

# Get started with Azure DevOps documentation

Start using Azure DevOps to collaborate on code, build and deploy apps, or plan and track work.

## About Azure DevOps

### OVERVIEW

[What is Azure DevOps?](#)

[What is Azure Boards?](#)

[What is Azure Repos?](#)

[What is Azure Pipelines?](#)

[What is Azure Test Plans?](#)

[Get started as a Stakeholder](#)

## Sign up for free

### QUICKSTART

[Azure DevOps \(includes all services\)](#)

[Azure Boards](#)

[Azure Repos](#)

[Azure Pipelines](#)

[Azure Artifacts](#)

### HOW-TO GUIDE

[Connect to a project](#)

## Manage your project

## QUICKSTART

- [Manage your project](#)
- [Add users to a team or project](#)
- [Add a project administrator](#)
- [Add a project collection administrator](#)
- [Create a new project](#)
- [Delete or restore a project](#)
- [Set up billing for your organization](#)

## CONCEPT

- [Security overview](#)
- [Default permissions and access](#)
- [Permission lookup guide](#)
- [About settings](#)

## Plan and track work

### QUICKSTART

- [Plan and track work](#)
- [Create your backlog](#)
- [Define sprints](#)
- [Use boards](#)

## Collaborate on code

### QUICKSTART

- [Clone a repository](#)
- [Create a repository](#)
- [Authenticate with SSH](#)
- [Search code across projects](#)

[Set Git repo permissions](#)

## Build and deploy your apps

### QUICKSTART

[Create your first pipeline](#)

[Build multiple branches](#)

### REFERENCE

[YAML schema](#)

[Pipeline variables](#)

## Set your preferences

### QUICKSTART

[Change profile preferences](#)

[Manage your notifications](#)

[Preview new features](#)

[Set favorites](#)

## Navigate

### HOW-TO GUIDE

[Web portal navigation](#)

[Team Explorer navigation](#)

[Use the command line](#)

## Migrate

---

## CONCEPT

[Migration overview](#)

[Get started](#)

[Prerequisites](#)

[Validate](#)

[Prepare test run](#)

[Test run](#)

[Migrate](#)

[Post-migration](#)

[Troubleshoot](#)

# What is Azure DevOps?

Article • 04/22/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Azure DevOps supports a collaborative culture and set of processes that bring together developers, project managers, and contributors to build software. It allows organizations to create and improve products at a faster pace than they can with traditional software development approaches.

You can work in the cloud with [Azure DevOps Services](#) or on-premises with Azure DevOps Server. For more information, see [Differences between Azure DevOps Services and Azure DevOps Server](#).

Azure DevOps provides integrated features that you can access through your web browser or IDE client. You can use all the services included with Azure DevOps or choose just what you need to complement your existing workflows.

## Explore standalone services

The following table describes the standalone services available with Azure DevOps:

[ ] [Expand table](#)

Standalone service	Description
<a href="#">Azure Boards</a> ↗	Delivers a suite of Agile tools to support planning and tracking work, code defects, and issues by using Kanban and Scrum methods. For more information about Azure Boards, see <a href="#">What is Azure Boards?</a>
<a href="#">Azure Repos</a> ↗	Provides Git repositories or Team Foundation Version Control (TFVC) for source control of your code. For more information about Azure Repos, see <a href="#">What is Azure Repos?</a>
<a href="#">Azure Pipelines</a> ↗	Provides build and release services to support continuous integration and delivery of your applications. For more information about Azure Pipelines, see <a href="#">What is Azure Pipelines?</a>
<a href="#">Azure Test Plans</a> ↗	Provides several tools to test your applications, including manual/exploratory testing and continuous testing. For more information about Azure Test Plans, see <a href="#">Overview of Azure Test Plans</a> .
<a href="#">Azure Artifacts</a> ↗	Allows teams to share packages such as Maven, npm, NuGet, and more from public and private sources and integrate package sharing into your pipelines. For more information about Azure Artifacts, see <a href="#">Overview of Azure Artifacts</a> .

Azure DevOps supports adding extensions and integrating with other popular services, such as Slack, Trello, UserVoice, and more. You can also develop your own custom extensions for use with Azure DevOps.

## Choose Azure DevOps Services

*Azure DevOps Services* supports integration with GitHub.com and GitHub Enterprise Server repositories. Choose Azure DevOps Services when you want the following outcomes:

- Quick set-up
- Maintenance-free operations
- Easy collaboration across domains
- Elastic scale
- Rock-solid security

Azure DevOps Services also gives you access to cloud build and deployment servers, and application insights. [Start for free](#) and create an organization. Then, either upload your code to share or source control. Begin tracking your work by using Scrum, Kanban, or a combination of methods.

For more information, see the [Azure DevOps and GitHub integration overview](#).

## Choose Azure DevOps Server

*Azure DevOps Server* supports integration with GitHub Enterprise Server repositories. Choose on-premises Azure DevOps Server if you need your data to stay within your network. The on-premises XML process model can also better support your work tracking customization requirements over the inheritance process model. The on-premises model supports modification of XML definition files.

When you deploy Azure DevOps Server, you can also configure the following servers or integration points:

- **Build server:** Support on-premises and cloud-hosted builds.
- **SQL Server and SQL Analysis Server:** Support SQL Server Reports and the ability to create Excel pivot charts based on the cube.

Start for free by downloading [Azure DevOps Server Express ↗](#). Then, either upload your code to share or source control. Or, begin tracking your work by using Scrum, Kanban, or a combination of methods.

For more information about managing Azure DevOps Server, see the [Administrative tasks quick reference](#).

## Get started with Azure DevOps

Get started working with Azure DevOps now:

- [Review pricing models for Azure DevOps ↗](#)
- [Sign up for Azure DevOps Services](#)
- [Install Azure DevOps Server](#)
- [Tour an overview of the services](#)

## Related content

- [Data protection overview](#)
- [Client-server tools](#)
- [Software development roles](#)
- [Azure DevOps and GitHub integration overview](#)

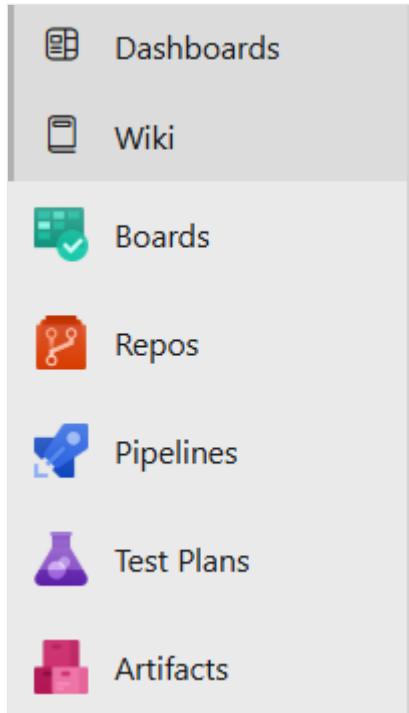
# What are the services in Azure DevOps?

Article • 04/22/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Azure DevOps offers a spectrum of service models to accommodate the unique needs of every team. The free access version helps small teams get started quickly, while the versatile subscription and pay-per-use plans support comprehensive project management.

- **End-to-end project management:** Azure DevOps stands as a cohesive suite of services designed to support the complete lifecycle of your software projects. It encompasses everything from initial planning and development, through rigorous testing, to final deployment.
- **Client/server model delivery:** Azure DevOps operates on a client/server model, offering flexibility in how you interact with its services. The web interface provides a convenient way to utilize most services and is compatible with all major browsers. Additionally, certain services like source control, build pipelines, and work tracking offer client-based management options for enhanced control.
- **Flexible and scalable service options:**
  - Azure DevOps caters to teams of all sizes by offering a range of service options. For small teams, many services are complimentary, ensuring that you have access to robust project management tools without any initial investment.
  - For larger teams or more advanced needs, services are accessible through a subscription model or on a pay-per-use basis. This flexibility allows you to scale your usage according to project demands and budget constraints.
  - Azure DevOps offers a hybrid model, so you can make the best use of the benefits you need. Manage your code and tasks by using an on-premises deployment for maximum control and security. When you need more resources, tap into cloud-based build or testing services. This approach ensures you only pay for what you use, optimizing your operational efficiency.
- **Azure DevOps navigation:** The left navigation menu in Azure DevOps is your gateway to its extensive features. It allows for intuitive access and management of the various services provided.



**Dashboards:** Create a personalized view of project data and workflows.

**Wiki:** Document projects in a centralized and accessible team location.

**Boards:** Access Agile tools for streamline planning and tracking projects.

**Repos:** Apply source control for project collaboration and maintenance.

**Pipelines:** Automate project build and test, and the release processes.

**Test Plans:** Create, manage, and run manual and automated project testing.

**Artifacts:** Share packages and integrate package sharing into pipelines.

For more information, see [Tools and clients that connect to Azure DevOps](#).

