

Administer a Microsoft Fabric environment

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/1-introduction>

Introduction

Completed

Administering a Microsoft Fabric environment involves tasks that are essential for ensuring the efficient and effective use of the Fabric platform within an organization.

As a Fabric administrator (admin), you need to know:

- Fabric architecture
- Security and governance features
- Analytics capabilities
- Deployment and licensing options

You also need to be familiar with the Fabric admin portal and other administrative tools, and be able to configure and manage the Fabric environment to meet the needs of your organization.

Fabric admins work with business users, data analysts, and IT professionals to deploy and use Fabric to meet business objectives and comply with organizational policies and standards.

By the end of this module, you'll have an understanding of the Fabric administrator role and the tasks and tools involved in administering Fabric.

2. Understand the Fabric Architecture

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/2-fabric-architecture>

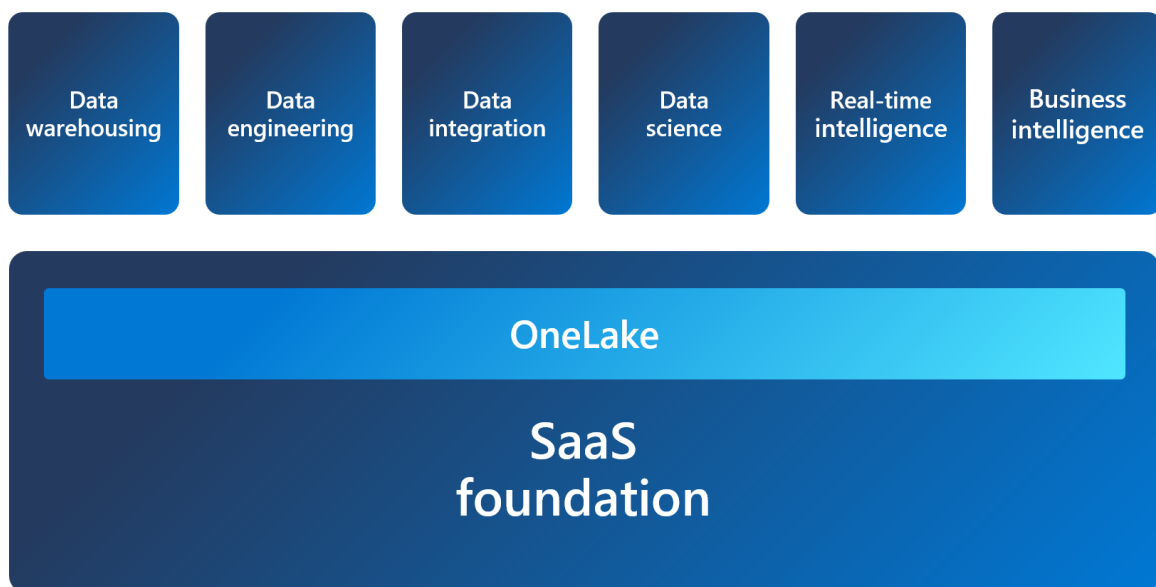
Understand the Fabric Architecture

Completed

Microsoft Fabric is a Software-as-a-Service platform, which provides a simple and integrated approach while reducing administrative overhead. Fabric provides an all-in-one analytics solution for enterprises that covers everything from data movement to data science, real-time analytics, and business intelligence. It offers a comprehensive suite of services, including:

- Data warehousing
- Data engineering
- Data integration
- Data science
- Real-time intelligence
- Business intelligence

All data in Fabric is stored in OneLake, which is built on Azure Data Lake Storage (ADLS) gen2 architecture. OneLake is hierarchical in nature to simplify management across your organization. There's only one OneLake per tenant and it provides a single-pane-of-glass file-system namespace that spans across users, regions, and even clouds.



Understand Fabric concepts

Tenant is a dedicated space for organizations to create, store, and manage Fabric items. There's often a single instance of Fabric for an organization, which is aligned with Microsoft Entra ID. The Fabric *tenant* maps to the root of OneLake and is at the top level of the hierarchy.

Capacity is a dedicated set of resources that is available at a given time to be used. A tenant can have one or more capacities associated with it. Capacity defines the ability of a resource to perform an activity or to produce output. Capacity needs vary by item and duration of use. Fabric offers capacity through the Fabric SKU and Trials.

Domain is a logical grouping of workspaces. Domains are used to organize items in a way that makes sense for your organization. You can group things together in a way that makes it easier for the groups of people to have access to workspaces. For example, you might have a domain for sales, another for marketing, and another for finance.

Workspace is a collection of items that brings together different functionality in a single tenant. It acts as a container that uses capacity for the work that is executed, and provides controls for who can access the items in it. For example, in a sales workspace, users associated with the sales organization can create a data warehouse, run notebooks, create datasets, create reports, and more.

