

- Copilot features use Azure OpenAI Service, which is fully controlled by Microsoft. Your data isn't used to train models and isn't available to other customers.
- You retain control over where your data is processed. Data processed by Copilot in Fabric stays within your tenant's geographic region, unless you explicitly allow data to be processed outside your region—for example, to let your users use Copilot when Azure OpenAI isn't available in your region or availability is limited due to high demand. Learn more about admin settings for Copilot.
- Copilot does not store your data for abuse monitoring. To enhance privacy and trust, we've updated our approach to abuse monitoring: previously, we retained data from Copilot in Fabric, containing prompt inputs and outputs, for up to 30 days to check for abuse or misuse.

Following customer feedback, we've eliminated this 30-day retention. Now, we no longer store prompt related data, demonstrating our unwavering commitment to your privacy and security.

Check Copilot outputs before you use them

- Copilot responses can include inaccurate or low-quality content, so make sure to review outputs before you use them in your work.
- Reviews of outputs should be done by people who can meaningfully evaluate the content's accuracy and appropriateness.
- Today, Copilot features work best in the English language. Other languages may not perform as well.

Important

Review the **supplemental preview terms for Fabric**, which includes terms of use for Microsoft Generative AI Service Previews.

How Copilot works

In this article, *Copilot* refers to a range of generative AI features and capabilities in Fabric that are powered by Azure OpenAI Service.

In general, these features are designed to generate natural language, code, or other content based on:

(a) inputs you provide, and,

(b) grounding data that the feature has access to.

For example, Power BI, Data Factory, and Data Science offer Copilot chats where you can ask questions and get responses that are contextualized on your data. Copilot for Power BI can also create reports and other visualizations. Copilot for Data Factory can transform your data and explain what steps it has applied. Data Science offers Copilot features outside of the chat pane, such as custom IPython magic commands in notebooks. Copilot chats may be added to other experiences in Fabric, along with other features that are powered by Azure OpenAI under the hood.

This information is sent to Azure OpenAI Service, where it's processed and an output is generated. Therefore, data processed by Azure OpenAI can include:

- The user's prompt or input.
- Grounding data.
- The AI response or output.

Grounding data may include a combination of dataset schema, specific data points, and other information relevant to the user's current task. Review each experience section for details on what data is accessible to Copilot features in that scenario.

Interactions with Copilot are specific to each user. This means that Copilot can only access data that the current user has permission to access, and its outputs are only visible to that user unless that user shares the output with others, such as sharing a generated Power BI report or generated code. Copilot doesn't use data from other users in the same tenant or other tenants.

Copilot uses Azure OpenAI—not the publicly available OpenAI services—to process all data, including user inputs, grounding data, and Copilot outputs. Copilot currently uses a combination of GPT models, including GPT 3.5. Microsoft hosts the OpenAI models in the Microsoft Azure environment, and the Service doesn't interact with any services by OpenAI, such as ChatGPT or the OpenAI API. Your data isn't used to train models and isn't available to other customers. Learn more about Azure OpenAI.

The Copilot process

These features follow the same general process:

1. **Copilot receives a prompt from a user**. This prompt could be in the form of a question that a user types into a chat pane, or in the form of an action such as selecting a button that says "Create a report."
2. **Copilot preprocesses the prompt through an approach called grounding**. Depending on the scenario, this might include retrieving relevant data such as dataset schema or chat history from the user's current session with Copilot. Grounding improves the specificity of the prompt, so the user gets responses that are relevant and actionable to their specific task. Data retrieval is scoped to data that is accessible to the authenticated user based on their permissions. See the section What data does Copilot use and how is it processed? in this article for more information.
3. **Copilot takes the response from Azure OpenAI and postprocesses it**. Depending on the scenario, this postprocessing might include responsible AI checks, filtering with Azure content moderation, or additional business-specific constraints.
4. **Copilot returns a response to the user in the form of natural language, code, or other content**. For example, a response might be in the form of a chat message or generated code, or it might be a contextually appropriate form such as a Power BI report or a Synapse notebook cell.

5. **The user reviews the response before using it**. Copilot responses can include inaccurate or low-quality content, so it's important for subject matter experts to check outputs before using or sharing them.

Just as each experience in Fabric is built for certain scenarios and personas—from data engineers to data analysts—each Copilot feature in Fabric has also been built with unique scenarios and users in mind. For capabilities, intended uses, and limitations of each feature, review the section for the experience you're working in.

Definitions

Prompt or input

The text or action submitted to Copilot by a user. This could be in the form of a question that a user types into a chat pane, or in the form of an action such as selecting a button that says "Create a report."

Grounding

A preprocessing technique where Copilot retrieves additional data that's contextual to the user's prompt, and then sends that data along with the user's prompt to Azure OpenAI in order to generate a more relevant and actionable response.

Response or output

The content that Copilot returns to a user. For example, a response might be in the form of a chat message or generated code, or it might be contextually appropriate content such as a Power BI report or a Synapse notebook cell.

What data does Copilot use and how is it processed?

To generate a response, Copilot uses:

- The user's prompt or input and, when appropriate,
- Additional data that is retrieved through the grounding process.

This information is sent to Azure OpenAI Service, where it's processed and an output is generated. Therefore, data processed by Azure OpenAI can include:

- The user's prompt or input.
- Grounding data.
- The AI response or output.

Grounding data may include a combination of dataset schema, specific data points, and other information relevant to the user's current task. Review each experience section for details on what data is accessible to Copilot features in that scenario.

Interactions with Copilot are specific to each user. This means that Copilot can only access data that the current user has permission to access, and its outputs are only visible to that user unless that user shares the output with others, such as sharing a generated Power BI report or generated code. Copilot doesn't use data from other users in the same tenant or other tenants.

Copilot uses Azure OpenAI—not OpenAI's publicly available services—to process all data, including user inputs, grounding data, and Copilot outputs. Copilot currently uses a combination of GPT models, including GPT 3.5. Microsoft hosts the OpenAI models in Microsoft's Azure environment and the Service doesn't interact with any services by OpenAI (for example, ChatGPT or the OpenAI API). Your data isn't used to train models and isn't available to other customers. Learn more about Azure OpenAI.

Data residency and compliance

You retain control over where your data is processed. Data processed by Copilot in Fabric stays within your tenant's geographic region, unless you explicitly allow data to be processed outside your region—for example, to let your users use Copilot when Azure OpenAI isn't available in your region or availability is limited due to high demand. (See where Azure OpenAI is currently available.)

To allow data to be processed elsewhere, your admin can turn on the setting **Data sent to Azure OpenAI can be processed outside your tenant's geographic region, compliance boundary, or national cloud instance**. Learn more about admin settings for Copilot.

What should I know to use Copilot responsibly?

Microsoft is committed to ensuring that our AI systems are guided by our AI principles and Responsible AI Standard. These principles include empowering our customers to use these systems effectively and in line with their intended uses. Our approach to responsible AI is continually evolving to proactively address emerging issues.

Copilot features in Fabric are built to meet the Responsible AI Standard, which means that they're reviewed by multidisciplinary teams for potential harms, and then refined to include mitigations for those harms.

Before you use Copilot, keep in mind the limitations of Copilot:

- Copilot responses can include inaccurate or low-quality content, so make sure to review outputs before using them in your work.
- People who are able to meaningfully evaluate the content's accuracy and appropriateness should review the outputs.
- Currently, Copilot features work best in the English language. Other languages may not perform as well.

Data use of Copilot for Data Factory

- Copilot can only access data that is accessible to the user's current Gen2 dataflow session, and that is configured and imported into the data preview grid. Learn more about getting data in Power Query.

Evaluation of Copilot for Data Factory

- The product team has tested Copilot to see how well the system performs within the context of Gen2 dataflows, and whether AI responses are insightful and useful.
- The team also invested in other harms mitigations, including technological approaches to focusing Copilot's output on topics related to data integration.

Tips for working with Copilot for Data Factory

- Copilot is best equipped to handle data integration topics, so it's best to limit your questions to this area.
- If you include descriptions such as query names, column names, and values in the input, Copilot is more likely to generate useful outputs.
- Try breaking complex inputs into more granular tasks. This helps Copilot better understand your requirements and generate a more accurate output.

Data use of Copilot for Data Science

- In notebooks, Copilot can only access data that is accessible to the user's current notebook, either in an attached lakehouse or directly loaded or imported into that notebook by the user. In notebooks, Copilot can't access any data that's not accessible to the notebook.
- By default, Copilot has access to the following data types:
    - Previous messages sent to and replies from Copilot for that user in that session.
    - Contents of cells that the user has executed.
    - Outputs of cells that the user has executed.
    - Schemas of data sources in the notebook.

    - Sample data from data sources in the notebook.
    - Schemas from external data sources in an attached lakehouse.

Evaluation of Copilot for Data Science

- The product team has tested Copilot to see how well the system performs within the context of notebooks, and whether AI responses are insightful and useful.
- The team also invested in additional harms mitigations, including technological approaches to focusing Copilot's output on topics related to data science.

Tips for working with Copilot for Data Science

- Copilot is best equipped to handle data science topics, so limit your questions to this area.
- Be explicit about the data you want Copilot to examine. If you describe the data asset, such as naming files, tables, or columns, Copilot is more likely to retrieve relevant data and generate useful outputs.
- If you want more granular responses, try loading data into the notebook as DataFrames or pinning the data in your lakehouse. This gives Copilot more context with which to perform analysis. If an asset is too large to load, pinning it's a helpful alternative.

Data use of Copilot for Data Warehouse

In warehouse, Copilot can only access the database schema that is accessible in the user's warehouse.

By default, Copilot has access to the following data types:

- Previous messages sent to and replies from Copilot for that user in that session.
- Contents of SQL query that the user has executed.
- Error messages of a SQL query that the user has executed (if applicable).
- Schemas of the warehouse.
- Schemas from attached warehouses or SQL analytics endpoints when cross-DB querying.

Tips for working with Copilot for Data Warehouse

- Copilot is best equipped to handle data warehousing topics, so limit your questions to this area.
- Be explicit about the data you want Copilot to examine. If you describe the data asset, with descriptive table and column names, Copilot is more likely to retrieve relevant data and generate useful outputs.

Evaluation of Copilot for Data Warehouse

The product team tested Copilot to see how well the system performs within the context of warehouses, and whether AI responses are insightful and useful.

The team also invested in additional harm mitigation, including technological approaches to focusing Copilot's output on topics related to data warehousing.

Data use in Copilot for Power BI

- Copilot uses the data in a semantic model that you provide, combined with the prompts you enter, to create visuals. Learn more about semantic models.
- To answer data questions from the semantic model, Copilot requires that Q&A be enabled in the semantic model's dataset settings. For more information, see Update your data model to work well with Copilot for Power BI.

Tips for working with Copilot for Power BI

Review FAQ for Copilot for Power BI for tips and suggestions to help you work with Copilot in this experience.

Evaluation of Copilot for Data Warehouse

The product team invested in harm mitigation, including technological approaches to focusing Copilot's output on topics related to reporting and data warehousing.

Data use of Copilot for Real-Time Intelligence

Copilot for Real-Time Intelligence has access to data, for example the database schema, that is accessible to the Copilot user. The Copilot refers to whichever database is currently connected to the KQL queryset. The Copilot doesn't store any data, and doesn't have access to data that isn't accessible to the Copilot user.

Evaluation of Copilot for Real-Time Intelligence

Following a thorough research period in which several configurations and methods have been tested, the OpenAI integration method had been proven to generate highest accuracy KQL queries. Copilot doesn't automatically run the generated KQL query, and users are advised to run the queries at their own discretion.

Tips for working with Copilot for Real-Time Intelligence

Copilot translates natural language business questions into KQL queries, based on the underlying dataset column names or schema. We recommend that you provide detailed and relevant requests to the copilot to avoid inaccurate or misleading suggested KQL queries. For example, if you're asking about a specific column, provide the column name and the type of data it contains. If you want to use specific operators or functions, this will also help. The more information you provide, the better the Copilot answer will be. You should also restrict questions to databases that are KQL Database tables or materialized views.

Data storage and handling

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

Data in multiple geographies

Many organizations have a global presence and require services in multiple Azure geographies. For example, a company can have its headquarters in the United States, while doing business in other geographical areas, such as Australia. To comply with local regulations, businesses with a global presence need to ensure that data remains stored at rest in several regions. In Fabric, this is called *multi-geo*.

The query execution layer, query caches, and item data assigned to a multi-geo workspace remain in the Azure geography of their creation. However, some metadata, and processing, is stored at rest in the tenant's home geography.

Fabric is part of a larger Microsoft ecosystem. If your organization is already using other cloud subscription services, such as Azure, Microsoft 365, or Dynamics 365, then Fabric operates within the same Microsoft Entra tenant. Your organizational domain (for example, contoso.com) is associated with Microsoft Entra ID. Like all Microsoft cloud services.

Fabric ensures that your data is secure across regions when you're working with several tenants that have multiple capacities across a number of geographies.

- **Data logical separation** - The Fabric platform provide logical isolation between tenants to protect your data.
- **Data sovereignty** - To start working with multi-geo, see Configure Multi-Geo support for Fabric.

Data at rest

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

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

Data in transit

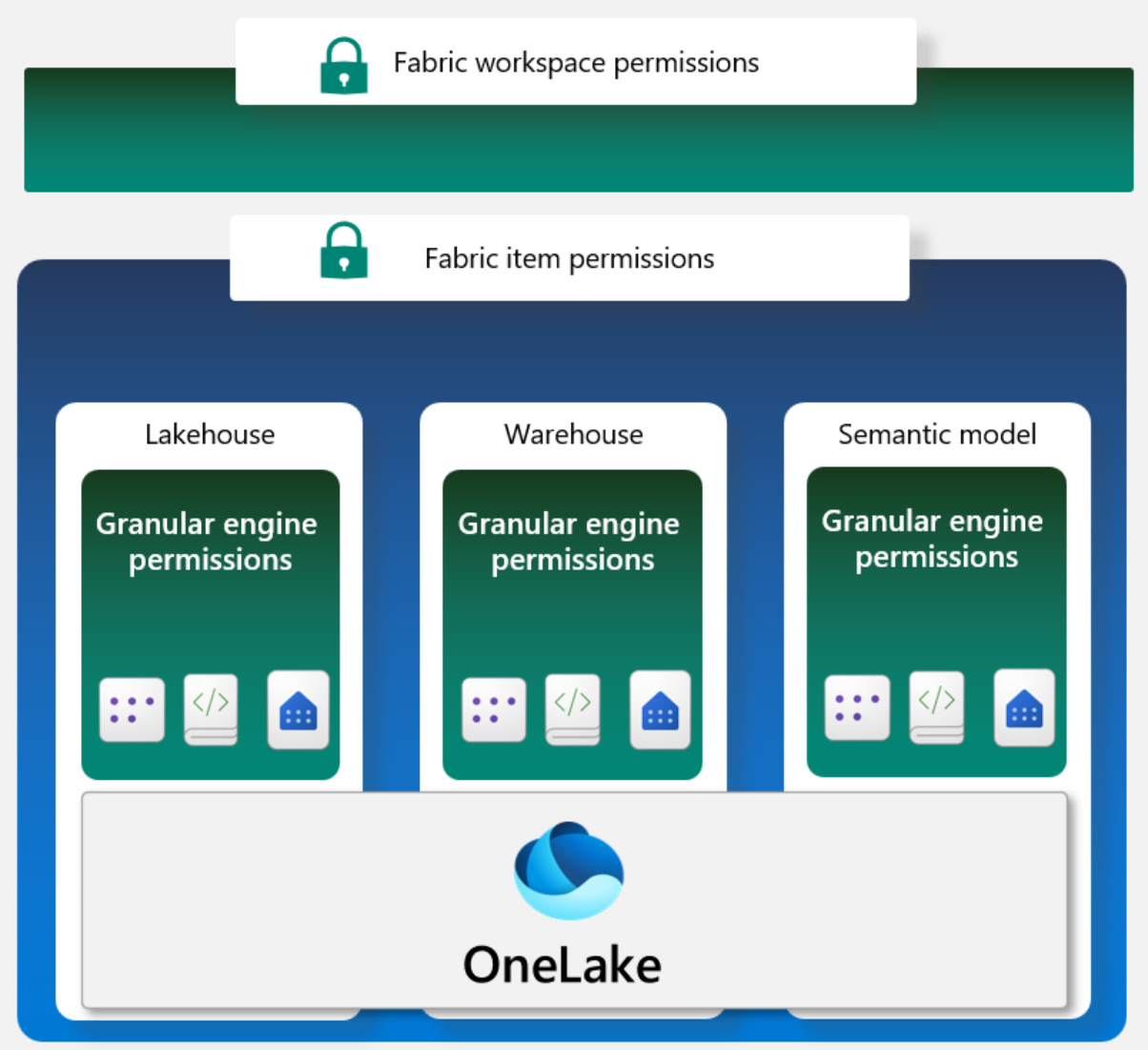
Data in transit across the public internet between Microsoft services is always encrypted with at least TLS 1.2. Fabric negotiates to TLS 1.3 whenever possible. Traffic between Microsoft services always routes over the Microsoft global network.