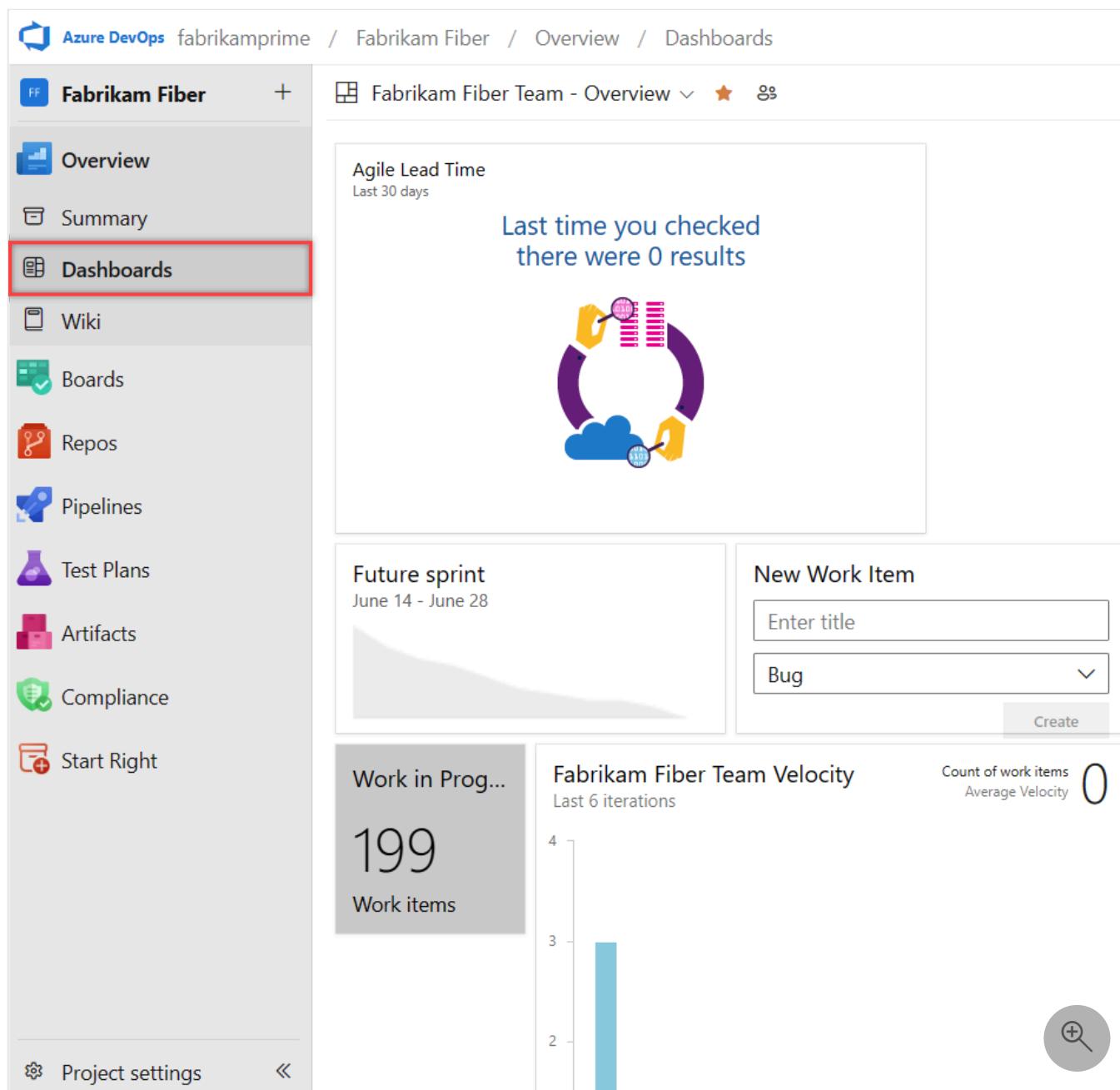
## Dashboards

Azure DevOps provides a powerful dashboard interface that allows you to create a personalized view of your project data and workflows. Here's how you can make the most of the Dashboards feature:

- **Add, configure, and manage dashboards:** Create multiple dashboards to reflect different aspects of your project. You can customize each dashboard by adding and arranging various widgets that display project data in real time.

- **Configure widgets:** Enhance your dashboards with widgets that provide insights into your project. Choose from a wide range of widgets to display information such as build status, test results, and work item queries.
- **Navigate quickly:** Use dashboards as a central hub for navigating to various areas of your project. Set up links and shortcuts that allow you to access important sections of Azure DevOps with just a selection.
- **Use extensibility points:** Use Azure DevOps extensibility points to further customize your dashboards. You can add new capabilities by integrating non-Microsoft services or creating your own extensions.

For more information, see the [Dashboards documentation](#).



The screenshot shows the Azure DevOps interface for the 'fabrikamprime' organization, specifically the 'Fabrikam Fiber' project. The left sidebar has a red box around the 'Dashboards' option. The main area displays several dashboard cards:

- Agile Lead Time (Last 30 days):** Shows a bar chart with 0 results.
- Future sprint (June 14 - June 28):** Shows a progress bar at 0% completion.
- New Work Item:** A form to enter a title (e.g., 'Bug') and a dropdown for type, with a 'Create' button.
- Work in Progress (199 Work items):** A summary card.
- Fabrikam Fiber Team Velocity (Last 6 iterations):** A bar chart showing an average velocity of 0.

## Azure Boards

In the dynamic world of software development, efficient information sharing and meticulous tracking of work, tasks, issues, and code defects are essential. Developers commonly work with tools like Microsoft Excel, Microsoft Project, and various bug tracking systems. The recent adoption of Agile methodologies revolutionizes planning and development processes.

Azure Boards provides several Agile tools designed to help streamline planning and tracking across your projects:

- **Work item management:** Seamlessly add and update various work items to keep your project organized and on track.
- **Queries and charts:** Define custom queries for work items and generate insightful status and trend charts to visualize progress.
- **Backlog handling:** Efficiently manage your product backlog and ensure priorities are clear and actionable.
- **Sprint planning:** Utilize sprint backlogs to plan and execute sprints with precision and align your team's efforts with project goals.
- **Task board utilization:** Review and update sprint tasks through interactive task boards that reflect real-time changes.
- **Workflow visualization:** Monitor your project workflow and update statuses by using intuitive boards that provide a clear view of the development pipeline.
- **Portfolio management:** Organize your work hierarchically, group user stories under features and features under epics, and maintain a structured overview.
- **Scrum meetings:** Use task boards during daily Scrum meetings to assess completed, remaining, or blocked work, and foster a collaborative and responsive team environment.

Azure Boards supports various work item types, where each is associated with a specific set of fields that can be updated as progress is made. These work types give you a tailored approach to tracking different aspects of your project.

**Agile support:** Whether you're practicing Scrum, Kanban, or Scrumban, Azure Boards offers backlogs and boards to facilitate these methodologies, empowering your team to deliver results effectively.

Project managers and developers can share information and track progress by using the comprehensive backlogs and boards. Azure Boards provides a complete picture of your project status, which enables teams to monitor trends and make informed decisions.

For an in-depth understanding of how backlogs, boards, and plans can transform your project management experience, see [What is Azure Boards?](#)

The screenshot shows the Azure DevOps Boards interface for the 'Fabrikam Fiber' project. The left sidebar lists various project management options like Overview, Boards, Work items, Boards, Backlogs, Sprints, Queries, Delivery Plans, Analytics views, Dependency Tracker, Repos, Pipelines, Test Plans, Artifacts, Compliance, Start Right, and Project settings. The 'Boards' option is highlighted with a red box. The main area displays a Kanban board titled 'Fabrikam Fiber Team'. At the top right, there are filters for 'Board' (selected), 'Analytics', and status indicators (7/5 Active). Below the header are buttons for 'New' (with '+ New item' and search), 'Analyze', and 'Active'. The board itself consists of several columns representing work items. A summary bar on the right indicates 1/4 tasks completed. The work items listed are:

- Add badge to README
- Story 1 (Jamal Hartnett, 0/2)
- Change initial view
- Cancel order form
- New welcome page
- As a <user>, I can select a user framework
- Slow response on information form (Jamal Hartnett)
- Update website to match new brand guidelines (0/1)
- Add animated emoticons to preview (Jamal Hartnett)
- 34 Welcome back page (Active, Jamal Hartnett, Story Points 3, Web, 0/1)
- 39 Secure sign-in (Active, fabrikam2@fabrikam.com, Story Points 5, Web, Security, 0/1)
- 40 Canadian addresses don't display correctly (Web, 0/1)

A vertical sidebar on the right provides quick access to 'Cancel', 'Story Point', 'Phone', '1/4', '63', 'Cus', 'history', 'New', 'fabrika', 'Work Item...', 'Draft te', 'fabrika', 'Implement abstracts', 'fabrika', '52', 'Filte', 'an item is s', 'New', and 'Work Item...'. A magnifying glass icon is also present.

## Azure Repos

Source or version control systems are pivotal for developers who need to collaborate seamlessly on codebases and maintain a comprehensive history of changes. These systems are indispensable for projects that involve multiple developers and ensure consistency and coordination throughout the development process.

The screenshot shows the Azure DevOps interface for the 'fabrikamprime' organization, specifically the 'Fabrikam Fiber' project. The 'Repos' menu item is highlighted with a red box. The main content area displays the 'Batch' repository, which contains several folders: 'arm-templates', 'client-application', 'hpc-application', and 'pipelines'. A 'README.md' file is also present. The right sidebar shows a list of files with the same structure, and below it are sections for 'Introduction', 'Getting Started', 'Build and Test', and 'Contribute'.

## Introduction

TODO: Give a short introduction of your

## Getting Started

TODO: Guide users through getting your

1. Installation process
2. Software dependencies
3. Latest releases
4. API references

## Build and Test

TODO: Describe and show how to build :

## Contribute

Azure DevOps supports two primary types of source control to suit diverse project needs: [Git](#) and [Team Foundation Version Control \(TFVC\)](#).

## Git

Git is a version control system where each developer has a local copy of the entire repository. This approach allows for offline work and easy branching and merging. Git is the default choice for new projects and is recommended for its flexibility and robustness.

### ! Note

Git in Azure DevOps is standard Git. You can use Visual Studio with third-party Git services. You can also use third-party Git clients with Azure DevOps Server.