Items are the building blocks of the Fabric platform. They're the objects that you create and manage in Fabric. There are different types of items, such as data warehouses, data pipelines, datasets, reports, and dashboards.

Understanding Fabric concepts is important for you as an admin, because it helps you understand how to manage the Fabric environment.

Note

For more information, see the [Start a Fabric trial](#) documentation.

3. Understand the Fabric administrator role

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/3-admin-role-tools>

Understand the Fabric administrator role

Completed

Now that you understand the Fabric architecture and what you and your team might use Fabric for, let's look at the admin role and the tools used to manage the platform.

There are several roles that work together to administer Microsoft Fabric for your organization. If you're a Microsoft 365 admin, a Power Platform admin, or a Fabric capacity admin, you're involved in administering Fabric. The Fabric admin role was formerly known as Power BI admin.

As a Fabric admin, you work primarily in the Fabric admin portal. You might also need to familiarize yourself with the following tools:

- [Microsoft 365 admin center](#)
- [Microsoft 365 Security & Microsoft Purview compliance portal](#)
- [Microsoft Entra ID in the Azure portal](#)

- [PowerShell cmdlets](#)
- [Administrative APIs and SDK](#)

Note

For specific details on the different admin roles and responsibilities, see the [What is Microsoft Fabric administration?](#) documentation.

Describe admin tasks

As an admin, you might be responsible for a wide range of tasks to keep the Fabric platform running smoothly. These tasks include:

Security and access control: One of the most important aspects of Fabric administration is managing security and access control to ensure that only authorized users can access sensitive data. You can use role-based access control (RBAC) to:

- Define who can view and edit content.
- Set up data gateways to securely connect to on-premises data sources.
- Manage user access with Microsoft Entra ID.

Data governance: Effective Fabric administration requires a solid understanding of data governance principles. You should know how to secure inbound and outbound connectivity in your tenant and how to monitor usage and performance metrics. You should also know how to apply data governance policies to ensure data within your tenant is only accessible to authorized users.

Customization and configuration: Fabric administration also involves customizing and configuring the platform to meet the needs of your organization. You might configure private links to secure your tenant, define data classification policies, or adjust the look and feel of reports and dashboards.

Monitoring and optimization: As a Fabric admin, you need to know how to monitor the performance and usage of the platform, optimize resources, and troubleshoot issues. Examples include configuring monitoring and alerting settings, optimizing query performance, managing capacity and scaling, and troubleshooting data refresh and connectivity issues.

Specific tasks vary depending on the needs of your organization and the complexity of your Fabric implementation.

Describe admin tools

It's important to familiarize yourself with a few tools to effectively implement the tasks previously outlined. Fabric admins can perform most admin tasks using one or more of the following tools: the Fabric admin portal, PowerShell cmdlets, admin APIs and SDKs, and the admin monitoring workspace.

Fabric admin portal

Fabric's *admin portal* is a web-based portal where you can manage all aspects of the platform. You can centrally manage, review, and apply settings for the entire tenant or by capacity in the admin portal. You can also manage users, admins and groups, access audit logs, and monitor usage and performance.

The admin portal enables you to turn settings on and off. There are many settings located in the admin portal. One noteworthy setting is the Fabric on/off switch, located in tenant settings that lets organizations that use Power BI opt into Fabric. Here, you can enable Fabric for your tenant or allow capacity admins to enable Fabric.

Admin portal

The screenshot displays the Fabric Admin Portal interface. On the left is a sidebar with a list of settings categories: Tenant settings (marked 'New'), Usage metrics, Users, Premium Per User, Audit logs, Domains (marked 'New'), Workloads, Tags (marked 'New'), Capacity settings, Refresh summary, Embed Codes, Organizational visuals, Azure connections, Workspaces, Custom branding, Fabric identities, Featured content, and Help + support. The main content area shows a notification at the top: 'There are new or updated tenant settings. Expand to review the changes.' Below this, the 'Microsoft Fabric' section is active, displaying the setting 'Users can create Fabric items' which is 'Enabled for the entire organization'. A descriptive text explains that this allows production-ready features and that turning it off doesn't impact Power BI items. A toggle switch is currently in the 'Enabled' position. Under 'Apply to:', 'The entire organization' is selected with a radio button. Other options are 'Specific security groups' and 'Except specific security groups'. There is a checkbox for 'Delegate setting to other admins' which is currently unchecked. Below this, a text prompt asks to 'Select the admins who can view and change this setting, including any security group selections you've made.' A checkbox for 'Capacity admins can enable/disable' is checked. At the bottom of the settings area are 'Apply' and 'Cancel' buttons.