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

Secure data

Fabric offers a multi-layer security model that provides both simplicity and flexibility in managing data access. Security can be set for an entire workspace, for individual items, or through granular permissions in each Fabric engine.

Granular engine permissions allow fine-grained access control such as table, column, and row-level security to be defined. These granular permissions apply to queries run against that engine. Different engines support different types of granular security, allowing each engine to be tailored specifically for its target users.



Fabric data security

Microsoft Fabric has a flexible permission model that allows you to control access to data in your organization. This article explains the different types of permissions in Fabric and how they work together to control access to data in your organization.

A workspace is a logical entity for grouping items in Fabric. Workspace roles define access permissions for workspaces. Although items are stored in one workspace, they can be shared with other users across Fabric. When you share Fabric items, you can decide which permissions to grant the user you're sharing the item with. Certain items such as Power BI reports, allow even more granular control of data. Reports can be set up so that depending on their permissions, users who view them only see a portion of the data they hold.

Workspace roles

Workspace roles are used to control access to workspaces and the content within them. A Fabric administrator can assign workspace roles to individual users or groups. Workspace roles are confined to a specific workspace and don't apply to other workspaces, the capacity the workspace is in, or the tenant.

There are four Workspace roles and they apply to all items within the workspace. Users that don't have any of these roles, can't access the workspace. The roles are:

- **Viewer** - Can view all content in the workspace, but can't modify it.
- **Contributor** - Can view and modify all content in the workspace.
- **Member** - Can view, modify, and share all content in the workspace.
- **Admin** - Can view, modify, share, and manage all content in the workspace, including managing permissions.

This table shows a small set of the capabilities each role has. For a full and more detailed list, see Microsoft Fabric workspace roles.

Expand table

Capability	Admin	Member	Contributor	Viewer
Delete the workspace	✅	❌	❌	❌
Add admins	✅	❌	❌	❌
Add members	✅	✅	❌	❌
Write data	✅	✅	✅	❌
Create items	✅	✅	✅	❌
Read data	✅	✅	✅	✅

Item permissions

Item permissions are used to control access to individual Fabric items within a workspace. Item permissions are confined to a specific item and don't apply to other items. Use item permissions to control who can view, modify, and manage individual items in a workspace. You can use item permissions to give a user access to a single item in a workspace that they don't have access to.

When you're sharing the item with a user or group, you can configure item permissions. Sharing an item grants the user the read permission for that item by default. Read permissions allow users to see the metadata for that item and view any reports associated with it. However, read permissions don't allow users to access underlying data in SQL or OneLake.

Different Fabric items have different permissions. To learn more about the permissions for each item, see:

- Semantic model
- warehouse
- Data Factory
- Lakehouse
- Data science
- Real-Time Intelligence

Compute permissions

Permissions can also be set within a specific compute engine in Fabric, specifically through the SQL endpoint or in a semantic model. Compute engine permissions enable a more granular data access control, such as table and row level security.

- **SQL endpoint** - The SQL endpoint provides direct SQL access to tables in OneLake, and can have security configured natively through SQL commands. These permissions only apply to queries made through SQL.
- **Semantic model** - Semantic models allow for security to be defined using DAX. Restrictions defined using DAX apply to users querying through the semantic model or Power BI reports built on the semantic model.

You can find more information in these articles:

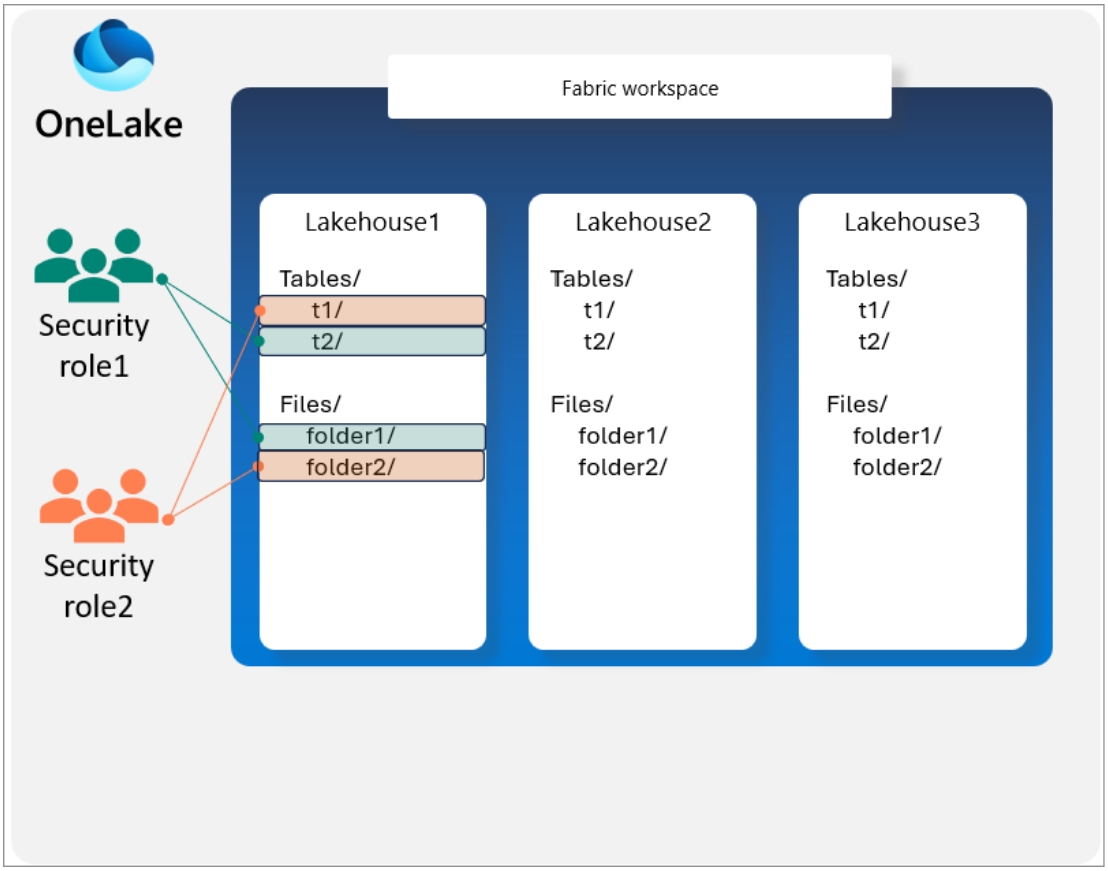
- Row-level security in Fabric data warehousing
- Row-level security (RLS) with Power BI
- Object-level security (OLS)

OneLake permissions

OneLake has its own permissions for governing access to files and folders in OneLake through [OneLake data access roles.](#) OneLake data access roles allow users to create custom roles within a lakehouse and to grant read permissions only to the specified folders when accessing OneLake. For each OneLake role, users can assign users, security groups or grant an automatic assignment based on the workspace role.

data access roles

OneLake data access roles (Preview) allow users to create custom roles within a lakehouse and to grant read permissions only to the specified folders when accessing OneLake. For each OneLake role, users can assign users, security groups or grant an automatic assignment based on the workspace role.



Role-based access control (RBAC)

OneLake RBAC uses role assignments to apply permissions to its members. You can either assign roles to individuals or to security groups, Microsoft 365 groups, and distribution lists. Every member in the user group gets the assigned role.

If someone is in two or more security groups or Microsoft 365 group, they get the highest level of permission that is provided by the roles. If you nest user groups and assign a role to a group, all the contained users have permissions.

OneLake RBAC enables users to define data access roles for **Lakehouse Items** only.

OneLake RBAC restricts data access for users with Workspace **Viewer** or read access to a lakehouse. It doesn't apply to Workspace Admins, Members, or Contributors. As a result, OneLake RBAC supports only Read level of permissions.

How to create RBAC roles

You can define and manage OneLake RBAC roles through your lakehouse data access settings.

Learn more in Get Started with Data Access Roles.

Default RBAC Role in lakehouse

When user creates a new lakehouse, OneLake generates a default RBAC Role named Default Readers. The role allows all users with ReadAll permission to read all folders in the Item.

Here's the default Role definition:

Fabric Item	Role Name	Permission	Folders included	Assigned members
Lakehouse	DefaultReader	ReadAll	All folders under Tables/ and Files/	All users with ReadAll permission

Note

In order to restrict the access to specific users or specific folders, you must either modify the default role or remove it and create a new custom role.

Inheritance in OneLake RBAC

For any given folder, OneLake RBAC permissions always inherit to the entire hierarchy of the folder's files and subfolders.

For example, given the following hierarchy of a lakehouse in OneLake.

```
Bash

Tables/
└── (empty folder)
Files/
└──folder1
|   |   file11.txt
|   |
|   └──subfolder11
|       |   file1111.txt
|       |
|       └──subfolder111
|           |   file1111.txt
|
└──folder2
    |   file21.txt
```

For the given hierarchy, OneLake RBAC permissions for Role1 and Role2 inherit in a following way:

Role	Permission	Folder defined in the Permission	Folders and files inheriting the Permission
Role1	Read	folder1	Bash Copy | | file11.txt | | | └──subfolder11 | | file1111.txt | | | └──subfolder111 | | file1111.txt
Role2	Read	folder2	Bash Copy | file21.txt

Traversal and listing in OneLake RBAC

OneLake RBAC provides automatic traversal of parent items to ensure that data is easy to discover. Granting a user Read to subfolder11 grants the user the ability to list and traverse the parent directory folder1. This functionality is similar to Windows folder permissions where giving access to a subfolder provides discovery and traversal for the parent directories. The list and traversal granted to the parent does not extend to other items outside of the direct parents, ensuring other folders are kept secure.

For example, given the following hierarchy of a lakehouse in OneLake.

```
Bash

Tables/
└── (empty folder)
Files/
└──folder1
|   |   file11.txt
|   |
|   └──subfolder11
|       |   file111.txt
|       |
|       └──subfolder111
|           |   file1111.txt
|
└──folder2
    |   file21.txt
```

For the given hierarchy, OneLake RBAC permissions for 'Role1' provides the following access. Note that access to file11.txt is not visible as it is not a parent of subfolder11. Likewise for Role2, file111.txt is not visible either.

Role	Permission	Folder defined in the Permission	Folders and files inheriting the Permission
Role1	Read	subfolder11	Bash Copy Files/ └──folder1 | | | └──subfolder11 | | file111.txt | | | └──subfolder111 | | file1111.txt
Role2	Read	subfolder111	Bash Copy Files/ └──folder1 | | | └──subfolder11 | | | └──subfolder111 | | file1111.txt

For shortcuts, the listing behavior is slightly different. Shortcuts to external data sources behave the same as folders do, however shortcuts to other OneLake locations have specialized behavior. Access to a OneLake shortcut is determined by the target permissions of the shortcut. When listing shortcuts, no call is made to check the target access. As a result, when listing a directory all internal shortcuts will be returned regardless of a user's access to the target. When a user tries to open the shortcut the access check will evaluate and a user will only see data they have the

required permissions to see. For more information on shortcuts, see the [shortcuts security section.]

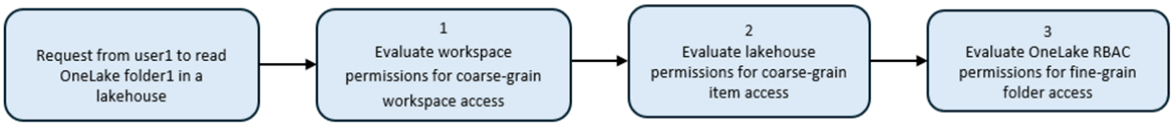
The examples below use the following folder hierarchy.

```
Files/
├──folder1
│
└──shortcut2
│
└──shortcut3
```

Role	Permission	Folder defined in the Permission	Result of listing Files
Role1	Read	folder1	Bash Copy Files/ ├──folder1 │ └──shortcut2 │ └──shortcut3
Role2	N/A	N/A	Bash Copy Files/ │ └──shortcut2 │ └──shortcut3

How OneLake RBAC permissions are evaluated with Fabric permissions

Workspace and Item permissions let you grant "coarse-grain" access to data in OneLake for the given Item. OneLake RBAC permissions enable you to restrict the data access in OneLake only to specific folders.



OneLake RBAC and Workspace permissions

The workspace permissions are the first security boundary for data within OneLake. Each workspace represents a single domain or project area where teams can

collaborate on data. You manage security in the workspace through Fabric workspace roles. Learn more about Fabric role-based access control (RBAC): Workspace roles

Workspace roles in Fabric grant the following permissions in OneLake.

Expand table

Permission	Admin	Member	Contributor	Viewer
View files in OneLake	Always* Yes	Always* Yes	Always* Yes	No by default. Use OneLake RBAC to grant the access.
Write files in OneLake	Always* Yes	Always* Yes	Always* Yes	No

Note

*Since Workspace Admin, Member and Contributor Roles automatically grant Write permissions to OneLake, it overrides any OneLake RBAC Read permissions.