You can do the following tasks with Azure Repos for Git:

- **Review files:** Examine the details and history of changes made to each file within your repository.
- **Download and edit files:** Obtain a local copy of files from the repository and make necessary modifications.
- **Manage commits:** Keep track of commits pushed to the repository and ensure a clear history of code changes.
- **Use pull requests:** Participate in the collaborative code review process by creating, approving, commenting on, and completing pull requests.
- **Use Git tags:** Organize and mark specific points in your repository's history by using Git tags for easy reference.

## TFVC

Team Foundation Version Control (TFVC) is a centralized version control system that simplifies code management. Developers work with a single version of each file on their local machines, while the server retains the full history of changes, providing a single source of truth.

TFVC includes the following key features:

- **Single version workflow:** Each developer's machine holds the current version of files. This approach reduces complexity and ensures consistency across the team.
- **Server-side history:** All historical data including changes and versions are securely stored on the server, which preserves the integrity of your project's evolution.
- **Path-based branching:** Branches are created and managed on the server by using a path-based approach. This approach allows for clear organization and straightforward merging processes.

## Azure Pipelines

Achieving rapid and reliable software releases is a hallmark of modern development practices. Azure Pipelines stands at the forefront of this endeavor by automating the build, test, and release processes.

- **Automated builds:** Set up your Azure Pipelines to trigger automated builds upon code check-ins and ensure every change is promptly integrated and verified.
- **Test integration:** Incorporate test runs post-build to validate changes, maintain high code quality, and detect issues early.
- **Release pipelines:** Manage the deployment of your software builds across various environments, from staging to production, with Azure Pipelines' robust release management capabilities.

Azure Pipelines includes the following features:

- **Continuous integration (CI):** Implement CI to automatically merge code changes into a central repository, followed by automated builds and tests.
- **Continuous delivery (CD):** Ensure that your software can be reliably released at any time with CD practices, streamlining the path from development to production.
- **Build automation:** Customize your build process with defined steps and triggers, creating a consistent and repeatable build environment.
- **Release management:** Oversee simultaneous releases with configurable release pipelines that mirror your development lifecycle, from development environments to production.
- **Deployment automation:** Automate the deployment process, reducing manual efforts and the potential for errors.
- **Approval workflows:** Integrate approval workflows to validate successful deployments, adding a layer of verification before promoting builds.
- **Release tracking:** Monitor your releases as they progress through different environments, gaining visibility into the deployment pipeline.

For a detailed guide on implementing continuous integration and delivery with Azure Pipelines, see [What is Azure Pipelines?](#)

Azure DevOps fabrikamprime / Fabrikam Fiber / Pipelines

F Fabrikam Fiber +

Overview Boards Repos Pipelines Environments Releases Library Task groups Deployment groups Test Plans Artifacts Compliance Start Right Project settings <

## Pipelines

Recent All Runs

### Recently run pipelines

Pipeline	Last run
pipelines-javascript-docker	#20240813.1 • Set up C 🕒 Individual CI for 1P 89m
pipelines-android (36)	#20240812.4 • Update C 🕒 Individual CI for 1P 89m
pipelines-xcode	#20240809.1 • Set up C 🕒 Individual CI for 1P 89m
appcenter-sampleapp-android	#20240809.1 • Microsoft 🕒 Manually triggered for 1P
pipelines-android	#20240809.1 • Set up C 🕒 Individual CI for 1P 89m
appcenter-sampleapp-ios-swift	#20240808.2 • Set up C 🕒 Manually triggered for 1P
Batch	#20240807.1 • . 🕒 Manually triggered for 1P
Fabrikam (1)	#Fabrikam (1)_2024.7.1. 🕒 Manually triggered for 1P
Fabrikam	#20211118.2 • Set up C 🕒 Manually triggered for 1P

+

## Azure Test Plans

Azure Test Plans is a comprehensive service designed to facilitate the creation, management, and execution of various testing methodologies, including manual, exploratory, and automated tests.

Azure Test Plans includes the following key features:

- **Workflow customization:** Tailor your testing workflow with customizable test plans, suites, and cases, and help ensure alignment with your project's needs.

- **Traceability:** Achieve end-to-end traceability and link requirements directly to test cases and bugs with requirement-based test suites.
- **Test selection:** Utilize query-based test suites for criteria-based test selection and streamline the testing process.
- **User-friendly interface:** Benefit from an Excel-like grid interface and simplify the creation and management of test cases.
- **Reusable elements:** Enhance efficiency with reusable test steps and shared parameters, and promote consistency across tests.
- **Collaboration:** Share test plans, suites, and cases with stakeholders for review and feedback, and foster a collaborative testing environment.
- **Cross-platform execution:** Execute tests directly from your browser on any platform, which offers flexibility and convenience.
- **Activity monitoring:** Monitor testing activities with real-time charts, and gain visibility into test progress and outcomes.

For a detailed exploration of how Azure Test Plans can streamline your testing processes, see the [Azure Test Plans documentation](#).

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar is highlighted with a red box around the 'Test Plans' item. The main area displays the 'Testing Test Plan' (ID: 226), which is past due from June 13 to June 27. It shows 0% run completion and a link to view the report. The 'Test Suites' section lists 'Testing Test Plan (1)'. The right panel shows the 'Define' tab selected, listing 'Test Cases (1 item)' with a checkbox for 'Title' and another for 'Testing Test Case'. A search icon is located in the bottom right corner of the main content area.

## Collaboration services

Azure DevOps enhances team collaboration through the following services designed to streamline communication and project tracking:

- **Team dashboards:** Create and customize dashboards to provide your team with real-time visibility into project metrics and progress.
- **Project wiki:** Document your project details, guidelines, and knowledge base in a centralized, easily accessible wiki.
- **Work item discussions:** Facilitate conversations directly within work item forms and enable contextual and timely communication.

- **Traceability links:** Establish links between [work items](#), [commits](#), [pull requests](#), and more, and help ensure comprehensive traceability across your project.
- **Alerts and notifications:** Set up personalized alerts and change notifications to keep team members informed about project updates and changes.
- **Feedback management:** Streamline the process of [requesting](#), [providing](#), and managing feedback to continuously improve project outcomes.
- **Analytics and Reporting:** Use the analytics service and Power BI reporting for insights into project performance and make data-driven decisions.

These collaboration services are integral to maintaining a cohesive and informed team capable of responding swiftly to project demands and opportunities.

## Service hooks

Service hooks in Azure DevOps empower you to automate and streamline interactions with other services, and respond swiftly to events within your projects. For instance, you can configure service hooks to send immediate push notifications to your team's devices if a build process encounters an error.

Utilize service hooks in the following ways:

- **Custom apps integration:** Integrate service hooks with your custom applications to initiate actions automatically, enhance efficiency, and improve project responsiveness.
- **Service targets:** Designate various services as targets for your service hooks and allow for a wide range of automated responses to project events.

For a comprehensive list of services that can be integrated with Azure DevOps by using service hooks, and to explore other apps and services that complement Azure DevOps, see the [Visual Studio Marketplace](#). To stay updated on the newest services supported by service hooks, see the [Integrate with service hooks](#) documentation.

## Azure cloud-hosted services

Azure offers a robust array of cloud-hosted services that are essential for the development and deployment of applications. These services can be utilized independently or with Azure DevOps to create a seamless workflow.

Key benefits of Azure cloud-hosted services include:

- **Comprehensive support:** Azure services provide the infrastructure and platform support necessary for the entire application lifecycle.

- **Integration with Azure DevOps:** You can combine these services with Azure DevOps for an integrated experience that covers source control, CI/CD, and more.

To explore the full range of services, features, and suites that integrate seamlessly with your development process, see the [Azure products](#)  directory.

## Administrative services

Managing a collaborative software development environment is a streamlined process with Azure DevOps. You can access various features and tasks that are tailored for administration. These tools are designed to facilitate the oversight of your projects and teams effectively.

Accessible administration is provided in the following ways:

- **Web portal management:** Perform most administrative tasks conveniently through the Azure DevOps web portal and ensure you have control at your fingertips.
- **Comprehensive settings:** Access detailed settings for users, teams, projects, and organizations. This approach allows for granular management of your development environment.

For a deeper understanding of the administrative capabilities available to you, including how to configure and manage various levels of settings, see [About user, team, project, and organization-level settings](#).

## Related content

- [Compare Azure DevOps Services and Azure DevOps Server](#)
- [Review client-server tools](#)
- [Examine Software development roles](#)
- [Review Azure DevOps pricing](#) 

 **Note:** The author created this article with assistance from AI. [Learn more](#)

# Compare Azure DevOps Services with Azure DevOps Server

Article • 04/23/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

The **cloud offering**, Azure DevOps Services, provides a scalable, reliable, and globally available hosted service. The 24/7 operations team monitors the cloud offering, which is backed by a 99.9% service level agreement (SLA) and available in local data centers around the world.

The **on-premises offering**, Azure DevOps Server, is built on a SQL Server backend. Customers usually choose the on-premises version when they need their data to stay within their network. This offering is also ideal when you need access to SQL Server reporting services that integrate with Azure DevOps Server data and tools.

Both offerings provide the same [essential features and services](#), but Azure DevOps Services offers more benefits:

- Simplifies server management
- Provides immediate access to the latest features
- Enhances connectivity with remote sites
- Transitions from capital expenditures (servers and hardware) to operational expenditures (subscriptions)

## Key differences

Azure DevOps Services and Azure DevOps Server offer similar core functionalities, but they have key differences in specific feature areas. To decide whether the cloud or on-premises offering best meets your needs, consider the following key differences.