PowerShell cmdlets

Fabric provides a set of *PowerShell cmdlets* that you can use to automate common administrative tasks. A PowerShell cmdlet is a simple command that can be executed in PowerShell.

For example, you can use cmdlets in Fabric to systematically create and manage groups, configure data sources and gateways, and monitor usage and performance. You can also use the cmdlets to manage the Fabric admin APIs and SDKs.

Note

See [Microsoft Power BI Cmdlets for Windows PowerShell and PowerShell Core](#) for more resources on PowerShell cmdlets that work with Fabric.

Admin APIs and SDKs

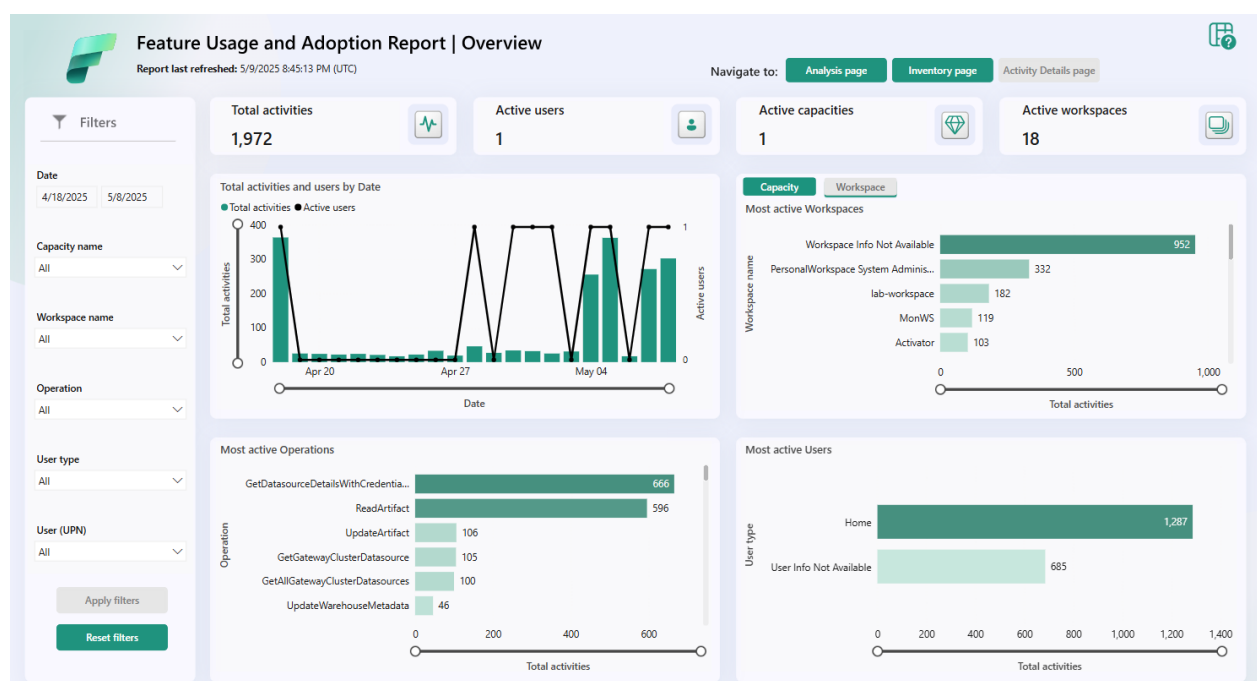
An admin *API and SDK* are tools that allow developers to interact with a software system programmatically. An API (Application Programming Interface) is a set of protocols and tools that enable communication between different software applications. An SDK (Software Development Kit) is a set of tools and libraries that helps developers create software applications that can interact with a specific system or platform. You can use APIs and SDKs to automate common administrative tasks and integrate Fabric with other systems.

For example, you can use APIs and SDKs to create and manage groups, configure data sources and gateways, and monitor usage and performance. You can also use the APIs and SDKs to manage the Fabric admin APIs and SDKs.

You can make these requests using any HTTP client library that supports OAuth 2.0 authentication, such as Postman, or you can use PowerShell scripts to automate the process.

Admin monitoring workspace

Fabric tenant admins have access to the *admin monitoring workspace*. You can choose to share access to the workspace or specific items within it with other users in your organization. The admin monitoring workspace includes the Feature Usage and Adoption dataset and report, which together provide insights on the usage and performance of your Fabric environment. You can use this information to identify trends and patterns, and troubleshoot issues.



Note

For more information about what is included in the Admin Monitoring Workspace, see [What is the Fabric admin monitoring workspace](#).

4. Manage Fabric security

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/4-manage-security>

Manage Fabric security

Completed

As a Fabric admin, part of your role is to manage security for the Fabric environment, including managing users and groups, and how users share and distribute content in Fabric.