Expand table

Workspace Role	Does OneLake apply RBAC Read permissions?
Admin, Contributor, Member	No, OneLake Security will ignore any OneLake RBC Read permissions
Viewer	Yes, if defined, OneLake RBAC Read permissions will be applied

OneLake RBAC and Lakehouse permissions

Within a workspace, Fabric items can have permissions configured separately from the workspace roles. You can configure permissions either through sharing an item or by managing the permissions of an item. The following permissions determine a user's ability to perform actions on data in OneLake.

Lakehouse permissions

Lakehouse Permission	Can view files in OneLake?	Can write files in OneLake?	Can read data through SQL analytics endpoint?
Read	No by default, use OneLake RBAC to grant access.	No	No

Lakehouse Permission	Can view files in OneLake?	Can write files in OneLake?	Can read data through SQL analytics endpoint?
ReadAll	Yes by default. Use OneLake RBAC to restrict the access.	No	No
Write	Yes	Yes	Yes
Execute, Reshare, ViewOutput, ViewLogs	N/A - can't be granted on its own	N/A - can't be granted on its own	N/A - can't be granted on its own

OneLake RBAC and Lakehouse SQL Analytics Endpoint permissions

SQL analytics endpoint is a warehouse that is automatically generated from a Lakehouse in Microsoft Fabric. A customer can transition from the "Lake" view of the Lakehouse (which supports data engineering and Apache Spark) to the "SQL" view of the same Lakehouse. Learn more about SQL analytics endpoint in Data Warehouse documentation: SQL analytics endpoint.

SQL Analytics Endpoint Permission	Users can view files via OneLake Endpoint?	Users can write files via OneLake Endpoint?	Users can read data via SQL analytics endpoint?
Read	No by default, use OneLake RBAC to grant access.	No	No by default, but can be configured with SQL granular permissions
ReadData	No by default. Use OneLake RBAC to grant access.	No	Yes
Write	Yes	Yes	Yes

OneLake RBAC and Default Lakehouse Semantic Model permissions

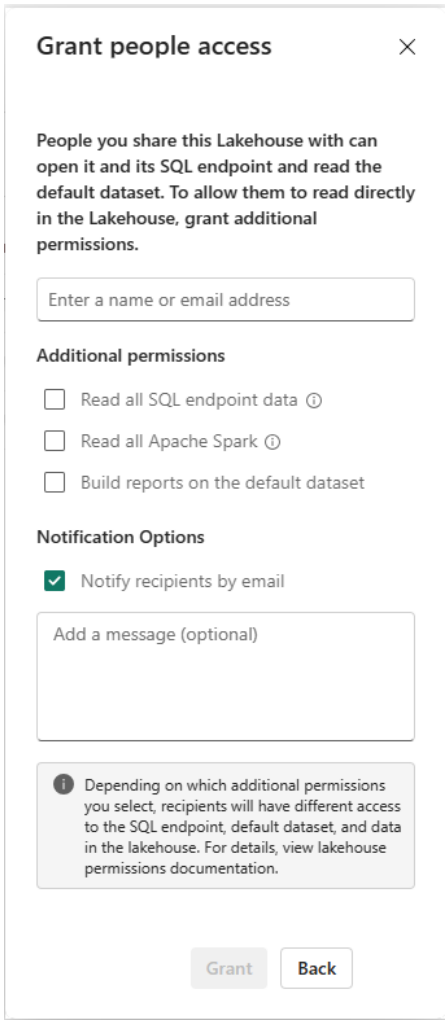
In Microsoft Fabric, when the user creates a lakehouse, the system also provisions the associated default semantic model. The default semantic model has metrics on top of lakehouse data. The semantic model allows Power BI to load data for reporting.

Default Semantic Model Permission	Can view files in OneLake?	Can write files in OneLake?	Can see schema in Semantic Model?	Can read data in Semantic Model?
Read	No by default, use OneLake RBAC to grant access.	No	No	Yes by default. Can be restricted with Power BI object-level security and Power BI row-level security
Build	Yes by default. Use OneLake RBAC to restrict the access.	Yes	Yes	Yes
Write	Yes	Yes	Yes	Yes
Reshare	N/A - can't be granted on its own	N/A - can't be granted on its own	N/A - can't be granted on its own	N/A - can't be granted on its own

Lakehouse Sharing and OneLake RBAC Permissions

When user shares a lakehouse, they grant other users or a group of users access to a lakehouse without giving access to the workspace and the rest of its items. Shared lakehouse can be found through Data Hub or the Shared with Me section in Microsoft Fabrics.

When someone shares a lakehouse, they can also grant access to the SQL analytics endpoint and associated default semantic model.



Sharing Option	Can view files in OneLake?	Can write files in OneLake?	Can read data through SQL analytics endpoint?	Can view and build Semantic Models?
No additional permissions selected	No by default, use OneLake RBAC to grant access.	No	No	No
Read all Apache Spark	Yes by default. Use OneLake RBAC to restrict the access.	No	No	No
Read all SQL endpoint data	No by default, use OneLake RBAC to grant access.	No	Yes	No
Build reports on the default dataset	Yes by default. Use OneLake RBAC to restrict the access.	No	No	Yes

Learn more about data sharing permissions model:

- How lakehouse sharing works
- Share your warehouse and manage permissions

Shortcuts

OneLake RBAC in Internal Shortcuts

For any folder in a lakehouse, RBAC permissions always inherit to all Internal shortcuts where this folder is defined as target.

When a user accesses data through a shortcut to another OneLake location, the identity of the calling user is used to authorize access to the data in the target path of the shortcut*. As a result, this user must have OneLake RBAC permissions in the target location to read the data.

Important

When accessing shortcuts through **Power BI semantic models** or **T-SQL**, the calling user's identity is not passed through to the shortcut target. The calling item owner's identity is passed instead, delegating access to the calling user.

Defining RBAC permissions for the internal shortcut is not allowed and must be defined on the target folder located in the target item. Since defining RBAC permissions is limited to lakehouse items only, OneLake enables RBAC permissions only for shortcuts targeting folders in lakehouse items.

The next table specifies whether the corresponding shortcut scenario is supported for defining OneLake RBAC permissions.

Expand table

Internal Shortcut scenario	OneLake RBAC permissions supported?	Comments
Shortcut in a lakehouse1 pointing to folder2 located in the **same lakehouse**.	Supported.	To restrict the access to data in shortcut, define OneLake RBAC for folder2.
Shortcut in a lakehouse1 pointing to folder2 located in **another lakehouse2**	Supported.	To restrict the access to data in shortcut, define OneLake RBAC for folder2 in lakehouse2.
Shortcut in a lakehouse pointing to a Table located in a **datawarehouse**	Not supported.	OneLake doesn't support defining RBAC permissions in datawarehouses. Access is

Internal Shortcut scenario	OneLake RBAC permissions supported?	Comments
		determined based on the ReadAll permission instead.
Shortcut in a lakehouse pointing to a Table located in a **KQL database**	Not supported.	OneLake doesn't support defining RBAC permissions in KQL databases. Access is determined based on the ReadAll permission instead.

OneLake RBAC in External Shortcuts (ADLS, S3, Dataverse)

OneLake supports defining RBAC permissions for shortcuts such as ADLS, S3 and Dataverse shortcuts. In this case, RBAC model is applied **on top** of the delegated authorization model enabled for this type of shortcut.

Suppose, user1 creates an S3 shortcut in a lakehouse pointing to a folder in an AWS S3 bucket. Then user2 is attempting to access data in this shortcut.

Does S3 Connection authorize access for the delegated user1?	Does OneLake RBAC authorize access for the requesting user2?	Result: Can user2 access data in S3 Shortcut?
Yes	Yes	Yes
No	No	No
No	Yes	No
Yes	No	No

The RBAC permissions must be defined for the entire scope of the shortcut (entire target folder), but inherit recursively to all its subfolders and files.

Learn more about S3, ADLS, and Dataverse shortcuts in OneLake Shortcuts.

Limits on OneLake RBAC

The following table provides the limitations of OneLake data access roles.

Scenario	Limit
Maximum number of OneLake RBAC roles per Fabric Item	At most 250 roles for each lakehouse item.
Maximum number of members per OneLake RBAC role	At most 500 users and user groups per role.

Scenario	Limit
Maximum number of permissions per OneLake RBAC role	At most 500 permissions per role

Latencies in OneLake RBAC

- If you change a OneLake RBAC Role definition, it takes about 5 minutes for OneLake to apply the updated definitions.
- If you change a user group in OneLake RBAC role, it takes about an hour for OneLake to apply the role's permissions on the updated user group.

Shortcut security

Shortcuts in Microsoft Fabric allow for simplified data management. OneLake Folder security applies for OneLake shortcuts based on roles defined in the lakehouse where the data is stored.

For more information on the security considerations of shortcuts, see OneLake access control model. More information on shortcuts can be found here..

Allow apps running outside of Fabric to access data via OneLake

OneLake allows you to restrict access to data from applications running outside of Fabric environments. Admins can find the setting in the OneLake section of Tenant Admin Portal. When you turn this switch ON, users can access data via all sources. When you turn the switch OFF, users can't access data via applications running outside of Fabric environments. For example, users can access data via applications like Azure Databricks, custom applications using Azure Data Lake Storage (ADLS) APIs, or OneLake file explorer.

Learn more about OneLake Data Access Control Model and view the how to guides.

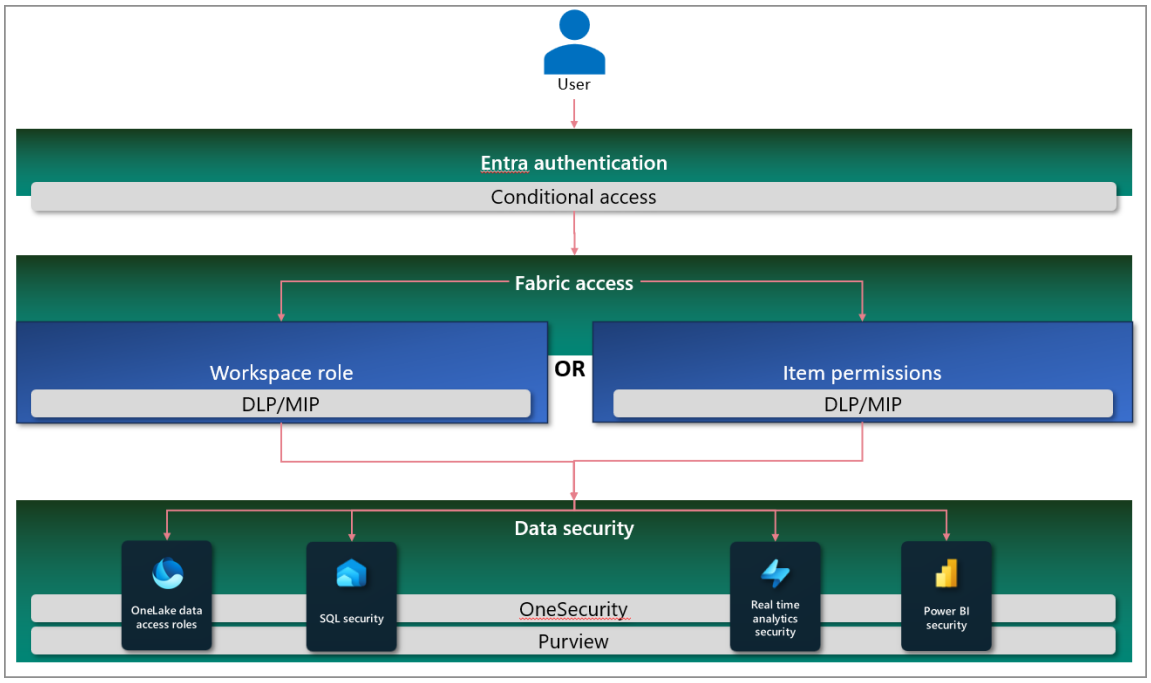
- How to secure a lakehouse for Data Science teams
- How to secure a lakehouse for Data Warehousing teams
- How to secure data for common data architectures

Order of operation

Fabric has three different security levels, and a user must have access at each level in order to access the data. Each level evaluates sequentially to determine if a user has access. Security rules such as Microsoft Information Protection policies evaluate at a given level to allow or disallow access. The order of operation when evaluating Fabric security is:

1. Entra authentication: Checks if the user is able to authenticate to the Microsoft Entra tenant.
2. Fabric access: Checks if the user can access Microsoft Fabric.
3. Data security: Checks if the user can perform the requested action on a table or file.

A diagram view of this order is as follows.



Examples

This sections provides two examples of how permissions can be set up in Fabric.

Example 1: Setting up team permissions

Wingtip Toys is set up with one tenant for the entire organization, and three capacities. Each capacity represents a different region. Wingtip Toys operates in the United States, Europe, and Asia. Each capacity has a workspace for each department in the organization, including the sales department.

The sales department has a manager, a sales team lead, and sales team members. Wingtip Toys also employs one analyst for the entire organization.

The following table shows the requirements for each role in the sales department and how permissions are set up to enable them.

Expand table

Role	Requirement	Setup
Manager	View and modify all content in the sales department in the entire organization	A *member* role for all the sales workspaces in the organization
Team lead	View and modify all content in the sales department in a specific region	A *member* role for the sales workspace in the region
Sales team member	• View stats of other sale members in the region • View and modify his own sales report	• *No roles* for any of the sales workspaces • Access to a specific report that lists the member's sale figures
Analyst	View all content in the sales department in the entire organization	A *viewer* role for all the sale workspaces in the organization

Wingtip also has a quarterly report that lists its sales income per sales member. This report is stored in a finance workspace. Using row-level security, the report is set up so that each sales member can only see their own sale figures. Team leads can see the sales figures of all the sale members in their region, and the sales manager can see sale figures of all the sale members in the organization.

Example 2: Workspace and item permissions

When you share an item, or change its permissions, workspace roles don't change. The example in this section shows how workspace and item permissions interact.

Veronica and Marta work together. Veronica is the owner of a report she want's to share with Marta. If Veronica shares the report with Marta, Marta will be able to access it regardless of the workspace role she has.

Let's say that Marta has a viewer role in the workspace where the report is stored. If Veronica decides remove Marta's item permissions from the report, Marta will still be able to view the report in the workspace. Marta will also be able to open the report from the workspace and view its content. This is because Marta has view permissions to the workspace.

If Veronica doesn't want Marta to view the report, removing Marta's item permissions from the report isn't enough. Veronica also needs to remove Marta's viewer permissions from the workspace. Without the workspace viewer permissions,

Marta won't be able to see that the report exists because she won't be able to access the workspace. Marta will also not be able to use the link to the report, because she doesn't have access to the report.

Now that Marta doesn't have a workspace viewer role, if Veronica decides to share the report with her again, Marta will be able to view it using the link Veronica shares with her, without having access to the workspace.

Example 3: Power BI App permissions

When sharing Power BI reports, you often want your recipients to only have access to the reports and not to items in the workspace. For this you can use Power BI apps or share reports directly with users.

Furthermore you can limit viewer access to data using Row-level security (RLS), with RLS you can create roles that have access to certain portions of your data, and limit results returning only what the user's identity can access.

This works fine when using Import models as the data is imported in the semantic model and the recipients have access to this as part of the app. With DirectLake the report reads the data directly from the Lakehouse and the report recipient needs to have access to these files in the lake. You can do this in several ways:

- Give ReadData permission on the Lakehouse directly.
- Switch the data source credential from Single Sign On (SSO) to a fixed identity that has access to the files in the lake.