[ ] Expand table

Feature area	Azure DevOps Services	Azure DevOps Server
Deployment	Cloud-based, hosted, and managed by Microsoft	On-premises solution, managed by your organization
Scalability	Highly scalable, accessible from anywhere with an internet connection	Scalability limited to your organizational infrastructure and server capacity
Authentication	Uses Microsoft accounts or Microsoft Entra ID	Uses Windows Authentication and Windows Server Active Directory domain credentials

Feature area	Azure DevOps Services	Azure DevOps Server
Data control	Data stored in secure Azure data centers	Organizations have complete control over their data and infrastructure
User management	Supports adding Microsoft Entra groups to Azure DevOps Services groups	Access granted by adding Windows Server Active Directory (Windows AD) groups to various Azure DevOps groups
Process customization	Inheritance process model with web UI and REST endpoint customization options	Offers both Inheritance and On-premises XML process models for customization
Analytics and reporting	Provides dashboards, Analytics service, Power BI integration, and OData support	Offers dashboards, SQL Server Reporting Services (SSRS) reports, and configurable lightweight charts
Integration with SQL Server	Doesn't support integration with SQL Server Analysis Services for reporting	Supports integration with SQL Server Analysis Services

These differences can help you decide which platform best suits your organization's needs. If you use Azure DevOps Server and you're considering a move to Azure DevOps Services, see the [Migration overview](#).

## Scalability

As your business grows, you might need to scale up your Azure DevOps instance. This scaling can involve adding more users, increasing storage capacity, or enhancing performance to handle larger workloads. You might also need to integrate other tools and services to support more complex workflows and ensure seamless collaboration across larger teams. Azure DevOps provides various options and configurations to help you scale efficiently, whether you're using Azure DevOps Services in the cloud or Azure DevOps Server on-premises.

## Azure DevOps Services

Azure DevOps Services offers two options for scoping and scaling data: organizations and projects. Organizations in Azure DevOps Services get their own URLs (for example, <https://dev.azure.com/fabrikamfiber>), and they always have exactly one project collection. Organizations can have many projects within a collection.

Create organizations in Azure DevOps Services wherever you might create collections in Azure DevOps Server. Consider the following scenarios:

- **Purchase users per organization.** Paid users can access only the organization where the payment is made. For users needing access to multiple organizations, Visual Studio subscriptions are an attractive option. Visual Studio subscribers can be added to any number of organizations at no charge.
- **Administer organizations individually.** Currently, you must administer organizations one at a time, which can be cumbersome if you have many organizations.

For more information, see [Plan your organizational structure in Azure DevOps](#).

## Azure DevOps Server

Azure DevOps Server provides three options for scoping and scaling data: deployments, project collections, and projects.

- **Deployments:** In the simplest case, deployments are servers. They can be more complex, such as two-server deployments where SQL is on a separate machine or high-availability farms with multiple servers.
- **Project collections:** Serve as containers for security, administration, and physical database boundaries. They're also used to group related projects.
- **Projects:** Encapsulate the assets of individual software projects, including source code, work items, and more.

For more information, see [Plan your organizational structure in Azure DevOps](#).

## Authentication

When you compare Azure DevOps Services and Azure DevOps Server, it's important to understand the differences in how authentication is handled for each platform.

## Azure DevOps Services

With Azure DevOps Services, you connect over the public internet (for example, <https://contoso.visualstudio.com>). You can authenticate by using either [Microsoft account](#) credentials or [Microsoft Entra ID](#) credentials, depending on your organization setup. Microsoft Entra ID also allows you to enable features such as multifactor authentication, IP address restrictions, and more.

The recommended approach is to configure your organizations to use Microsoft Entra rather than Microsoft accounts. This method provides a better experience in many scenarios and offers more options for enhanced security.

For more information, see [About accessing Azure DevOps Services with Microsoft Entra ID](#).

## Azure DevOps Server

With Azure DevOps Server, you connect to an intranet server (for example, <https://tfs.corp.contoso.com:8080/tfs>). Authenticate by using Windows Authentication and your Windows AD domain credentials. This process is seamless, and you never encounter a sign-in experience.

## Data control

Many entities seek information about data protection when considering a move to the cloud. Microsoft is committed to keeping Azure DevOps Services projects safe and secure. Technical features and business processes are established to uphold this commitment. You can also take steps to secure your data. For more information, see the [Data protection overview](#).

## User management

When you manage users and groups in Azure DevOps Services and Azure DevOps Server, there are distinct methods and tools available for each platform to ensure proper access and organization.

## Azure DevOps Services

In Azure DevOps Services, you can [provide access to groups of users](#) by adding Microsoft Entra groups to Azure DevOps Services groups. If you use Microsoft Accounts instead of Microsoft Entra ID, you must [add users](#) individually.

You must also [assign an access level](#) to each user in your organization. Azure DevOps Services validates Visual Studio subscribers as they sign in. You can assign Basic access for free to up to five users without Visual Studio subscriptions.

To give at least Basic access to more users, [set up billing](#) and [pay for more users](#). Otherwise, all other users receive Stakeholder access.

Microsoft Entra groups provide access to groups of users, with access levels automatically assigned at first sign-in. For organizations that use Microsoft accounts for signing in, you must explicitly assign access levels to each user.

## Azure DevOps Server

In Azure DevOps Server, you grant users access to deployments by adding Windows AD groups to various Azure DevOps groups, such as the Contributors group for an individual project. Windows AD group memberships stay in sync. As users are added or removed in Windows AD, they automatically gain or lose access to Azure DevOps Server.

All use is on the honor system. To set access levels for users based on their licenses, specify their [access levels](#) on the administration page. For example, assign unlicensed users Stakeholder access only.

Users with an Azure DevOps Server Client Access License (CAL) can have Basic access. Visual Studio subscribers can have either Basic or Advanced access, depending on their subscription. Azure DevOps Server doesn't verify these licenses or enforce compliance.

In both Azure DevOps Services and Azure DevOps Server, you manage access to features by assigning users to an [access level](#). All users must be assigned to a single access level. In both the cloud and on-premises offerings, you can give free access to work item features to an unlimited number of Stakeholders. Also, an unlimited number of Visual Studio subscribers can have access to all Basic features at no extra charge. You pay only for other users who need access.

## Process customization

You can customize the work-tracking experience in different ways depending on the supported process model.

### Azure DevOps Services

Azure DevOps Services uses the **Inheritance** process model, which supports WYSIWYG (What You See Is What You Get) customization. This model allows you to easily customize work item types, states, and fields directly through the user interface without needing to edit XML files. You can create and modify processes to fit your team's workflow, and ensure the tools align with your specific project requirements. This flexibility makes it easier to manage and adapt to changes in your development process.

### Azure DevOps Server

With Azure DevOps Server, you can choose between the **Inheritance** process model and the **On-premises XML** process model.

The **Inheritance process model** supports WYSIWYG customization, which allows you to easily customize work item types, states, and fields directly through the user interface. This approach

simplifies the customization process and ensures that changes are immediately reflected in your projects.

The **On-premises XML process model** supports customization through the import or export of XML definition files for work-tracking objects. It provides a powerful and flexible way to define and manage your processes. However, it can cause various issues, such as:

- Processes for existing projects aren't automatically updated, requiring manual intervention to apply changes.
- The complexity of managing XML files can lead to errors and inconsistencies.
- It might be challenging to maintain and troubleshoot customizations, especially in large or complex environments.

To help you avoid issues, custom process templates and the *witadmin.exe* tool are always disabled. This approach ensures that all projects are automatically updated with each Azure DevOps Services upgrade.

With the process customization capability, you can make changes directly within the web user interface (UI). If you prefer to customize your processes programmatically, you can use REST endpoints. Customizing projects this way ensures they're automatically updated when new versions of their base processes are released with Azure DevOps Services upgrades.

For more information, see [Customize your work-tracking experience](#).

## Analytics and reporting

Azure DevOps Services and Azure DevOps Server offer various tools to provide insight into the progress and quality of your software projects. These tools include:

- **Dashboards and lightweight charts:** These tools are available on both cloud and on-premises platforms, and are easy to set up and use. Dashboards provide a customizable overview of your project status, while charts offer visual representations of key metrics and trends.
- **The Analytics service** and **Analytics widgets:** The Analytics service is optimized for fast read-access and server-based aggregations to help you gain deeper insights into your project data. Analytics widgets can be added to your dashboards to display real-time data and trends.
- **Microsoft Power BI integration:** This integration allows you to bring Analytics data into Power BI reports, combining simplicity and power. With Power BI, you can create interactive and visually appealing reports that provide a comprehensive view of your project performance.

- **OData support:** OData support enables you to directly query the Analytics service from a supported browser and use the returned JSON data as needed. You can generate queries that span multiple projects or your entire organization, providing flexibility in how you analyze and utilize your data. For more information about the Analytics service, see the [Reporting roadmap](#).

These tools offer robust capabilities for monitoring, analyzing, and reporting on the progress and quality of your software projects. They help you make informed decisions and drive continuous improvement.

## Pricing models

The **cloud offering**, Azure DevOps Services, and the **on-premises offering**, Azure DevOps Server, are available in different pricing models. For more information, review the following articles:

- [Pricing for Azure DevOps Services ↗](#)
- [Pricing for Azure DevOps Server ↗](#)

## Related content

- Explore [essential services](#)
- Discover [client-server tools](#)
- Understand [software development roles](#)

ⓘ **Note:** The author created this article with assistance from AI. [Learn more](#)

# Connect to a project

Article • 02/06/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Learn how to connect to a project from a client, to share code, build apps, track work, and collaborate with team members. You can connect to a project from any of the following clients:

- [Web portal](#)
- [Visual Studio or Team Explorer](#)
- [Android Studio with the Azure DevOps Services Plugin for Android Studio](#)
- [IntelliJ with the Azure DevOps Services Plugin for IntelliJ](#)
- [Visual Studio Code](#)

A project defines a process and data storage in which you manage your software projects from planning to deployment. When you connect to a project, you connect to an organization or project collection. For more information, see [About projects and scaling your organization](#).