Manage users: assign and manage licenses

User licenses control the level of user access and functionality within the Fabric environment. Administrators ensure licensed users have the access they need to data and analytics to do their jobs effectively. They also limit access to sensitive data and ensure compliance with data protection laws and regulations.

Managing licenses allows administrators to monitor and control costs by ensuring that licenses are allocated efficiently and only to users who need them. This can help to prevent unnecessary expenses and ensure that the organization is utilizing its resources effectively.

Having the appropriate procedures in place to assign and manage licenses helps to control access to data and analytics, ensure compliance with regulations, and optimize costs.

License management for Fabric is handled in the Microsoft 365 admin center. For more information about managing licenses, see [Assign licenses to users](#).

Note

The *license type* in workspace settings is related to the user licenses listed here. Users can see reports depending on the user license and the workspace license. For detailed information, see the [Microsoft Fabric licenses](#) documentation.

Manage items and sharing

As an admin, you can manage how users share and distribute content. You can manage how users share content with others, and how they distribute content to others. You can also manage how users interact with items, such as data warehouses, data pipelines, datasets, reports, and dashboards.

Items in workspaces are best distributed through a workspace app or the workspace directly. Granting the least permissive rights is the first step in securing the data. Share the read only app for access to the reports or grant access to the workspaces for collaboration and development. Another aspect of managing and distributing items is enforcing these types of best practices.

You can manage sharing and distribution both internally and outside of your organization, in compliance with your organization's policies and procedures.

Note

For more information, see the [Security in Microsoft Fabric](#) documentation.

5. Govern data in Fabric

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/5-govern-fabric>

Govern data in Fabric

Completed

Fabric includes built-in governance features to help you manage and control your data. *Endorsement* is a way for you as an admin to designate specific Fabric items as trusted and approved for use across the organization.

Admins can also make use of the *scanner API* to scan Fabric items for sensitive data, and the *data lineage* feature to track the flow of data through Fabric.

Endorse Fabric content

Endorsement is a key governance feature that builds trust in your data assets by marking Fabric items as reviewed and approved. Endorsed items display a badge, signaling to users that these assets are reliable. Endorsement helps users trust the data, and it also helps you as an admin manage the overall growth of items across your environment.

Promoted Fabric content appears with a Promoted badge in the Fabric portal. Workspace members with the contributor or admin role can promote content within a workspace. The Fabric admin can promote content across the organization.

Certified content requires a more formal process that involves a review of the content by a designated reviewer. Content appears with a Certified badge in the Fabric portal. Admins manage the certification process and can customize it to meet the needs of your organization.

If you aren't an admin, you need to request item certification from an admin. You can perform request certification by selecting the item in the Fabric portal, and then selecting **Request certification** from the **More** menu.

Note

For more detailed information on the content endorsement process, see [Promote or certify content](#).

Scan for sensitive data

Metadata scanning facilitates governance of data by enabling cataloging and reporting on all the metadata of your organization's Fabric items. The *scanner API* is a set of Admin REST APIs that allows you to scan Fabric items for sensitive data. Use the scanner API to scan data warehouses, data pipelines, datasets, reports, and dashboards for sensitive data. The scanner API can be used to scan both structured and unstructured data.

Important

Before metadata scanning can be run, it needs to be set up in your organization by an Admin. For more information, see the [Metadata scanning overview](#).

Track data lineage

Data lineage is the ability to track the flow of data through Fabric, also known as *impact analysis*. Data lineage allows you to see where data comes from, how it's transformed, and where it goes. The lineage view in workspaces helps you understand the data that is available in Fabric, and how it's being used.

Report on sensitive data

With the Microsoft Purview hub (preview) in Fabric, you can manage and govern your organization's Fabric data estate. It contains reports that provide insights about sensitive data, item endorsement, and domains, and also serves as a gateway to more advanced capabilities in the Microsoft Purview portal such as Data Catalog, Information Protection, Data Loss Prevention, and Audit.

6. Module assessment

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/6-knowledge-check>

Module assessment

Completed

7. Summary

<https://learn.microsoft.com/en-us/training/modules/administer-fabric/7-summary>

Summary

Completed

In this module, you learned about the Fabric architecture and the role of an administrator for the Fabric platform. You also explored the different tools available for managing security and sharing, as well as the governance features that can be used to enforce standards and ensure compliance. Your understanding of how to manage a Fabric environment ensures that it's secure, compliant, and well-governed. With this knowledge, you're well-equipped to help your organization get the most out of Fabric and derive valuable insights from all your data.

For more information about data governance, complete the [Govern data in Microsoft Fabric with Purview](#) module.