Because RLS is defined in the Semantic Model the data will be read first and then the rows will be filtered.

If any security is defined in the SQL endpoint that the report is built on, the queries automatically fall back to DirectQuery mode. If you do not want this default fallback behaviour, you can create a new Lakehouse using shortcuts to the tables in the original Lakehouse and not define RLS or OLS in SQL on the new Lakehouse.

Example 4: Difference between control plane and data plane permissions

There are two categories of permissions in Fabric: control plane and data plane. Control plane permissions are the Fabric Workspace and Item level permissions. These enable actions in Fabric such as viewing or creating an item. Data plane permissions are those that give access to view or write data. In general, write access granted at the control plane level will also extend to write access at the data plane level. However, users with read permissions at the control plane level might also have the ability to write on the data plane through compute engine security.

For instance, Nat has the item read permission on the warehouse item named *Sales*. This permission allows Nat to connect to the warehouse and execute metadata queries. If Nat needs to create new tables in the *Sales* warehouse, she can be added to the "db_owner" role in the warehouse, granting her the ability to create tables and write data.

In summary, while permissions granted at the control plane level often dictate access at the data plane level, additional compute engine security permissions can provide users with expanded capabilities, potentially allowing them to perform actions not explicitly permitted at the control plane level.

Shortcut security

OneLake shortcuts serve as pointers to data residing in various storage accounts, whether within OneLake itself or in external systems like Azure Data Lake Storage (ADLS). This article looks at the permissions required to create shortcuts and access data using them.

To ensure clarity around the components of a shortcut this document uses the following terms:

- Target path: The location that a shortcut points to.
- Shortcut path: The location where the shortcut appears.

Create and delete shortcuts

To create a shortcut a user needs to have Write permission on the Fabric Item where the shortcut is being created. (the shortcut path) In addition, the user needs Read access to the data the shortcut is pointing to. (the target path) Shortcuts to external sources may require certain permissions in the external system. The What are shortcuts? article has the full list of shortcut types and required permissions.

Expand table

Capability	Permission on shortcut path	Permission on target path
Create a shortcut	Write	ReadAll[1]
Delete a shortcut	Write	N/A

[1] If OneLake data access roles is enabled the user needs to be in a role that grants access to the target path.

Accessing shortcuts

A combination of the permissions in the shortcut path and the target path governs the permissions for shortcuts. When a user accesses a shortcut, the most restrictive permission of the two locations is applied. Therefore, a user that has read/write permissions in the lakehouse but only read permissions in the target path can't write to the target path. Likewise, a user that only has read permissions in the lakehouse but read/write in the target path also can't write to the target path.

The following table shows the shortcut-related permissions for each shortcut action.

Expand table

Capability	Permission on shortcut path	Permission on target path
Read file/folder content of shortcut	ReadAll[1]	ReadAll[1]
Write to shortcut target location	Write	Write
Read data from shortcuts in table section of the lakehouse via TDS endpoint	Read	ReadAll[2]

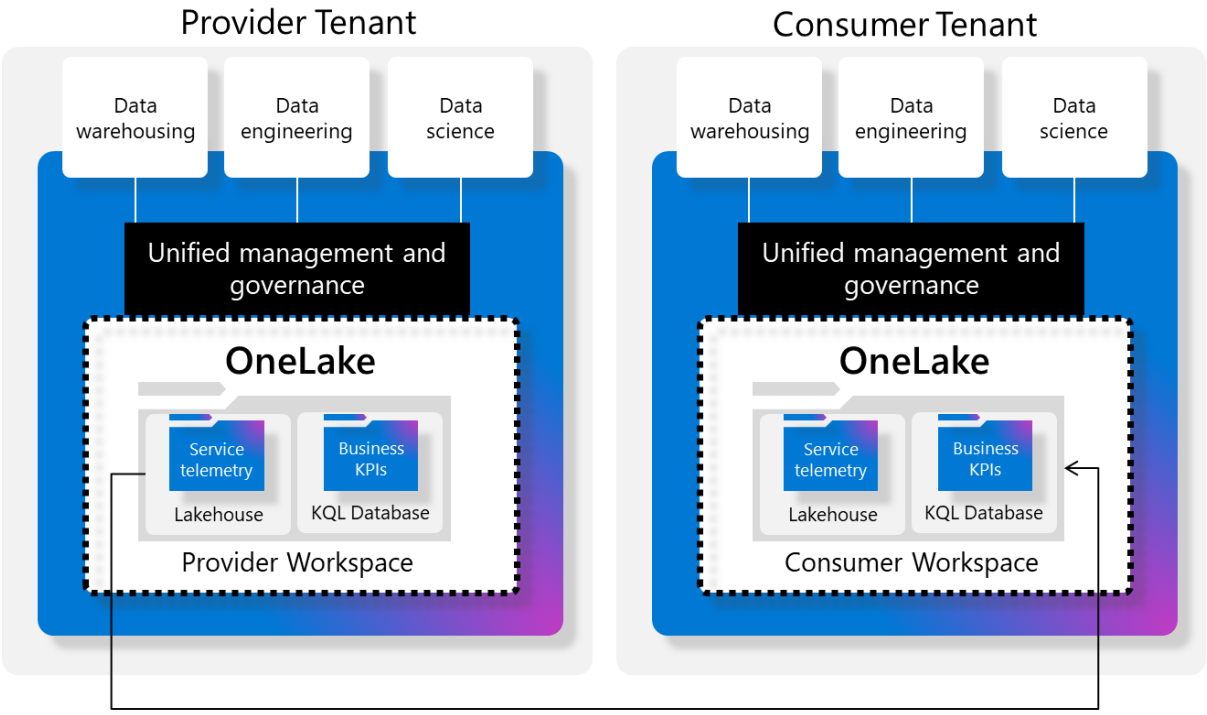
[1] If OneLake data access roles is enabled the user needs to be in a role that grants access to the data.

Important

[2] When accessing shortcuts through Power BI semantic models or T-SQL, **the calling user's identity is not passed through to the shortcut target path.** The calling item owner's identity is passed instead, delegating access to the calling user.

External data sharing in Microsoft Fabric

Fabric external data sharing is a feature that enables Fabric users to share data from their tenant with users in another Fabric tenant. The data is shared *in-place* from OneLake storage locations in the sharer's tenant, meaning that no data is actually copied to the other tenant. Rather, this cross-tenant sharing creates a OneLake shortcut in the other tenant that points back to the original data in the sharer's tenant. Data that is shared across tenant boundaries is exposed to users in the other tenant as read-only, and can be consumed by any OneLake compatible Fabric workload in that tenant.



Cross tenant OneLake data share

This external data sharing feature for Fabric OneLake data isn't related to the mechanism that exists for sharing Power BI semantic models with Entra B2B guest users.

How does external data sharing work

As a prerequisite to external data sharing, Fabric admins need to turn on external data sharing both in the sharer's tenant and in the external tenant. Enabling external data sharing includes specifying who can create and accept external data shares. For more information, see Enable external data sharing.

Users who are allowed to create external data shares can share data residing in tables or files within supported Fabric items, as long as they have the standard Fabric read and reshare permissions for the item being shared. The user creating the share invites a user from another tenant to accept the external data share. This user receives a link that they use to accept the share. Upon accepting the share, the recipient chooses a lakehouse where a shortcut to the shared data will be created.

External data share links don't work for users who are in the tenant where the external data share was created. They work only for users in external tenants. To share data from OneLake storage accounts with users in the same tenant, use OneLake shortcuts.

Note

Cross-tenant data access is enabled via a dedicated Fabric-to-Fabric authentication mechanism and does not require **Entra B2B guest user access**.

Supported Fabric item types

External data sharing is currently supported for data residing in tables or files within:

- Lakehouses
- KQL databases

Revoking external data shares

Any user in the sharing tenant who has read and reshare permissions on an externally shared item can revoke the external data share at any time using the **External data shares** tab on the manage permissions page. Revoking external data shares can have serious implications for the consuming tenants and should be considered carefully. For more information, see Revoking external data shares.

Security Considerations

Sharing data with users outside your home tenant has implications for data security and privacy that you should consider. It's important to understand the underlying flows of data sharing to better evaluate these implications.

Data is shared across tenants using Fabric-internal security mechanisms. The share security mechanism grants read-only access to **any user** within the home tenant of the user that was invited to accept the share. Data is shared “in-place”. No data is copied, and it isn't even accessed until the someone in the receiving tenant executes

a Fabric workload over the shared data. Fabric evaluates and enforces Entra-ID-based roles and permissions locally, within the tenant they're defined in. This means that access control policies defined in the sharer's tenant, such as semantic model row-level security (RLS), Microsoft Purview Information Protection policies, and Purview Data Loss Prevention policies **are not** enforced on data that crosses organization boundaries. Rather, it is the policies defined in the consumer's tenant that are enforced on the incoming share, the same way that they're enforced on any data within that tenant.

With this understanding in mind, be aware of the following:

- The sharer can't control who has access to the data in the consumer's tenant.
- The consumer can grant access to the data to anyone, even guest users from outside the consumer's organization.
- Data might be transferred across geographic boundaries when it's accessed within the consumer's tenant.

Considerations and limitations

- **Shortcuts:** Shortcuts contained in folders that are shared via external data sharing won't resolve in the consumer tenant.

Governing data

Microsoft Fabric governance and compliance provides set of capabilities that help you manage, protect, monitor, and improve the discoverability of your organization's sensitive information, so as to gain and maintain customer trust and to meet data governance and compliance requirements and regulations. Many of these capabilities are built in and included with your Microsoft Fabric license, while some others require additional licensing from Microsoft Purview.

This article describes at a high level the main features and components that help you govern your organization's data estate, and includes some guidance regarding taking advantage of the capabilities these features and components offer. It also provides links to

Manage your data estate

This section describes some of the main features you can use to help manage your data estate.

Admin portal

The Microsoft Fabric admin portal is a centralized place that allows your organization's administrators to control your overall Fabric estate. This includes settings that govern Microsoft Fabric. For example, you can make changes to tenant settings, govern capacities, domains, and workspaces, and control how users interact with Microsoft Fabric. To provide flexibility, some aspects of administration and governance can be delegated to capacities, domains, and workspaces so the respective admins can manage them in their scope.

For more information about the admin portal, see What is the admin portal?.

Guidance: Platform/IT owners should have access to the admin portal. They can define domains, and delegate domain and capacity management to domain and capacity owners as best suits your organizational needs.

Tenant, domain, and workspace settings

Tenant, domain, and workspace admins each have settings within their scope that they can configure to control who has access to certain functionalities at different levels. Some tenant-level settings can be delegated to domain and capacity admins.

For more information see About tenant settings, Configure domain settings, and Workspace settings.

Guidance: Fabric admins should define tenant-wide settings, leaving domain admins to override delegated settings as needed. Individual teams (workspace owners) are expected to define their own more granular workspace-level controls and settings.

Domains

Domains are a way of logically grouping together all the data in an organization that is relevant to particular areas or fields, for example, by business unit. One of the most common uses for domains is to group data by business department, making it possible for departments to manage their data according to their specific regulations, restrictions, and needs.

Grouping data into domains and subdomains enables better discoverability and governance. For instance, in the OneLake data hub, users can filter content by domain in order find content that is relevant to them. With respect to governance, some tenant-level settings for managing and governing data can be delegated to the domain level, thus allowing domain-specific configuration of those settings.

For more information, see Domains.

Guidance: Business and enterprise architects should design the organization's domain setup, while Fabric admins should implement this design by creating domains and subdomains and assigning domain owners. Preferably, center of excellence (COE) teams should be part of this discussion to align the domains with the overall strategy of the organization.

Workspaces

Teams in organizations use workspaces to create Fabric items and collaborate with each other. These workspaces can be assigned to teams or departments based on governance requirements and data boundaries. How exactly workspace assignment is done depends on internal team structure and how the teams want to handle their Fabric items (for example, do they need one or many workspaces).

Guidance: For development purposes, a best practice is to have isolated workspaces per developer, so that they can work on their own without interfering with the shared workspace. Fabric admins are expected to define who has permission to create workspaces. Workspace admins are expected to define Spark environments that can be reused by users. For further information about best practices, see Best practices for lifecycle management in Fabric.

Capacities

Capacities are the compute resources used by all Fabric workloads. Based on organizational requirements, capacities can be used as isolation boundaries for compute, chargebacks etc.

Guidance: Split up capacities based on the requirements of the environment, for example, development/test/acceptance/production (DTAP). This makes for better workload isolation and chargeback.

Metadata scanning

Metadata scanning facilitates governance of your organization's Microsoft Fabric data by making it possible for cataloging tools to catalog and report on the metadata of all your organization's Fabric items. It accomplishes this using a set of Admin REST APIs that are collectively known as the *scanner APIs*. The scanner APIs extract metadata such as item name, ID, sensitivity, endorsement status, etc.

For more information, see Metadata scanning.

Secure, protect, and comply

Data security and having a compliant data platform are important for making sure that your data stays safe and is not compromised. For details about network security, access control, and encryption, see the Security overview.

Fabric leverages Microsoft Purview for protecting sensitive data and helping ensure compliance with data privacy regulations and requirements.

Privacy

The first phase of any data protection strategy is to identify where your private data sits. This is considered one of the most challenging but important steps towards making sure you can protect your data at the source. The following sections describe capabilities Fabric provides to help your organization meet this challenge.

Data security

To make sure data in Fabric is secure from unauthorized access and stays compliant with data privacy requirements, you can use sensitivity labels from Microsoft Purview Information Protection in combination with built-in Fabric capabilities to manually or automatically tag your organization's data. Purview Audit then captures audit trails

on activities performed in Fabric. This includes capturing user activities in the Fabric tenant, such as Lakehouse access, Power BI access, Spark activities, data factory activities, logins, etc.

Purview Information Protection

Information protection in Fabric enables you to discover, classify, and protect Fabric data using sensitivity labels from Microsoft Purview Information Protection. Fabric provides multiple capabilities, such as default labeling, label inheritance, and programmatic labeling, to help achieve maximal sensitivity label coverage across your entire Fabric data estate. Once labeled, data remains protected even when it's exported out of Fabric via supported export paths. Compliance admins can monitor activities on sensitivity labels in Microsoft Purview Audit.

For more information, see Information Protection in Microsoft Fabric.

Guidance: Sensitivity labels from Microsoft Purview Information Protection and their associated label policies should be specified at an organizational level and be valid for the whole organization.

Purview Data Loss Prevention

To help organizations detect and protect their sensitive data, Fabric supports Microsoft Purview Data Loss Prevention (DLP) polices. When a DLP policy for Fabric detects a supported item type containing sensitive information, a policy tip can be attached to the item that explains the nature of the sensitive content, and an alert can be registered on the data loss prevention **Alerts** page in the Microsoft Purview compliance portal for monitoring and management by administrators. In addition, email alerts can be sent to administrators and specified users.