## Prerequisites

[+] [Expand table](#)

Category	Requirements
Project membership	<a href="#">Project member</a> .
Remote work	If you work remotely, configure your client to <a href="#">connect to an Azure DevOps Proxy Server</a> . From each client, you can switch context to a different project and connect as a different user.
Code base setup	<a href="#">Set up Git</a> or <a href="#">Set up Team Foundation Version Control (TFVC)</a> .

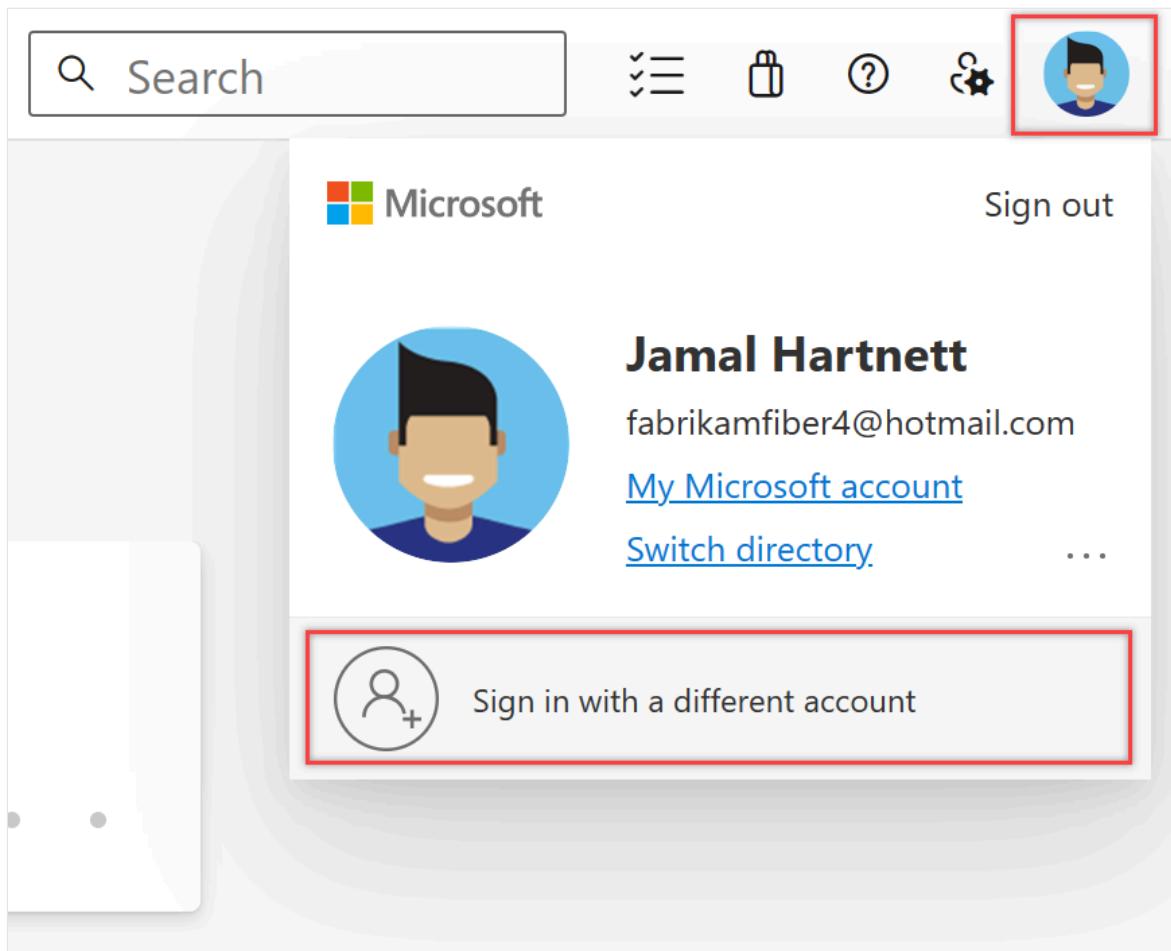
## Connect from the web portal

- Sign in to your project  
([https://dev.azure.com/{Your\\_Organization}/{Your\\_Project}](https://dev.azure.com/{Your_Organization}/{Your_Project})).

For more information, see [Web portal navigation](#).

## Sign in with different credentials

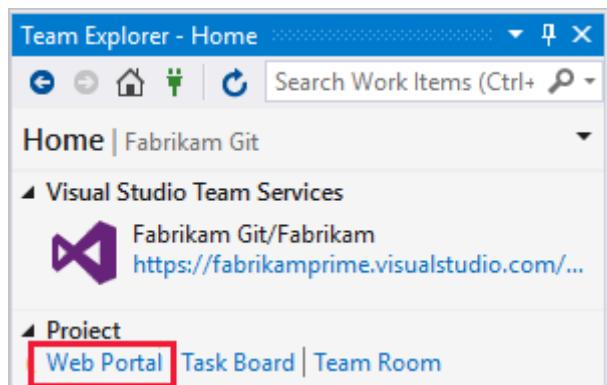
1. Open your profile menu and select **Sign in with a different account**.



2. Choose **Sign in** and enter your credentials.

## Open the web portal from Team Explorer

Open the web portal from the home page.



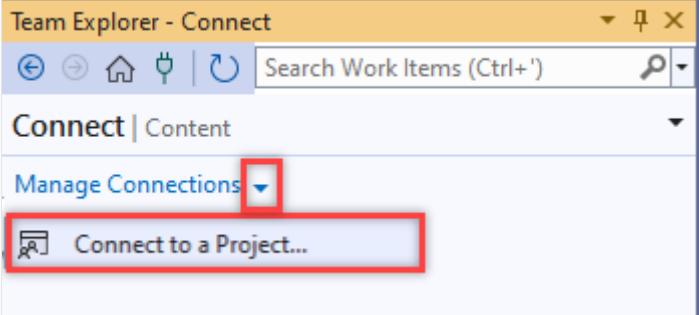
## Connect from Visual Studio or Team Explorer

If you haven't already, [download and install a version of Visual Studio](#).

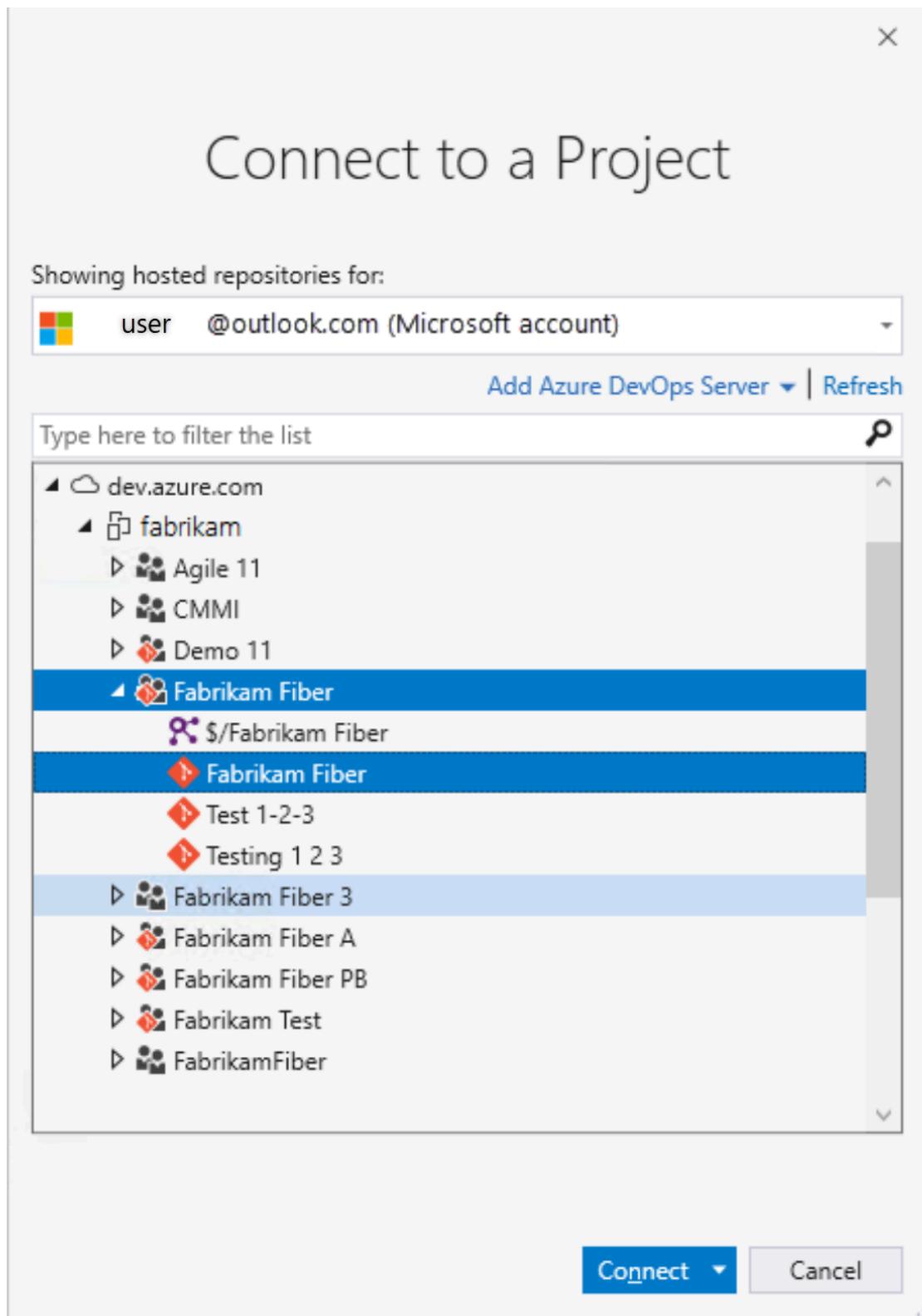
If you're not a member of an Azure DevOps security group, [get added to one](#). Check with a team member. You need the names of the server, project collection, and project to connect to.