This article describes how DLP in Fabric works, lists considerations and limitations as well as licensing and permissions requirements, and explains how DLP CPU usage is metered. For more information, see:

- Configure a DLP policy for Fabric to see how to configure DLP policies for Fabric.
- Respond to a DLP policy violation in Fabric to see how to respond when a policy tip tells you your lakehouse or semantic model has a DLP policy violation.
- Monitor DLP policy violations in Fabric to see how to sign in to the Microsoft Purview portal to see details about DLP violation alerts.

Considerations and limitations

- DLP policies for Fabric are defined in the Microsoft Purview compliance portal.
- DLP policies apply to workspaces. Only workspaces hosted in Fabric or Premium capacities are supported. For more information, see Microsoft Fabric concepts and licenses.
- DLP evaluation workloads impact capacity. Currently, DLP for Fabric is available at no additional cost, but this is subject to change. Check this document and the Fabric blog for updates.
- DLP policy templates aren't yet supported for Fabric DLP policies. When creating a DLP policy for Fabric, choose the "custom policy" option.
- Fabric DLP policy rules currently support sensitivity labels and sensitive info types as conditions.
- DLP policies for Fabric aren't supported for sample semantic models, streaming datasets, or semantic models that connect to their data source via DirectQuery or live connection. This includes semantic models with mixed storage, where some of the data comes via import-mode and some comes via DirectQuery.
- DLP policies for Fabric apply only on data in Lakehouse Tables/ folder stored in Delta format.
- DLP policies for Fabric support all the primitive Delta types except *timestamp_ntz*.
- DLP policies for Fabric aren't supported for the following Delta Parquet data types:
    - Binary, timestamp_ntz, Struct, Array, List, Map, Json, Enum, Interval, Void.
    - Data with LZ4, Zstd, and Gzip compression codecs.
- Exact data match (EDM) classifiers and trainable classifiers aren't supported by DLP for Fabric. If you select an EDM or trainable classifier in the condition of a policy, the policy will yield no results even if the semantic model or lakehouse does in fact contain data that satisfies the EDM or trainable classifier. Other classifiers specified in the policy will return results, if any.
- DLP policies for Fabric aren't supported in the China North region. See How to find the default region for your organization to learn how to find your organization's default data region.
- Azure capacities aren't supported for DLP in Fabric in the following clusters:
    - WUS3
    - WUS2
    - SCUS
- Onboarding a new tenant to DLP can take a few hours, depending on the number of supported workspaces that are being onboarded.

Licensing and permissions

SKU/subscriptions licensing

Before you get started with DLP for Fabric, you should confirm your Microsoft 365 subscription. The admin account that sets up the DLP rules must be assigned one of the following licenses:

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection & Governance
- Purview capacities

Permissions

Data from DLP for Fabric can be viewed in Activity explorer. There are four roles that grant permission to Activity explorer; the account you use for accessing the data must be a member of any one of them.

To view the Activity explorer, the account you use for accessing the data must be a member of any of the following roles or above.

- Compliance administrator
- Security administrator
- Compliance data administrator

Supported item types

DLP policies for Fabric currently support the following item types.

- Semantic models
- Lakehouses

See Considerations and limitations for exceptions.

How do DLP policies for Fabric work

You define a DLP policy in the data loss prevention section of the Microsoft Purview portal. In the policy, you specify the sensitivity labels and/or sensitive info types you want to detect. You also specify the actions that will happen when the policy detects a semantic model or lakehouse that contains sensitive data of the kind you specified. DLP policies for Fabric support 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 semantic model or lakehouse is evaluated by DLP policies, if it matches the conditions specified in a DLP policy, the actions specified in the policy occur. DLP policies are initiated by the following actions:

Semantic models:

A semantic model is evaluated against DLP policies whenever one of the following events occurs:

- Publish
- Republish
- On-demand refresh
- Scheduled refresh

Note

DLP evaluation of the semantic model doesn't occur if either of the following is true:

- The initiator of the event (publish, republish, on-demand refresh, scheduled refresh) is an account using service principal authentication.
- The semantic model owner is a service principal.

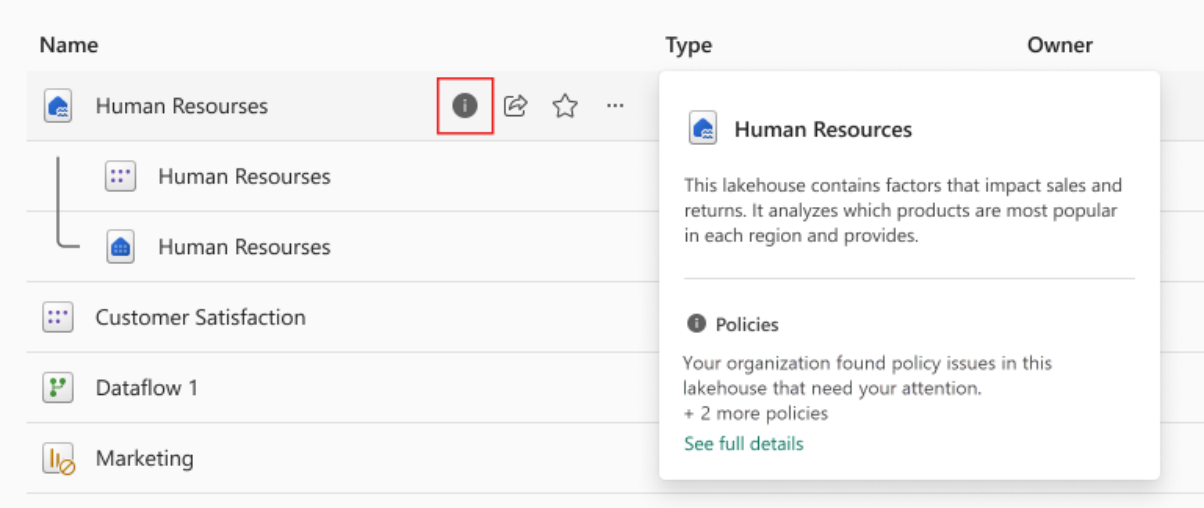
Lakehouse:

A lakehouse is evaluated against DLP policies When the data within a lakehouse undergoes a change, such as getting new data, connecting a new source, adding or updating existing tables, and more.

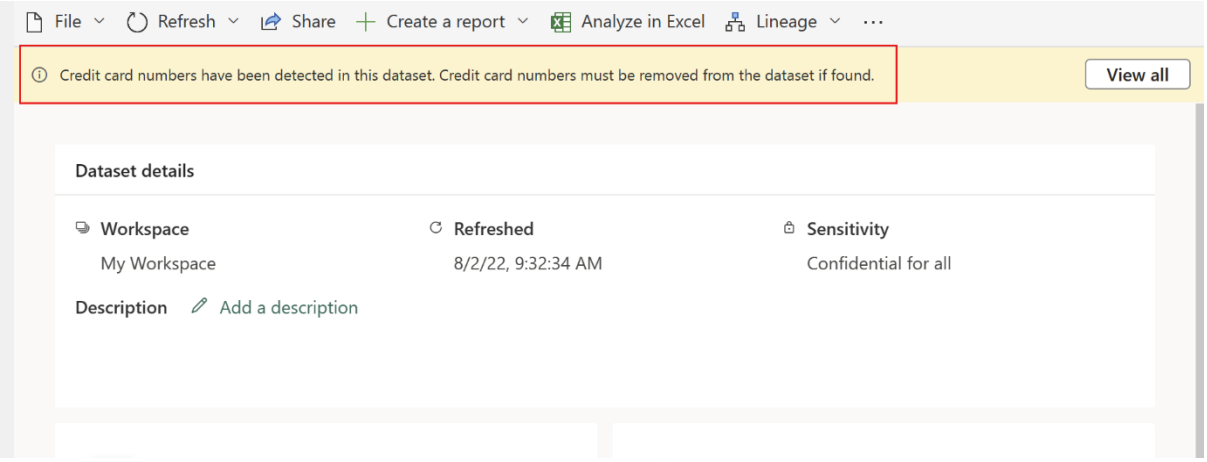
What happens when an item is flagged by a Fabric DLP policy

When a DLP policy detects an issue with an item:

- If "user notification" is enabled in the policy, the item will be marked in Fabric with an icon that indicates that a DLP policy has detected an issue with the item. Hover over the icon to display a hover card that provides an option to see the full details in a side panel. For more information about what you see in the side panel, see Respond to a DLP violation in Fabric.



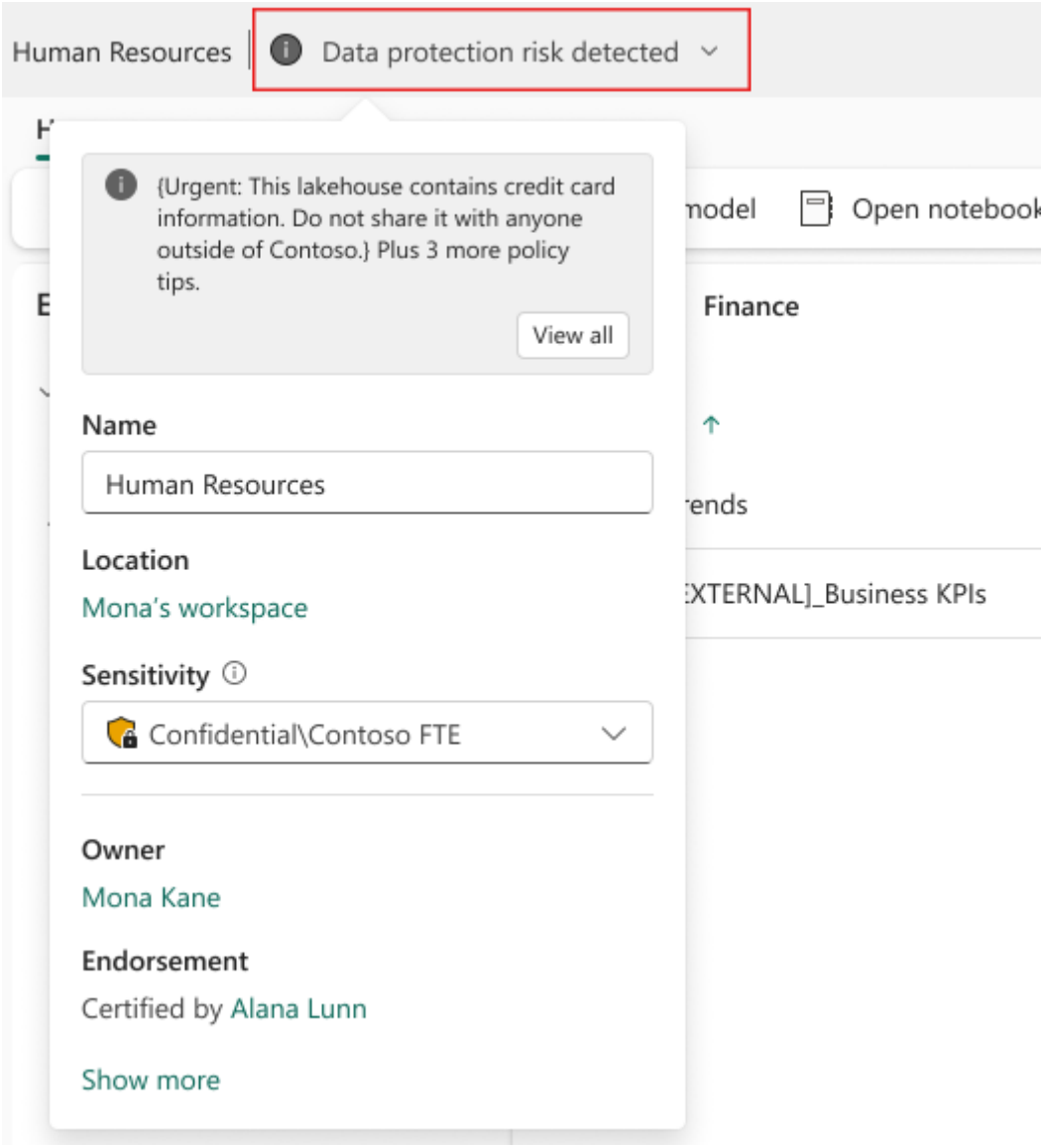
For semantic models, opening the details page will show a policy tip that explains the policy violation and how the type of sensitive information detected should be handled. Selecting **View all** opens a side panel with all the policy details.



Note

If you hide the policy tip, it doesn't get deleted. It will appear the next time you visit the page.

For lakehouses, the indication will appear in the header in edit mode, and opening the fly out makes it possible to see more details about the policy tips affecting the lakehouse. Selecting **View all** opens a side panel with all the policy details.



- If alerts are enabled in the policy, an alert will be recorded on the data loss prevention **Alerts** page in the Microsoft Purview portal, and (if configured) an email will be sent to administrators and/or specified users. For more information, see Monitor and manage DLP policy violations.

Securing items in a workspace

Organizational teams can have individual workspaces where different personas collaborate and work on generating content. Access to the items in the workspace is regulated via workspace roles assigned to users by the workspace admin.

Guidance: Data owners should recommend users who could be workspace administrators. These could be team leads in your organization, for example. These

workspace administrators should then govern access to the items in their workspace by assigning appropriate workspace roles to users and consumers of the items.

Securing data in Fabric items

Along with the broad security that gets applied at the tenant or workspace level, there are other data-level controls that can be deployed by individual teams to manage access to individual tables, rows, and columns. Fabric currently provides such data-level control for SQL analytics endpoints, Synapse Data Warehouses in Fabric, Direct Lake, and KQL Database.

Guidance: Individual teams are expected to apply these additional controls at the item and data level.

Auditing

To mitigate the risks of unauthorized access and use of your Fabric data, Fabric administrators and compliance teams in your organizations can track and investigate user activity on Fabric items using Purview Audit, which is available in the Purview compliance portal. Many companies also need these audit logs for regulatory requirements, which often mandate storing audit logs for forensic investigation and potential data regulation violations.

Guidance: Fabric administrators and compliance teams should be made aware that Fabric item-level audits are logged in Purview Audit and can be used for analysis.

Encourage data discovery, trust, and use

Fabric provides built-in capabilities to help users find and use reliable, quality data.

OneLake data hub

The OneLake data hub makes it easy to find, explore, and use the Fabric data items in your organization that you have access to. It provides information about the items and entry points for working with them. Filtering and search options make it easier to get to relevant data.

For more information, see Discover data items in the OneLake data hub.

Guidance: Carefully defining and setting up domains is essential for creating an efficient experience in the data hub. Carefully defined domains help set the context for teams and makes for better definition of boundaries and ownership. Mapping workspaces to domains is key to helping implement this in Fabric.

Endorsement

Endorsement is a way to make trustworthy, quality data more discoverable. Organizations often have large numbers of Microsoft Fabric items - data, processes, and content - available for sharing and reuse by their Fabric users. Endorsement helps users identify and find the trustworthy high-quality items they need. With endorsement, item owners can promote their quality items, and organizations can certify items that meet their quality standards. Endorsed items are then clearly labeled, both in Fabric and in other places where users look for Fabric items. Endorsed items are also given priority in some searches, and you can sort for endorsed items for in some lists. In the Microsoft Purview hub, admins can get insights about their organization's endorsed items in order to better drive users to quality content.

For more information, see Endorsement.