Visual Studio 2022

1. Select the **Manage Connections** icon in Team Explorer, and then **Connect to a Project**.



All the projects that you can connect to are displayed, along with the repos in those projects.



2. Select **Add Azure DevOps Server** to connect to a project in Azure DevOps Server. Enter the URL to your server and select **Add**.



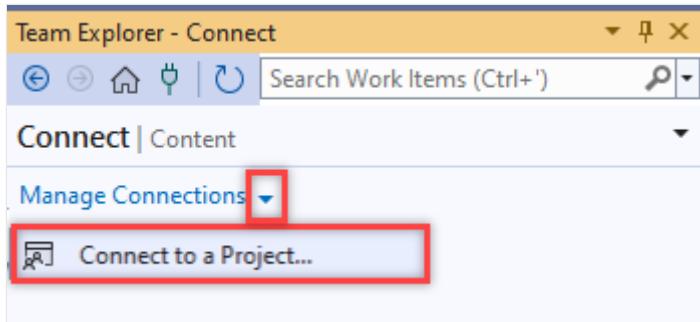
3. Select a project from the list and then select **Connect**.

## Change sign-in credentials

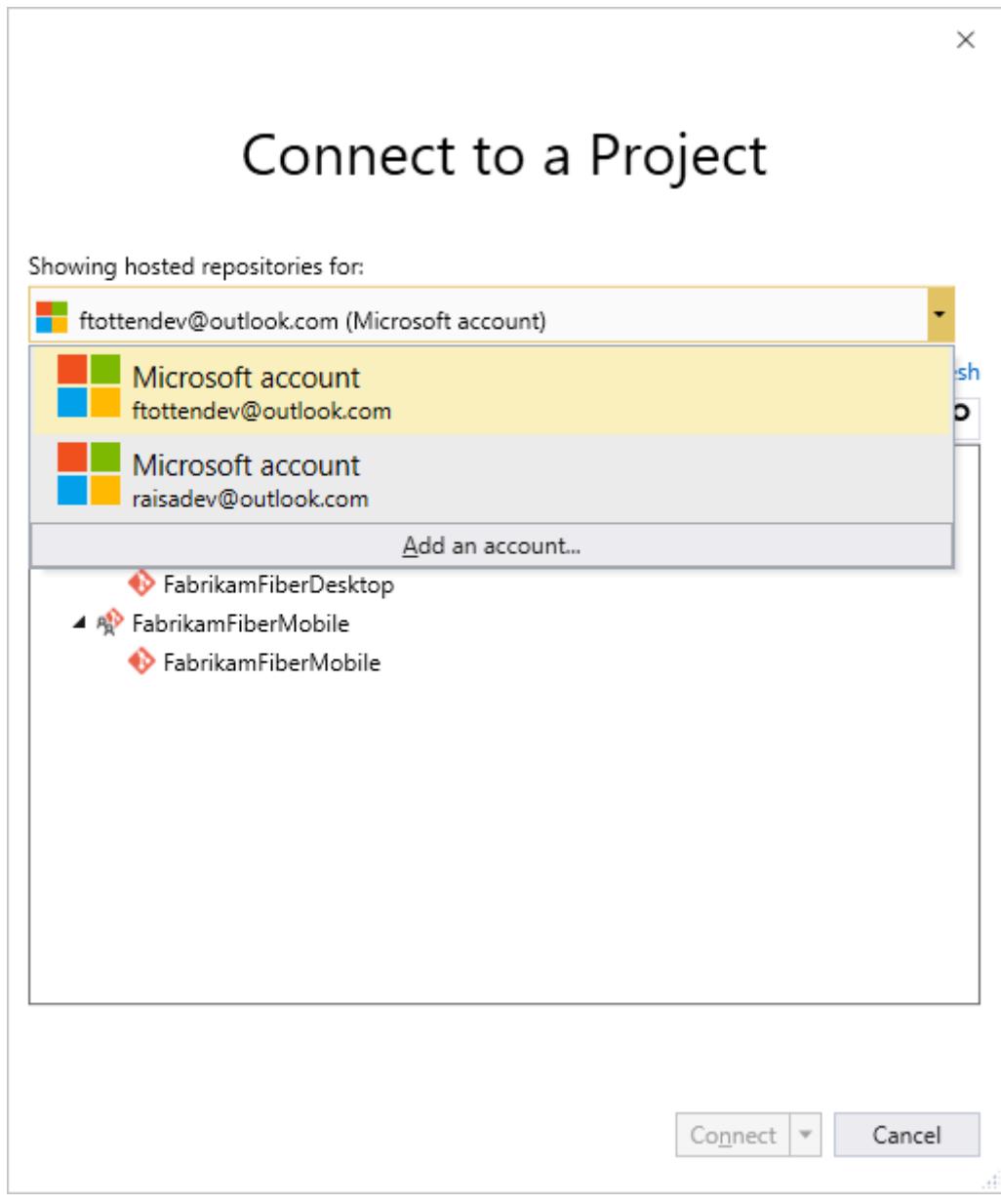
Visual Studio 2022

### Visual Studio 2022

1. Select the **Manage Connections** icon in Team Explorer, and then **Connect to a Project**.



2. Select a different user or select **Add an account** to access a project using different credentials.

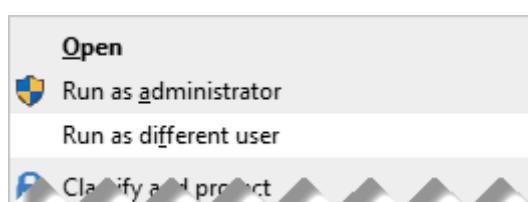


3. Sign in with a Microsoft or GitHub account associated with an Azure DevOps project.

## Use different Visual Studio credentials

You can run Visual Studio with credentials different from your current Windows user account. Find *devenv.exe* under the *Program Files (86)* folder for your version of Visual Studio.

Select Shift and right-click *devenv.exe*, then select **Run as different user**.



# User accounts and licensing for Visual Studio

To connect to a project, you need your user account added to the project. The **Organization owner** for Azure DevOps or a member of the **Project Administrators** group usually adds user accounts. For more information, see [Add organization users and manage access](#) or [Add or remove users or groups, manage security groups](#).

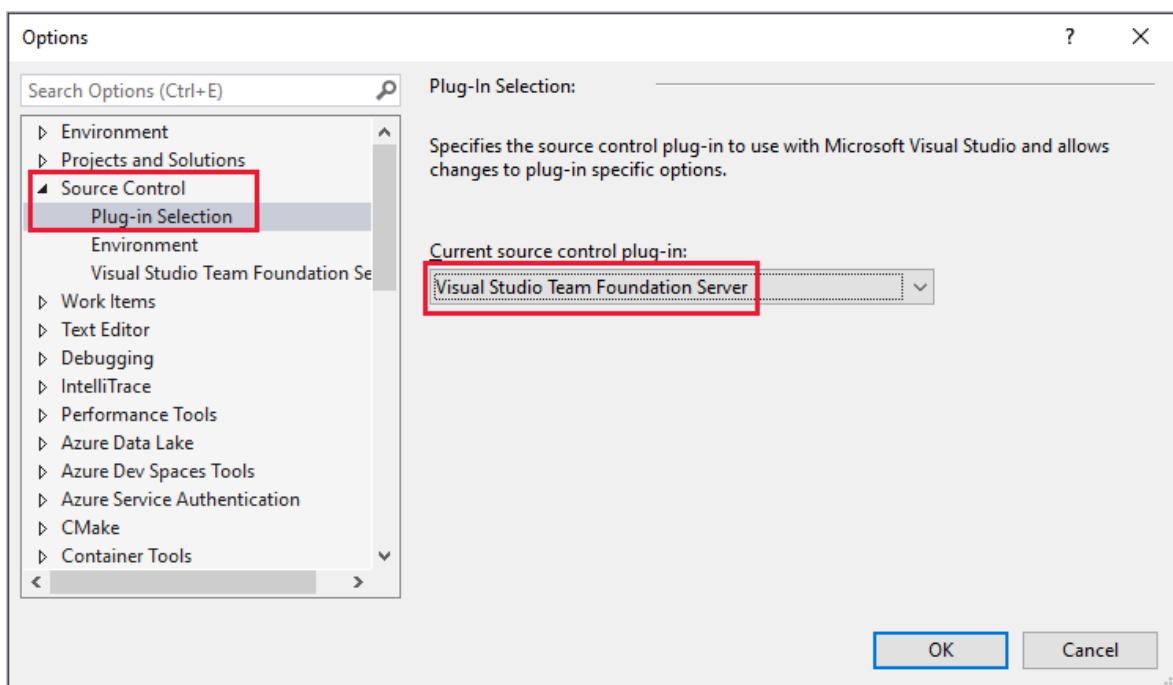
Azure DevOps Services provides access to the first five account users free. After that, you need to [pay for more users](#).

You can also provide access to Stakeholders in your organization with limited access to specific features as described in [Work as a Stakeholder](#).