Guidance: Certification enablement should be delegated to domain admins, and the domain admins should authorize data owners and producers to be able to certify the items they create. The data owners and producers should then always certify their items that have been tested and are ready for use by other teams. This helps separate low-quality, nontrusted items from trusted, ready-to-use assets. It also makes these trusted assets easier to find. In addition, data consumers should be educated about how to find trusted assets, and encouraged to use only certified items in their reports and other downstream processing.

Data lineage and impact analysis

In modern business intelligence projects, understanding the flow of data from a data source to its destination is a complex task. Questions like "What happens if I change this data?" or "Why isn't this report up to date?" can be hard to answer. They might require a team of experts or deep investigation to understand. Lineage helps users understand the flow of data by providing a visualization that shows the relations between all the items in a workspace. For each item in the lineage view, you can display an impact analysis that shows what downstream items would be affected if you made changes to the item.

For more information, see Lineage and Impact analysis.

Guidance: We recommend using proper and consistent naming conventions for items. This can help while looking at lineage information.

Purview for governance across the org

Microsoft Purview offers solutions for protecting and governing data across an organization's entire data estate. The integration between Purview and Fabric makes it possible to use some of Purview's capabilities to govern and monitor your Fabric data in the context of your organization's entire data estates.

The data governance capabilities offered on Fabric via Purview's live view (preview) are described in the following sections. See also Use Microsoft Purview to govern Microsoft Fabric.

Data curation

Data curation in your organization involves gathering metadata information, lineage information, and others from all sources that your organization uses. These could be on-premises, third-party clouds, third-party products and services, or CRM systems to name a few. This extraction process is also referred to as scanning in Purview. All information is retrieved using built-in scanners in Purview that scan your organization's data estate to collect this information. In Purview this is executed by Data Map.

Data Map

Purview has a scanning engine that can scan and fetch metadata from disparate sources and populate Purview's data map. Purview exposes this metadata via Atlas APIs so that it can be consumed by external services or ISVs. Data Map also interacts with Fabric and gets its metadata populated internally, so that business users can search, find, and use these data products to build their insights. Currently, data consumers can look at all Fabric workspaces they have viewer access to. This is known as live view. On top of this, manual scans can be executed on all Fabric Items from Purview, where item level metadata is picked and made available for use in Purview. This is only available for the enterprise tier. Currently you can have lineage on an item level.

Data discovery in Purview

Data consumers who work with your data should be able to search and find the relevant data. Purview helps here by providing concepts of domains. Business-friendly terminology and groupings make it more relevant and easier to search for data which teams are interested in, based on terms they're familiar with. This also blends well with the data mesh architectural pattern. Data catalog is the application layer in Purview that helps teams search for data.

Guidance: Enterprise and business architecture teams should define domains and also a persona mapping between business and technical players to make roles and responsibilities clear. These definitions must be in line with the domain definitions in Fabric.

Data Catalog in Purview

Purview Data Catalog exposes the metadata captured from all sources feeding your data platform. With Data Catalog, customers can search for the data and items they're interested in working with without having to know which systems are holding your data. All Fabric item metadata is available inside Purview.

Monitor, uncover, get insights, and act

Monitoring hub

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

For more information, see Use the Monitoring hub.

Guidance: This capability should be exposed to developers and team members for monitoring scheduled workloads (such as a data flow or pipeline refresh), a Spark run, a data warehouse query, etc.

Capacity metrics

Guidance: Platform owners and users with platform administrator roles should be aware of this feature and use it to monitor usage and consumption. For more information, see What is the Microsoft Fabric Capacity Metrics app?.

Purview hub

Microsoft Purview hub is a centralized page in Fabric that helps Fabric administrators and data owners manage and govern their Fabric data estate. For administrators and data owners, the hub offers reports that provide insights about their Fabric items, particularly with respect to sensitivity labeling and endorsement. The hub also serves as a gateway to more advanced Purview capabilities such as Information Protection, Data Loss Prevention, and Audit. For more information, see Microsoft Purview hub.

Guidance: Data stewards and owners should be made aware of the Fabric's Purview hub and what it provides in terms of getting insights about your organization's sensitive and endorsed data.

Admin monitoring

The admin monitoring workspace provides admins with monitoring capabilities for their organization. Using the admin monitoring workspace resources, admins can perform security and governance tasks such as audits and usage checks. For more information, see What is the admin monitoring workspace?.

Guidance: We recommend that platform owners/Fabric administrators use this feature to gain an overall view of the Fabric platform.

Administer Fabric

Controlling feature access and capabilities allow you to comply with company policies and external rules and regulations. Fabric also allows admins to delegate their responsibilities. Delegation lets you create different groups of admins for different tasks in your organization. Delegating admin responsibilities can reduce pressure that might cause one admin team to become a bottleneck for organizational processes.

Administration

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

Grant licenses

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

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

Fabric admins can buy licenses and control them with tools such as capacity pause and resume and scale.

Assign admin roles

Fabric admins can assign and manage Fabric admin roles. Admin roles allow users to buy licenses, and control organizational settings. For example, as an admin you can access the admin center and manage your organization's tenant settings.

Customize a Fabric tenant

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

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

To distribute management across the organization, you can also use domains. With a domain, you create a logical grouping of workspaces. For example, your organization

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

Add and remove users

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

Govern and secure data

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

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

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

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

Control

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

Delegate admin rights

To avoid becoming a bottleneck for every single setting in your organization, a Fabric admin can delegate many of the controls to capacity, workspace, and domain admins. Delegating settings allows your organization to have several admins with different levels of admin rights in multiple logical locations within your organization.

For example, you can have a three admins with access to all the settings in your organization, and another admin for each team in your organization. The team admin can control settings and permissions relevant for the team, at the capacity, workspace, or domain level, depending on the way your organization is set up. You can also have multiple levels of admins in your organization, depending on your organization's needs.

Enable Fabric settings

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

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

Grant permissions

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

Monitor

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

Admin monitoring workspace

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

Monitoring hub

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

View audit logs

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

Prerequisites

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

Access

To access the audit logs, in Fabric go to the admin portal, select **Audit logs**, and then select **Go to Microsoft 365 Admin Center**.

Audit logs are also available directly through Microsoft Purview.

Search the audit logs

You can search the audit logs using the filters in the following list. When you combine filters, the search results show only items that match all of the filter criteria.

- **Activities** - Your search returns the selected activities.
- **Date and time range** - Search the logs by date range using the *Start date* and *End date* fields. The default selection is the past seven days. The display presents the date and time in UTC format. The maximum date range that you can specify is 90 days.
- **Users** - Search for activities performed by specific users. Enter one or more user names in the *Users* field. User names appear in email address format. Leave blank to return entries for all users (and service accounts) in your organization.
- **File, folder, or site** - Search by file name, folder name, or URL.

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

Understand consumption

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

Reviewing bills

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

Recover data

Fabric data resiliency ensures that your data is available if there is a disaster. Fabric also enables you to recover your data in case of a disaster, Disaster recovery. For more information, see Reliability in Microsoft Fabric.

Compliance

Adherence to compliance standards transcends mere rule-following. It represents a commitment to building software with a foundation of security, privacy, and quality. These frameworks, encompassing legal requirements, industry standards, and internal best practices, serve as guiding principles throughout the development process.

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

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

Business continuity and disaster recovery

When it comes to business continuity and disaster recovery (BCDR), Microsoft uses the shared responsibility model for disaster recovery (DR). In a shared responsibility model, Microsoft ensures that the baseline infrastructure and platform services are available. At the same time, many Azure services don't automatically replicate data or fall back from a failed region to cross-replicate to another enabled region. For those services, the customer is responsible for setting up a disaster recovery plan that works for their workload. Most services that run on Azure platform as a service (PaaS) offerings provide features and guidance to support DR, and you can use service-specific features to support fast recovery to help develop your DR plan.

DR is about recovering from high-impact events, such as natural disasters or failed deployments that result in downtime and data loss. Regardless of the cause, the best remedy for a disaster is a well-defined and tested DR plan and an application design that actively supports DR. Before you begin to think about creating your disaster recovery plan, see Recommendations for designing a disaster recovery strategy.

Security development lifecycle

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

Compliance offerings

Compliance offerings are grouped into four segments: **globally applicable**, **US government**, **industry specific**, and **region/country specific**. Compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Each offering description provides links to downloadable resources to assist you with your own compliance obligations. You can access Azure and other Microsoft cloud services audit documentation via the Service Trust Portal (STP).

While certifications typically occur after a product launch (Generally Available or GA), Microsoft integrates compliance best practices throughout the development lifecycle. This proactive approach ensures a strong foundation for future certifications, even though they follow established audit cycles. In simpler terms, Microsoft prioritizes building compliance in from the start, even if formal certification comes later.

Compliance is a shared responsibility. To comply with laws and regulations, cloud service providers and their customers enter a shared responsibility to ensure that each does their part.

- Compliance Offerings - Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Learn
- Audit Reports - Service Trust Portal Home Page (microsoft.com)
- Compliance is a Shared Responsibility - Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn
- Azure compliance - Azure - Compliance Offerings

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

Reliability in Microsoft Fabric

Microsoft Fabri supports both regional resiliency with availability zones and cross-region recovery and business continuity.

Availability zone support

Azure availability zones are at least three physically separate groups of datacenters within each Azure region. Datacenters within each zone are equipped with independent power, cooling, and networking infrastructure. In the case of a local zone failure, availability zones are designed so that if the one zone is affected, regional services, capacity, and high availability are supported by the remaining two zones.

Failures can range from software and hardware failures to events such as earthquakes, floods, and fires. Tolerance to failures is achieved with redundancy and logical isolation of Azure services. For more detailed information on availability zones in Azure, see Regions and availability zones.

Azure availability zones-enabled services are designed to provide the right level of reliability and flexibility. They can be configured in two ways. They can be either zone redundant, with automatic replication across zones, or zonal, with instances pinned to a specific zone. You can also combine these approaches. For more information on zonal vs. zone-redundant architecture, see Recommendations for using availability zones and regions.

Fabric makes commercially reasonable efforts to support zone-redundant availability zones, where resources automatically replicate across zones, without any need for you to set up or configure.

Prerequisites

- Fabric currently provides partial availability-zone support in a limited number of regions. This partial availability-zone support covers experiences (and/or certain functionalities within an experience).
- Experiences such as Data Factory (pipelines), Data Engineering, Data Science, and Event Streams don't support availability zones.
- Zone availability may or may not be available for Fabric experiences or features/functionalities that are in preview.
- On-premises gateways and large semantic models in Power BI don't support availability zones.

Supported regions

Fabric makes commercially reasonable efforts to provide availability zone support in various regions as follows: Reliability in Microsoft Fabric | Microsoft Learn

Zone down experience

During a zone-wide outage, no action is required during zone recovery. Fabric capabilities in regions listed in supported regions self-heal and rebalance automatically to take advantage of the healthy zone.

Important

While Microsoft strives to provide uniform and consistent availability zone support, in some cases of availability-zone failure, Fabric capacities located in Azure regions with higher customer demand fluctuations might experience higher than normal latency.

Cross-region disaster recovery and business continuity

Disaster recovery (DR) is about recovering from high-impact events, such as natural disasters or failed deployments that result in downtime and data loss. Regardless of the cause, the best remedy for a disaster is a well-defined and tested DR plan and an application design that actively supports DR. Before you begin to think about creating your disaster recovery plan, see Recommendations for designing a disaster recovery strategy.

When it comes to DR, Microsoft uses the shared responsibility model. In a shared responsibility model, Microsoft ensures that the baseline infrastructure and platform services are available. At the same time, many Azure services don't automatically replicate data or fall back from a failed region to cross-replicate to another enabled region. For those services, you are responsible for setting up a disaster recovery plan that works for your workload. Most services that run on Azure platform as a service (PaaS) offerings provide features and guidance to support DR and you can use service-specific features to support fast recovery to help develop your DR plan.

This section describes a disaster recovery plan for Fabric that's designed to help your organization keep its data safe and accessible when an unplanned regional disaster occurs. The plan covers the following topics:

- **Cross-region replication**: Fabric offers cross-region replication for data stored in OneLake. You can opt in or out of this feature based on your requirements.
- **Data access after disaster**: In a regional disaster scenario, Fabric guarantees data access, with certain limitations. While the creation or modification of new items is restricted after failover, the primary focus remains on ensuring that existing data remains accessible and intact.
- **Guidance for recovery**: Fabric provides a structured set of instructions to guide you through the recovery process. The structured guidance makes it easier for you to transition back to regular operations.

Power BI, now a part of the Fabric, has a solid disaster recovery system in place and offers the following features:

- **BCDR as default**: Power BI automatically includes disaster recovery capabilities in its default offering. You don't need to opt in or activate this feature separately.
- **Cross-region replication**: Power BI uses Azure storage geo-redundant replication and Azure SQL geo-redundant replication to guarantee that backup instances exist in other regions and can be used. This means that data is duplicated across different regions, enhancing its availability, and reducing the risks associated with regional outages.
- **Continued services and access after disaster**: Even during disruptive events, Power BI items remain accessible in read-only mode. Items include semantic models, reports, and dashboards, ensuring that businesses can continue their analysis and decision-making processes without significant hindrance.

For more information, see the Power BI high availability, failover, and disaster recovery FAQ

Important

For customers whose home regions don't have an Azure pair region and are affected by a disaster, the ability to utilize Fabric capacities may be compromised—even if the data within those capacities is replicated. This limitation is tied to the home region's infrastructure, essential for the capacities' operation.

Home region and capacity functionality

For effective disaster recovery planning, it's critical that you understand the relationship between your home region and capacity locations. Understanding home region and capacity locations helps you make strategic selections of capacity regions, as well as the corresponding replication and recovery processes.

The **home region** for your organization's tenancy and data storage is set to the billing address location of the first user that signs up. For further details on tenancy setup, go to Power BI implementation planning: Tenant setup. When you create new capacities, your data storage is set to the home region by default. If you wish to change your data storage region to another region, you'll need to enable Multi-Geo, a Fabric Premium feature.

Important

Choosing a different region for your capacity doesn't entirely relocate all of your data to that region. Some data elements still remain stored in the home region. To see which data remains in the home region and which data is stored in the Multi-Geo enabled region, see **Configure Multi-Geo support for Fabric Premium**.

In the case of a home region that doesn't have a paired region, capacities in any Multi-Geo enabled region may face operational issues if the home region encounters a disaster, as the core service functionality is tethered to the home region.

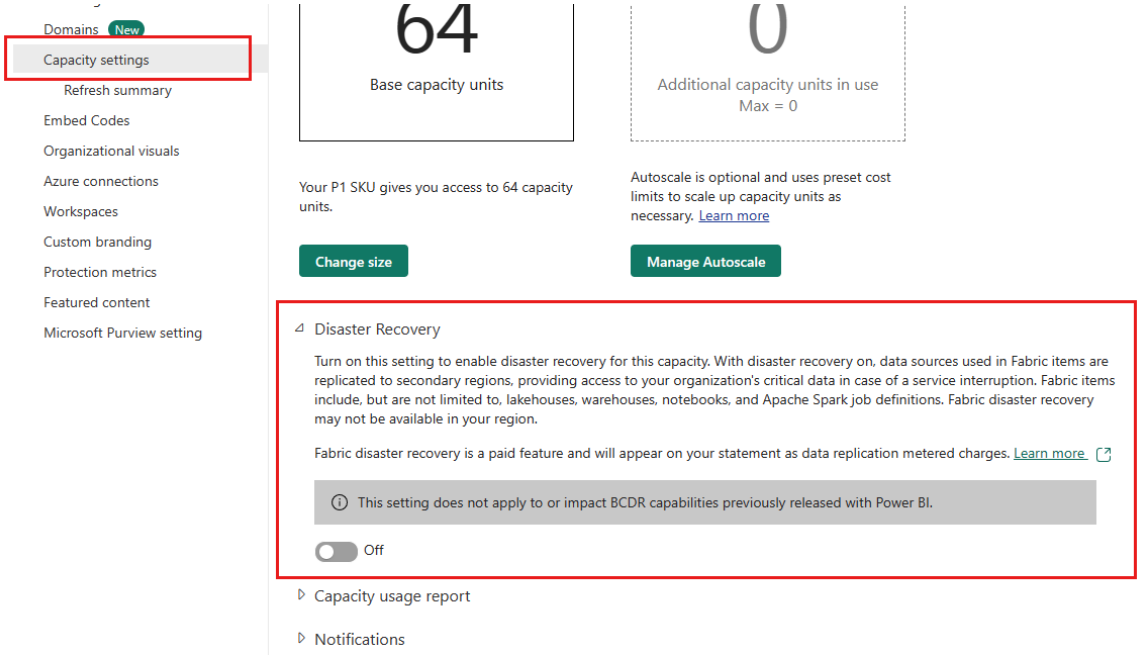
If you select a Multi-Geo enabled region within the EU, it's guaranteed that your data is stored within the EU data boundary.

To learn how to identify your home region, see Find your Fabric home region.

Disaster recovery capacity setting

Fabric provides a disaster recovery switch on the capacity settings page. It's available where Azure regional pairings align with Fabric's service presence. Here are the specifics of this switch:

- **Role access**: Only users with the capacity admin role or higher can use this switch.
- **Granularity**: The granularity of the switch is the capacity level. It's available for both Premium and Fabric capacities.
- **Data scope**: The disaster recovery toggle specifically addresses OneLake data, which includes Lakehouse and Warehouse data. **The switch does not influence your data stored outside OneLake.**
- **BCDR continuity for Power BI**: While disaster recovery for OneLake data can be toggled on and off, BCDR for Power BI is always supported, regardless of whether the switch is on or off.
- **Frequency**: Once you change the disaster recovery capacity setting, you must wait 30 days before being able to alter it again. The wait period is set in place to maintain stability and prevent constant toggling,



Note

After turning on the disaster recovery capacity setting, it can take up to 72 hours for the data to start replicating.

Data replication

When you turn on the disaster recovery capacity setting, cross-region replication is enabled as a disaster recovery capability for OneLake data. The Fabric platform aligns with Azure regions to provision the geo-redundancy pairs. However, some regions don't have an Azure pair region, or the pair region doesn't support Fabric. For these regions, data replication isn't available. For more information, see Regions with availability zones and no region pair and Fabric region availability.

Note

While Fabric offers a data replication solution in OneLake to support disaster recovery, there are notable limitations. For instance, the data of KQL databases and query sets is stored externally to OneLake, which means that a separate disaster recovery approach is needed. Refer to the rest of this document for details of the disaster recovery approach for each Fabric item.

Billing

The disaster recovery feature in Fabric enables geo-replication of your data for enhanced security and reliability. This feature consumes more storage and transactions, which are billed as BCDR Storage and BCDR Operations respectively.

You can monitor and manage these costs in the Microsoft Fabric Capacity Metrics app, where they appear as separate line items.

For an exhaustive breakdown of all associated disaster recovery costs to help you plan and budget accordingly, see OneLake compute and storage consumption.

Set up disaster recovery

While Fabric provides disaster recovery features to support data resiliency, you **must** follow certain manual steps to restore service during disruptions. This section details the actions you should take to prepare for potential disruptions.

Phase 1: Prepare

- **Activate the disaster recovery capacity settings**: Regularly review and set the disaster recovery capacity settings to make sure they meet your protection and performance needs.
- **Create data backups**: Copy critical data stored outside of OneLake to another region in a way that aligns to your disaster recovery plan.

Phase 2: Disaster failover

When a major disaster renders the primary region unrecoverable, Microsoft Fabric initiates a regional failover. Access to the Fabric portal is unavailable until the failover is complete and a notification is posted on the Microsoft Fabric support page.

The time it takes for failover to complete can vary, although it typically takes less than one hour. Once failover is complete, here's what you can expect:

- **Fabric portal**: You can access the portal, and read operations such as browsing existing workspaces and items continue to work. All write operations, such as creating or modifying a workspace, are paused.
- **Power BI**: You can perform read operations, such as displaying dashboards and reports. Refreshes, report publish operations, dashboard and report modifications, and other operations that require changes to metadata aren't supported.
- **Lakehouse/Warehouse**: You can't open these items, but files can be accessed via OneLake APIs or tools.
- **Spark Job Definition**: You can't open Spark job definitions, but code files can be accessed via OneLake APIs or tools. Any metadata or configuration will be saved after failover.
- **Notebook**: You can't open notebooks, and code content won't be saved after the disaster.

- **ML Model/Experiment**: You can't open ML models or experiments. Code content and metadata such as run metrics and configurations won't be saved after the disaster.
- **Dataflow Gen2/Pipeline/Eventstream**: You can't open these items, but you can use supported disaster recovery destinations (lakehouses or warehouses) to protect data.
- **KQL Database/Queryset**: You won't be able to access KQL databases and query sets after failover. More prerequisite steps are required to protect the data in KQL databases and query sets.

In a disaster scenario, the Fabric portal and Power BI are in read-only mode, and other Fabric items are unavailable, you can access their data stored in OneLake using APIs or third-party tools. Both portal and Power BI retain the ability to perform read-write operations on that data. This ability ensures that critical data remains accessible and modifiable, and mitigates potential disruption of your business operations.

OneLake data remains accessible through multiple channels:

- OneLake ADLS Gen2 API: See Connecting to Microsoft OneLake
- Examples of tools that can connect to OneLake data:
    - Azure Storage Explorer: See Integrate OneLake with Azure Storage Explorer
    - OneLake File Explorer: See Use OneLake file explorer to access Fabric data

Phase 3: Recovery plan

While Fabric ensures that data remains accessible after a disaster, you can also act to fully restore their services to the state before the incident. This section provides a step-by-step guide to help you through the recovery process.

Recovery steps

1. Create a new Fabric capacity in any region after a disaster. Given the high demand during such events, we recommend selecting a region outside your primary geo to increase likelihood of compute service availability. For information about creating a capacity, see Buy a Microsoft Fabric subscription.
2. Create workspaces in the newly created capacity. If necessary, use the same names as the old workspaces.
3. Create items with the same names as the ones you want to recover. This step is important if you use the custom script to recover lakehouses and warehouses.

4. Restore the items. For each item, follow the relevant section in the Experience-specific disaster recovery guidance to restore the item.

Microsoft Fabric end-to-end scenario: security focus

Security is a key aspect of any data analytics solution, especially when it involves sensitive or confidential data. For this reason, Microsoft Fabric provides a comprehensive set of security features that enables you to protect your data at rest and in transit, as well as control access and permissions for your users and applications.

Background

This article presents a scenario where you're a data engineer who works for a healthcare organization in the United States. The organization collects and analyzes patient data that's sourced from various systems, including electronic health records, lab results, insurance claims, and wearable devices.

You plan to build a lakehouse by using the medallion architecture in Fabric, which consists of three layers: bronze, silver, and gold.

- The *bronze layer* stores the raw data as it arrives from the data sources.
- The *silver layer* applies data quality checks and transformations to prepare the data for analysis.
- The *gold layer* provides aggregated and enriched data for reporting and visualization.

While some data sources are located on your on-premises network, others are behind firewalls and require secure, authenticated access. There are also some data sources that are managed in Azure, such as Azure SQL Database and Azure Storage. You need to connect to these Azure data sources in a way that doesn't expose data to the public internet.

You've decided to use Fabric because it can securely ingest, store, process, and analyze your data in the cloud. Importantly, it does so while complying with the regulations of your industry and policies of your organization.

Because Fabric is software as a service (SaaS), you don't need to provision individual resources, such as storage or compute resources. All you need is a Fabric capacity.

You need to set up data access requirements. Specifically, you need to ensure that only you and your fellow data engineers have access to the data in the bronze and

silver layers of the lakehouse. These layers are where you plan to perform data cleansing, validation, transformation, and enrichment. You also need to restrict access to the data in the gold layer. Only authorized users, including data analysts and business users, should have access to the gold layer. They require this access to use the data for various analytical purposes, such as reporting, machine learning, and predictive analytics. Data access needs to be further restricted by the role and department of the user.

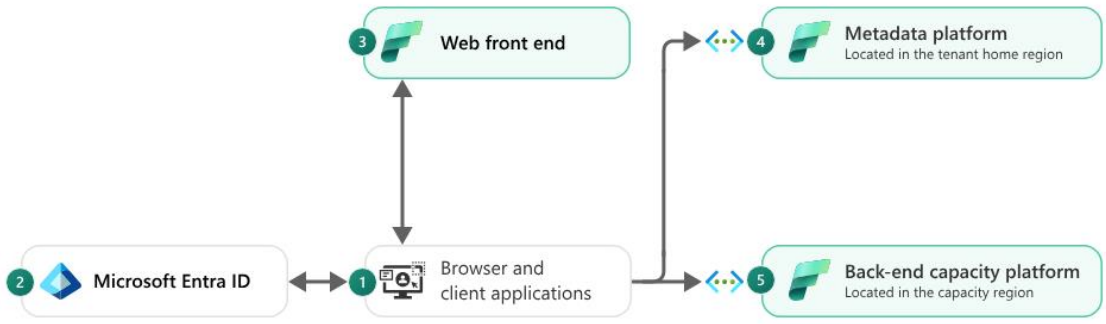
Connect to Fabric (inbound protection)

You first set up *inbound protection*, which is concerned with how you and other users sign in and have access to Fabric.

Because Fabric is deployed to a Microsoft Entra tenant, authentication and authorization are handled by Microsoft Entra. You sign in with a Microsoft Entra organization account (work or school account). Next, you consider how other users will connect to Fabric.

The Microsoft Entra tenant is an *identity security boundary* that's under the control of your IT department. Within this security boundary, the administration of Microsoft Entra objects (such as user accounts) and the configuration of tenant-wide settings are done by your IT administrators. Like any SaaS service, Fabric logically isolates tenants. Data and resources in your tenant can't ever be accessed by other tenants unless you explicitly authorize them to do so.

Here's what happens when a user signs in to Fabric.



Item	Description
1	The user opens a browser (or a client application) and signs in to the Fabric portal.

2	The user is immediately redirected to Microsoft Entra ID, and they're required to authenticate. Authentication verifies that it's the correct person signing in.
3	After authentication succeeds, the web front end receives the user's request and delivers the front-end (HTML and CSS) content from the nearest location. It also routes the request to the metadata platform and backend capacity platform.
4	The metadata platform, which resides in your tenant's home region, stores your tenant's metadata, such as workspaces and access controls. This platform ensures that the user is authorized to access the relevant workspaces and Fabric items.
5	The back-end capacity platform performs compute operations and stores your data. It's located in the capacity region. When a workspace is assigned to Fabric capacity, all data that resides in the workspace, including the data lake OneLake, is stored and processed in the capacity region.

The metadata platform and the back-end capacity platform each run in secured virtual networks. These networks expose a series of secure endpoints to the internet so that they can receive requests from users and other services. Apart from these endpoints, services are protected by network security rules that block access from the public internet.

When users sign in to Fabric, you can enforce other layers of protection. That way, your tenant will only be accessible to certain users *and* when other conditions, like network location and device compliance, are met. This layer of protection is called inbound protection.

In this scenario, you're responsible for sensitive patient information in Fabric. So, your organization has mandated that all users who access Fabric must perform multifactor authentication (MFA), and that they must be on the corporate network—just securing user identity isn't enough.

Your organization also provides flexibility for users by allowing them to work from anywhere and to use their personal devices. Because Microsoft Intune supports bring-your-own-device (BYOD), you enroll approved user devices in Intune.

Further, you need to ensure that these devices comply with the organization policies. Specifically, these policies require that devices can only connect when they have the latest operating system installed and the latest security patches. You set up these security requirements by using Microsoft Entra Conditional Access.

Conditional Access offers several ways to secure your tenant. You can:

- Grant or block access by network location.
- Block access to devices that run on unsupported operating systems.
- Require a compliant device, Intune-joined device, or MFA for all users.
- And more.

In the case that you need to lock down your entire Fabric tenant, you can use a virtual network and block public internet access. Access to Fabric is then only allowed from within that secure virtual network. This requirement is set up by enabling private links at the tenant level for Fabric. It ensures that all Fabric endpoints resolve to a private IP address in your virtual network, including access to all your Power BI reports. (Enabling private endpoints impacts on many Fabric items, so you should thoroughly read this article before enabling them.)

Secure access to data outside of Fabric (outbound protection)

Next, you set up *outbound protection*, which is concerned with securely accessing data behind firewalls or private endpoints.

Your organization has some data sources that are located on your on-premises network. Because these data sources are behind firewalls, Fabric requires secure access. To allow Fabric to securely connect to your on-premises data source, you install an on-premises data gateway.

The gateway can be used by Data Factory dataflows and data pipelines to ingest, prepare, and transform the on-premises data, and then load it to OneLake with a copy activity. Data Factory supports a comprehensive set of connectors that enable you to connect to more than 100 different data stores.

You then build dataflows with Power Query, which provides an intuitive experience with a low-code interface. You use it to ingest data from your data sources, and transform it by using any of 300+ data transformations. You then build and orchestrate a complex extract, transform, and load (ETL) process with data pipelines. You ETL processes can refresh dataflows and perform many different tasks at scale, processing petabytes of data.

In this scenario, you already have multiple ETL processes. First, you have some pipelines in Azure Data Factory (ADF). Currently, these pipelines ingest your on-premises data and load it into a data lake in Azure Storage by using the self-hosted integration runtime. Second, you have a data ingestion framework in Azure Databricks that's written in Spark.

Now that you're using Fabric, you simply redirect the output destination of the ADF pipelines to use the lakehouse connector. And, for the ingestion framework in Azure Databricks, you use the OneLake APIs that supports the Azure Blog Filesystem (ABFS) driver to integrate OneLake with Azure Databricks. (You could also use the same method to integrate OneLake with Azure Synapse Analytics by using Apache Spark.)

You also have some data sources that are in Azure SQL Database. You need to connect to these data sources by using private endpoints. In this case, you decide to set up a virtual network (VNet) data gateway and use dataflows to securely connect to your Azure data and load it into Fabric. With VNet data gateways, you don't have to provision and manage the infrastructure (as you need to do for on-premises data gateway). That's because Fabric securely and dynamically creates the containers in your Azure Virtual Network.