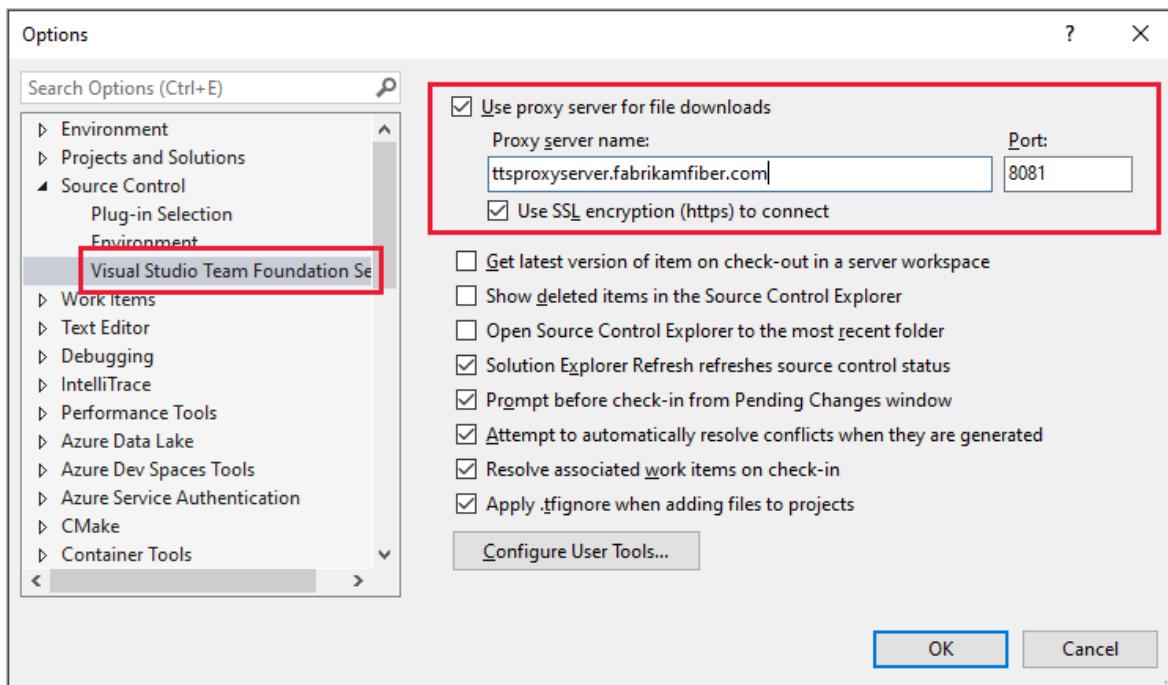
## Configure Visual Studio to connect to Azure DevOps Proxy Server

If your remote team uses an [Azure DevOps Proxy Server](#) to cache files, you can configure Visual Studio to connect through that proxy server and download files under Team Foundation version control.

1. Make sure you're connected to Azure DevOps, as described [in the previous section](#).
2. From the Visual Studio Tools menu, select **Options**, and then select **Source Control > Plug-in Selection**. Select **Visual Studio Team Foundation Server**.



3. For **Visual Studio Team Foundation Server**, enter the name and port number for the Azure DevOps Proxy Server. Select **Use SSL encryption (https) to connect**.



Make sure you specify the port number that your administrator assigned to Azure DevOps Proxy.

To associate a file type with a compare or merge tool, see [Associate a file type with a file-comparison tool](#) or [Associate a file type with a merge tool](#).

## Requirements and client compatibility

Some tasks or features aren't available when you connect to a later version of Azure DevOps than your client supports. For more information, see [client compatibility](#).

## Determine your platform version

See [Look up your Azure DevOps platform and version](#).

## Next steps

[Get started with Agile tools to plan and track work](#)

## Related articles

- [Work in web portal](#)
- [Work in Team Explorer](#)

- Work in Office Excel or Project
  - Troubleshoot connection
- 

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Share your code with Git

Article • 02/05/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Share your code with others in Azure DevOps when you use a Git repository.

## Prerequisites

[ ] Expand table

Category	Requirements
Project access	<a href="#">Project member</a> .
Git command-line tool	One of the following Git command-line tools: - <a href="#">Git for Windows and Git Credential Manager</a> . - <a href="#">Git for macOS or Linux</a> . For macOS and Linux, we recommend that you configure SSH authentication.

## 1. Clone the repo to your computer

To work with a Git repo, clone it to your computer, which creates a complete local copy of the repo. Your code might be in one of several places.

1. Complete the following step that's applicable to your scenario:
  - If You don't have any code yet, first [Create a new Git repo in your project](#), and then complete the next step.
  - If the code is in another Git repo, such as a GitHub repo or a different Azure Repo instance, [import it into a new or existing empty Git repo](#), and then complete the next step.
  - If the code is on your local computer and not yet in version control, either [create a new Git repo in your project](#) or add your code to an existing repository.
2. From your web browser, open the team project for your organization and select **Repos > Files**.

The screenshot shows the 'About this project' page for the 'Fabrikam Fiber' project in Azure DevOps. The left sidebar lists various project management sections: Overview, Summary, Dashboards, Wiki, Boards, Repos (highlighted with a red box and numbered 1), Pipelines, Test Plans, Artifacts, Compliance, and Start Right. The main content area displays the project's name 'Fabrikam Fiber' and its description as an 'Agile process template'. It also lists 'Languages' and provides links to 'Files', 'Commits', 'Pushes', 'Branches', 'Tags', 'Pull requests', and 'Advanced Security'. A red box highlights the 'Files' link, which is numbered 2.

### 3. Select Clone.

The screenshot shows the 'Files' page for the 'Batch' repository within the 'Fabrikam Fiber' project. The left sidebar shows the project navigation. The main content area displays the contents of the 'Batch' folder, including 'arm-templates', 'client-application', 'hpc-application', 'pipelines', and 'README.md'. The 'Clone' button in the top right corner is highlighted with a red box and numbered 2.

### 4. Copy the URL.

## Clone Repository

X

Command line

HTTPS

SSH

[https://fabrikamprime@dev.azure.com/FabrikamFiber01/FabrikamFiber01-01/\\_git/FabrikamFiber01-01](https://fabrikamprime@dev.azure.com/FabrikamFiber01/FabrikamFiber01-01/_git/FabrikamFiber01-01)



[Generate Git Credentials](#)

IDE

[Clone in VS Code](#)

Having problems authenticating in Git? Be sure to get the  
latest version [Git for Windows](#) or our plugins for [IntelliJ](#),  
[Eclipse](#), [Android Studio](#) or [Windows command line](#).

5. Open the Git command window (Git Bash on Git for Windows). Go to the folder where you want the code from the repo stored on your computer, and run `git clone`, followed by the path copied from **Clone URL** in the previous step. See the following example:

```
git clone  
https://FabrikamFiber01@dev.azure.com/FabrikamFiber01/FabrikamFiber01-01/_git/FabrikamFiber01-01
```

Git downloads a copy of the code, including all [commits](#), and [branches](#) from the repo, into a new folder for you to work with.

6. Switch your directory to the repository that you cloned.

```
cd fabrikam-web
```

Keep this command window open to work in a branch.

## 2. Work in a branch

Git [branches](#) isolate your changes from other work being done in the project. We recommend using the [Git workflow](#), which uses a new branch for every feature or fix

that you work on. For our examples, we use the branch, `users/jamal/feature1`.

1. Create a branch with the `branch` command.

```
git branch users/jamal/feature1
```

This command creates a reference in Git for the new branch. It also creates a pointer back to the parent commit so Git can keep a history of changes as you add commits to the branch.

If you're working with a previously cloned repository, ensure you checked out the right branch (`git checkout main`) and that it's up to date (`git pull origin main`) before you create your new branch.

2. Use `checkout` to switch to that branch.

```
git checkout users/jamal/feature1
```

Git changes the files on your computer to match the latest commit on the checked-out branch.

### 💡 Tip

When you create a branch from the command line, the branch is based on the currently checked-out branch. When you clone the repository, the default branch (typically `main`) gets checked out. Because you cloned, your local copy of `main` has the latest changes.

```
git checkout main
git pull origin main
git branch users/jamal/feature1
git checkout users/jamal/feature1
```

You can replace the first three commands in the previous example with the following command, which creates a new branch named `users/jamal/feature1` based on the latest `main` branch.

```
git pull origin main:users/jamal/feature1
```

Switch back to the Git Bash window that you used in the previous section. Run the following commands to create and check out a new branch based on the main branch.

```
git pull origin main:users/jamal/feature1  
git checkout feature1
```

## 3. Work with the code

In the following steps, we make a change to the files on your computer, commit the changes locally, and then push the commit to the repo stored on the server.

1. Browse to the folder on your computer where you cloned the repo, open the `README.md` file in your editor of choice, and make some changes. Then, **Save** and close the file.
2. In the Git command window, go to the `contoso-demo` directory by entering the following command:

```
cd contoso-demo
```

3. Commit your changes by entering the following commands in the Git command window:

```
git add .  
git commit -m "My first commit"
```

The `git add .` command stages any new or changed files, and `git commit -m` creates a commit with the specified commit message.

Check which branch you're working on before you commit, so that you don't commit changes to the wrong branch. Git always adds new commits to the current local branch.

4. Push your changes to the Git repo on the server. Enter the following command into the Git command window:

```
git push origin users/jamal/feature1
```

Your code is now shared to the remote repository, in a branch named `users/jamal/feature1`. To merge the code from your working branch into the `main` branch, use a pull request.

## 4. Merge your changes with a pull request

Pull requests combine the review and merge of your code into a single collaborative process. After you're done fixing a bug or new feature in a branch, create a new pull request. Add the members of the team to the pull request so they can review and vote on your changes. Use pull requests to review works in progress and get early feedback on changes. There's no commitment to merge the changes because you can abandon the pull request at any time.

The following example shows the basic steps of creating and completing a pull request.

1. Open the team project for your organization in your web browser and select **Repos** > **Files**. If you kept your browser open after getting the clone URL, you can just switch back to it.
2. Select **Create a pull request** in the upper-right corner of the **Files** window. If you don't see a message like **You updated users/jamal/feature1 just now**, refresh your browser.