If you're developing or migrating your data ingestion framework in Spark, then you can connect to data sources in Azure securely and privately from Fabric notebooks and jobs with the help of managed private endpoints. Managed private endpoints can be created in your Fabric workspaces to connect to data sources in Azure that have blocked public internet access. They support private endpoints, such as Azure SQL Database and Azure Storage. Managed private endpoints are provisioned and managed in a managed VNet that's dedicated to a Fabric workspace. Unlike your typical Azure Virtual Networks, managed VNets and managed private endpoints won't be found in the Azure portal. That's because they're fully managed by Fabric, and you find them in your workspace settings.

Because you already have a lot of data stored in Azure Data Lake Storage (ADLS) Gen2 accounts, you now only need to connect Fabric workloads, such as Spark and Power BI, to it. Also, thanks to OneLake ADLS shortcuts, you can easily connect to your existing data from any Fabric experience, such as data integration pipelines, data engineering notebooks, and Power BI reports.

Fabric workspaces that have a workspace identity can securely access ADLS Gen2 storage accounts, even when you've disabled the public network. That's made possible by trusted workspace access. It allows Fabric to securely connect to the storage accounts by using a Microsoft backbone network. That means communication doesn't use the public internet, which allows you to disable public network access to the storage account but still allow certain Fabric workspaces to connect to them.

Compliance

You want to use Fabric to securely ingest, store, process, and analyze your data in the cloud, while maintaining compliance with the regulations of your industry and the policies of your organization.

Fabric is part of Microsoft Azure Core Services, and it's governed by the Microsoft Online Services Terms and the Microsoft Enterprise Privacy Statement. While certifications typically occur after a product launch (Generally Available, or GA), Microsoft integrates compliance best practices from the outset and throughout the development lifecycle. This proactive approach ensures a strong foundation for future certifications, even though they follow established audit cycles. In simpler terms, we prioritize building compliance in from the start, even when formal certification comes later.

Fabric is compliant with many industry standards such as ISO 27001, 27017, 27018 and 27701. Fabric is also HIPAA compliant, which is critical to healthcare data privacy and security. You can check the Appendix A and B in the Microsoft Azure Compliance Offerings for detailed insight into which cloud services are in scope for the certifications. You can also access the audit documentation from the Service Trust Portal (STP).

Compliance is a shared responsibility. To comply with laws and regulations, cloud service providers and their customers enter a shared responsibility to ensure that each does their part. As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks the cloud provider handles and which tasks you handle.

Data handling

Because you're dealing with sensitive patient information, you need to ensure that all your data is sufficiently protected both at rest and in transit.

Encryption at rest provides data protection for stored data (at rest). Attacks against data at rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the data on that hardware. Encryption at rest is designed to prevent an attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. Encryption at rest is a mandatory measure required for compliance with some of the industry standards and regulations, such as the International Organization for Standardization (ISO) and Health Insurance Portability and Accountability Act (HIPAA).

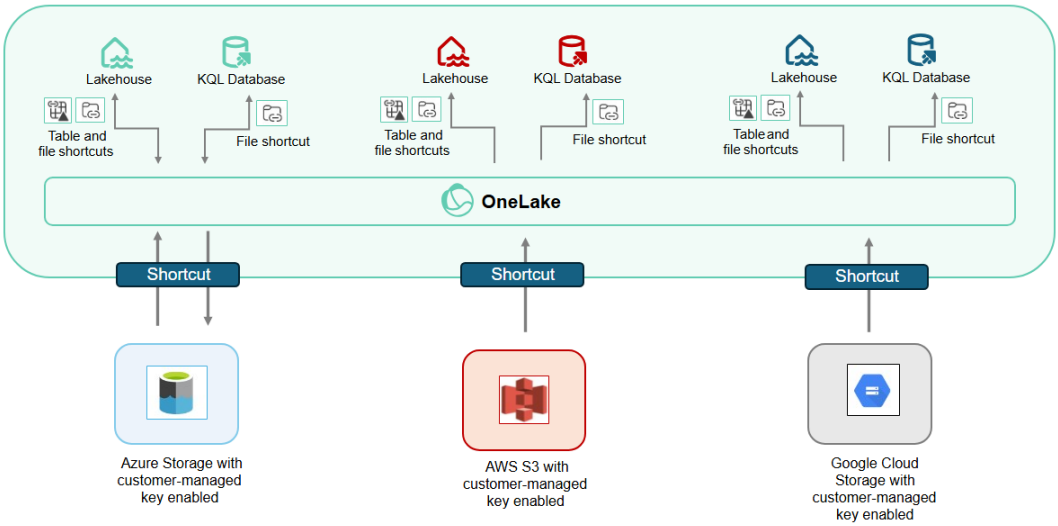
All Fabric data stores are encrypted at rest by using Microsoft-managed keys, which provides protection for customer data and also system data and metadata. Data is never persisted to permanent storage while in an unencrypted state. With Microsoft-managed keys, you benefit from the encryption of your data at rest without the risk or cost of a custom key management solution.

Data is also encrypted in transit. All inbound traffic to Fabric endpoints from the client systems enforces a minimum of Transport Layer Security (TLS) 1.2. It also negotiates TLS 1.3, whenever possible. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

In addition to encryption, network traffic between Microsoft services always routes over the Microsoft global network, which is one of the largest backbone networks in the world.

Customer-managed key (CMK) encryption and Microsoft Fabric

Customer-managed keys (CMK) allows you to encrypt data at-rest using your own keys. By default, Microsoft Fabric encrypts data-at-rest using platform managed keys. In this model, Microsoft is responsible for all aspects of key management and data-at-rest on OneLake is encrypted using its keys. From a compliance perspective, customers may have a requirement to use CMK to encrypt data-at-rest. In the CMK model, customer assumes full control of the key and uses their key(s) to encrypt data-at-rest.



If you have a requirement to use CMK to encrypt data-at-rest, we recommend you use cloud storage services (ADLS Gen2, AWS S3, GCS) with CMK encryption enabled and access data from Microsoft Fabric using OneLake shortcuts. In this pattern, your data continues to reside on a cloud storage service or an external storage solution where encryption at rest using CMK is enabled, and you can perform in-place read operations from Fabric whilst staying compliant. Once a shortcut has been created, within Fabric, the data can be accessed by other Fabric experiences.

There are some considerations for using this pattern:

- Use the pattern discussed here for data which has encryption at-rest requirement using CMK. Data which does not have this requirement can be encrypted at-rest using platform-managed keys, and that data can be stored natively on Microsoft Fabric OneLake.
- Fabric Lakehouse and KQL database are the two workloads within Microsoft Fabric which support creation of shortcuts. In this pattern where data continues to reside on an external storage service where CMK is enabled, you can use shortcuts within Lakehouses and KQL databases to bring your data into Microsoft Fabric for analysis, but data is physically stored outside of OneLake where CMK encryption is enabled.
- ADLS Gen2 shortcut supports write and using this shortcut type, you can also write data back out to storage service, and it'll be encrypted at-rest using CMK. While using CMK with ADLS Gen2, following considerations for Azure Key Vault (AKV) and Azure Storage apply.
- If you are using a third-party storage solution which is AWS S3 compatible (Cloudflare, Qumolo Core with public endpoint, Public MinIO and Dell ECS with public endpoint) and it has CMK enabled, the pattern discussed here in this document can be extended to these third-party storage solutions. Using Amazon S3 compatible shortcut, you can bring data into Fabric using a shortcut from these solutions. As with cloud-based storage services, you can store the data on external storage with CMK encryption, and carry out in-place reads so that data.
- AWS S3 supports encryption at-rest using customer-managed keys. Fabric can perform in-place reads on S3 buckets using S3 shortcut; however, write operations using a shortcut to AWS S3 are not supported.

- Google cloud storage supports data encryption using customer-managed keys. Fabric can perform in-place reads on GCS; however, write operations using a shortcut to GCS are not supported.
- Enable audit for Microsoft Fabric to keep track of activities.
- In Microsoft Fabric, Power BI experience supports customer-managed key.

Data residency

As you're dealing with patient data, for compliance reasons your organization has mandated that data should never leave the United States geographical boundary. Your organization's main operations take place in New York and your head office in Seattle. While setting up Power BI, your organization has chosen the East US region as the tenant home region. For your operations, you have created a Fabric capacity in the West US region, which is closer to your data sources. Because OneLake is available around the globe, you're concerned whether you can meet your organization's data residency policies while using Fabric.

In Fabric, you learn that you can create Multi-Geo capacities, which are capacities located in geographies (geos) other than your tenant home region. You assign your Fabric workspaces to those capacities. In this case, compute and storage (including OneLake and experience-specific storage) for all items in the workspace reside in the multi-geo region, while your tenant metadata remains in the home region. Your data will only be stored and processed in these two geographies, thus ensuring your organization's data residency requirements are met.

Access control

You need to ensure that only you and your fellow data engineers have full access to the data in the bronze and silver layers of the lakehouse. These layers allow you to perform data cleansing, validation, transformation, and enrichment. You need to restrict access to the data in the gold layer to only authorized users, such as data analysts and business users, who can use the data for various analytical purposes, such as reporting and analytics.

Fabric provides a flexible permission model that allows you to control access to items and data in your workspaces. A workspace is a securable logical entity for grouping items in Fabric. You use workspace roles to control access to items in the workspaces. The four basic roles of a workspace are:

- **Admin:** Can view, modify, share, and manage all content in the workspace, including managing permissions.
- **Member:** Can view, modify, and share all content in the workspace.
- **Contributor:** Can view and modify all content in the workspace.
- **Viewer:** Can view all content in the workspace, but can't modify it.

In this scenario, you create three workspaces, one for each of the medallion layers (bronze, silver, and gold). Because you created the workspace, you're automatically assigned to the *Admin* role.

You then add a security group to the *Contributor* role of those three workspaces. Because the security group includes your fellow engineers as members, they're able to create and modify Fabric items in those workspaces—however they can't share any items with anyone else. Nor can they grant access to other users.

In the bronze and silver workspaces, you and your fellow engineers create Fabric items to ingest data, store the data, and process the data. Fabric items comprise a lakehouse, pipelines, and notebooks. In the gold workspace, you create two lakehouses, multiple pipelines and notebooks, and a Direct Lake semantic model, which delivers fast query performance of data stored in one of the lakehouses.

You then give careful consideration to how the data analysts and business users can access the data they're allowed to access. Specifically, they can only access data that's relevant to their role and department.

The first lakehouse contains the actual data and doesn't enforce any data permissions in its SQL analytics endpoint. The second lakehouse contains shortcuts to the first lakehouse, and it enforces granular data permissions in its SQL analytics endpoint. The semantic model connects to the first lakehouse. To enforce appropriate data permissions for the users (so they can only access data that's relevant to their role and department), you don't share the first lakehouse with the users. Instead, you share only the Direct Lake semantic model and the second lakehouse that enforces data permissions in its SQL analytics endpoint.

You set up the semantic model to use a fixed identity, and then implement row-level security (RLS) in the semantic model to enforce model rules to govern what data the users can access. You then share only the semantic model with the data analysts and business users because they shouldn't access the other items in the workspace, such as the pipelines and notebooks. Lastly, you grant Build permission on the semantic

model so that the users can create Power BI reports. That way, the semantic model becomes a *shared* semantic model and a source for their Power BI reports.

Your data analysts need access to the second lakehouse in the gold workspace. They'll connect to the SQL analytics endpoint of that lakehouse to write SQL queries and perform analysis. So, you share that lakehouse with them and provide access only to objects they need (such as tables, rows, and columns with masking rules) in the lakehouse SQL analytics endpoint by using the SQL security model. Data analysts can now only access data that's relevant to their role and department and they can't access the other items in the workspace, such as the pipelines and notebooks.

Common security scenarios

The following table lists common security scenarios and the tools you can use to accomplish them.

Expand table

Scenario	Tools	Direction
I'm an **ETL developer** and I want to load large volumes of data to Fabric at-scale from multiple source systems and tables. The source data is on-premises (or other cloud) and is behind firewalls and/or Azure data sources with private endpoints.	Use on-premises data gateway with data pipelines (copy activity).	Outbound
I'm a **power user** and I want to load data to Fabric from source systems that I have access to. Because I'm not a developer, I need to transform the data by using a low-code interface. The source data is on-premises (or other cloud) and is behind firewalls.	Use on-premises data gateway with Dataflow Gen 2.	Outbound
I'm a **power user** and I want to load data in Fabric from source systems that I have access to. The source data is in Azure behind private endpoints, and I don't want to install and maintain on-premises data gateway infrastructure.	Use a VNet data gateway with Dataflow Gen 2.	Outbound

I'm a **developer** who can write data ingestion code by using Spark notebooks. I want to load data in Fabric from source systems that I have access to. The source data is in Azure behind private endpoints, and I don't want to install and maintain on-premises data gateway infrastructure.	Use Fabric notebooks with Azure private endpoints.	Outbound
I have many existing pipelines in Azure Data Factory (ADF) and Synapse pipelines that connect to my data sources and load data into Azure. I now want to modify those pipelines to load data into Fabric.	Use the Lakehouse connector in existing pipelines.	Outbound
I have a data ingestion framework developed in Spark that connects to my data sources securely and loads them into Azure. I'm running it on Azure Databricks and/or Synapse Spark. I want to continue using Azure Databricks and/or Synapse Spark to load data into Fabric.	Use the OneLake and the Azure Data Lake Storage (ADLS) Gen2 API (Azure Blob Filesystem driver)	Outbound
I want to ensure that my Fabric endpoints are protected from the public internet.	As a SaaS service, the Fabric back end is already protected from the public internet. For more protection, use Microsoft Entra conditional access policies for Fabric and/or enable private links at tenant level for Fabric and block public internet access.	Inbound
I want to ensure that Fabric can be accessed from only within my corporate network and/or from compliant devices.	Use Microsoft Entra conditional access policies for Fabric.	Inbound
I want to ensure that anyone accessing Fabric must perform multifactor authentication.	Use Microsoft Entra conditional access policies for Fabric.	Inbound

I want to lock down my entire Fabric tenant from the public internet and allow access only from within my virtual networks.	Enable private links at tenant level for Fabric and block public internet access.	Inbound

Further reading

This document is based on online Microsoft documentation:

- Security in Microsoft Fabric - Microsoft Fabric | Microsoft Learn
- Microsoft Fabric security fundamentals - Microsoft Fabric | Microsoft Learn
- Protect inbound traffic - Microsoft Fabric | Microsoft Learn
- On-premises data gateway architecture | Microsoft Learn
- Virtual network (VNet) data gateway architecture | Microsoft Learn
- Privacy, security, and responsible use for Copilot in Microsoft Fabric (preview) - Microsoft Fabric | Microsoft Learn
- Governance and compliance in Microsoft Fabric - Microsoft Fabric | Microsoft Learn
- Administration overview - Microsoft Fabric | Microsoft Learn
- Standards compliance in Microsoft Fabric - Microsoft Fabric | Microsoft Learn
- Reliability in Microsoft Fabric | Microsoft Learn
- Microsoft Fabric end-to-end security scenario - Microsoft Fabric | Microsoft Learn