A screenshot of the GitHub Files interface. At the top, there is a search bar with placeholder text "Find a file or folder...". To the right of the search bar are three buttons: "Set up build" (blue), "Fork", and "Clone". Below the search bar, a red box highlights a message: "You updated users/jamal/feature1 just now — Create a pull request". This message is enclosed in a red-bordered box. Below the message, there is a navigation bar with links: "Contents" (underlined), "History", "README", and "New". To the right of the navigation bar are buttons for "Upload file(s)" and "Download as Zip". Further to the right is a "diff" icon. The main content area displays a table of files. The table has columns: "Name", "Last change", and "Commits". The data in the table is as follows:

Name	Last change	Commits
AzureEndpoint.png	5/2/2018	ae9e9911 Initial Commi...
gear.png	5/2/2018	ae9e9911 Initial Commi...
README.md	5/2/2018	ae9e9911 Initial Commi...

New pull requests are configured to merge your branch into the default branch, which in this example is `main`. The title and description are prepopulated with your commit message.

 New Pull Request

From `users/jamal/feature1` into To `main` ↗

Title \*

Add label

Description

My first commit

*Markdown supported.*

Aa **B** *I*      @ # 

My first commit

Reviewers

Search users and groups to add as reviewers

Work Items

Search work items by ID or title



You can [add reviewers](#) and [link work items](#) to your pull request.

You can review the files included in the pull request at the bottom of the **New Pull Request** window.

The screenshot shows a GitHub pull request interface. At the top right is a blue 'Create' button. Below it, under the 'Files (1)' tab, is a list of changes in 'README.md'. The diff shows several additions and one deletion. The additions include instructions for deployment and an exercise about endpoint creation. The deletion is a previous instruction.

```
... ...
13 13
14 14 -----
15 15
16 - Please follow below exercises inorder to deploy your application, :
16 + Please follow below exercises inorder to deploy your application:
17 17
18 18 ## Exercise 1: Endpoint Creation
19 19
... ...
```

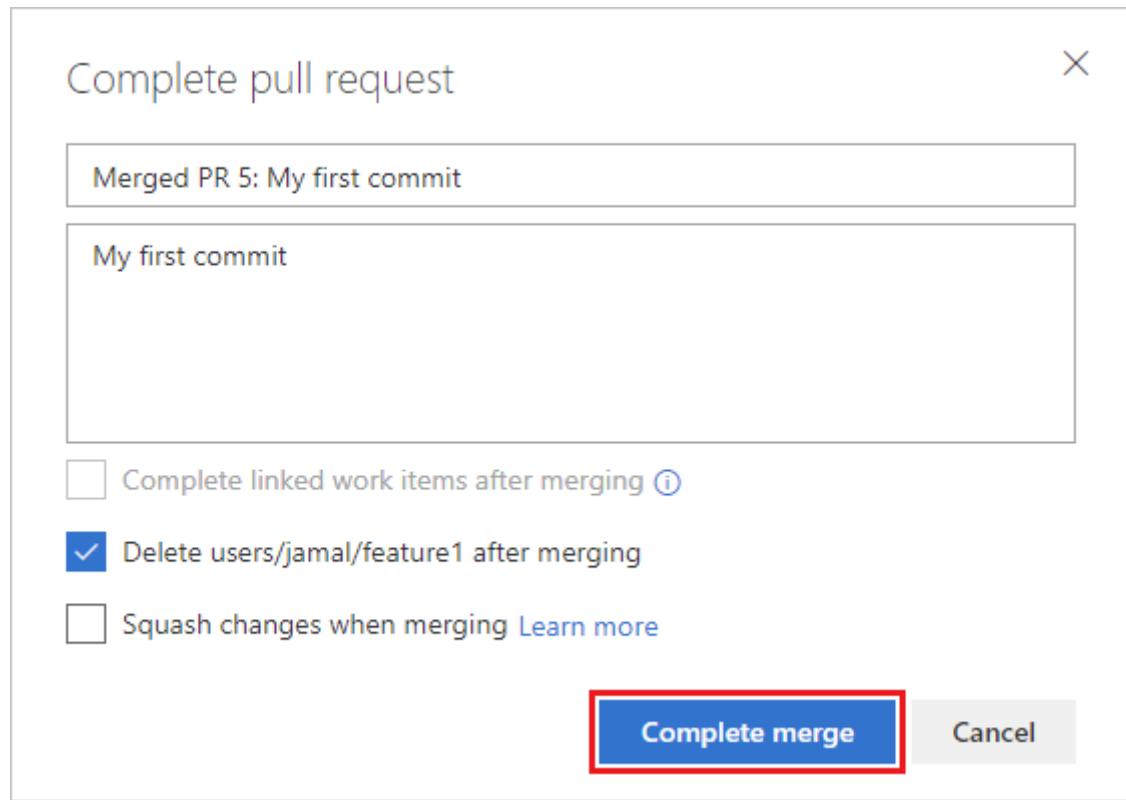
### 3. Select **Create**.

View the details of your pull request from the **Overview** tab. You can also view the changed files, updates, and commits in your pull request from the other tabs.

### 4. Select **Complete** to begin the process of completing the pull request.

The screenshot shows the 'My first commit' pull request page. The 'Overview' tab is selected. A red box highlights the 'Complete' button at the top right. Other tabs shown are 'Files', 'Updates', and 'Commits'. The pull request details include a description, a comment input field, and information about the creator. To the right, there are sections for 'Work Items', 'Reviewers', and 'Labels'.

### 5. Select **Complete merge** to complete the pull request and merge your code into the `main` branch.



#### ① Note

This example shows the basic steps of creating and completing a pull request. For more information, see [Create, view, and manage pull requests](#).

Your changes are now merged into the `main` branch, and your `users/jamal/feature1` branch is deleted on the remote repository.

## View history

1. Switch back to the web portal and select **History** from the **Code** page to view your new commit.

The screenshot shows the GitHub Code History page for the 'FabrikamFibe...' repository. The sidebar on the left shows a file named 'README.md' with a modification icon. The main area has a title 'Files' and tabs for 'Contents' and 'History', with 'History' highlighted. Below this are tabs for 'Graph' and 'Commit'. A single commit is listed at the bottom: 'Added README.md' by '436135f1 Jamal Hartnett Just now'.

2. Switch to the **Files** tab, and select the README file to view your changes.

The screenshot shows a commit history entry for changeset 1529. The commit message is "Updated README". Below the commit message, there is a list of files: "1 My first edit to README file.". The "Annotate" tab is selected.

## Clean up

To delete your local copy of the branch, switch back to your Git Bash command prompt and run the following command:

```
git checkout main  
git pull origin main  
git branch -d users/jamal/feature1
```

This action completes the following tasks:

- The `git checkout main` command switches you to the `main` branch.
- The `git pull origin main` command pulls down the latest version of the code in the main branch, including your changes and the fact that `users/jamal/feature1` was merged.
- The `git branch -d users/jamal/feature1` command deletes your local copy of that branch.

## Next steps

[Set up continuous integration & delivery](#)

## Related articles

- [Understand key concepts for new users to Azure Pipelines](#)
- [Discover what Azure Repos is](#)
- [Learn how to work with a Git repo](#)
- [Explore what source control is](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Create your first pipeline

Article • 03/31/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

This is a step-by-step guide to using Azure Pipelines to build a sample application from a Git repository. This guide uses YAML pipelines configured with the [YAML pipeline editor](#).

For more information on the different sections in a YAML pipeline, see [pipeline](#) in the [Azure Pipelines YAML schema](#) and [Customize your YAML pipeline](#).

If you'd like to use Classic pipelines instead, see [Define your Classic pipeline](#). For guidance on using TFVC, see [Build TFVC repositories](#).

## Prerequisites - Azure DevOps

Make sure you have the following items:

- A GitHub account where you can create a repository. [Create one for free ↗](#).
- An Azure DevOps organization. [Create one for free](#). If your team already has one, then make sure you're an administrator of the Azure DevOps project that you want to use.
- An ability to run pipelines on Microsoft-hosted agents. To use Microsoft-hosted agents, your Azure DevOps organization must have access to Microsoft-hosted parallel jobs. You can either purchase a [parallel job](#) or you can [request a free grant](#).

## Create your first pipeline

Java

### Get the Java sample code

To get started, fork the following repository into your GitHub account.

<https://github.com/MicrosoftDocs/pipelines-java>

## Create your first Java pipeline

1. Sign in to your Azure DevOps organization and go to your project.
2. Go to **Pipelines**, and then select **New pipeline** or **Create pipeline** if creating your first pipeline.
3. Do the steps of the wizard by first selecting **GitHub** as the location of your source code.
4. You might be redirected to GitHub to sign in. If so, enter your GitHub credentials.
5. When you see the list of repositories, select your repository.
6. You might be redirected to GitHub to install the Azure Pipelines app. If so, select **Approve & install**.
7. Azure Pipelines will analyze your repository and recommend the **Maven** pipeline template.
8. When your new pipeline appears, take a look at the YAML to see what it does. When you're ready, select **Save and run**.

If you want to watch your pipeline in action, select the build job.  
You just created and ran a pipeline that we automatically created for you, because your code appeared to be a good match for the [Maven](#) template.  
You now have a working YAML pipeline (`azure-pipelines.yml`) in your repository that's ready for you to customize!
9. You're prompted to commit a new `azure-pipelines.yml` file to your repository. After you're happy with the message, select **Save and run** again.
10. When you're ready to make changes to your pipeline, select it in the **Pipelines** page, and then **Edit** the `azure-pipelines.yml` file.

Learn more about [working with Java](#) in your pipeline.

## View and manage your pipelines

You can view and manage your pipelines by choosing **Pipelines** from the left-hand menu to go to the pipelines landing page.

The screenshot shows the Azure DevOps Pipelines landing page for the 'FabrikamFiber' project. On the left, a navigation bar lists various project management features: Overview, Boards, Repos, Pipelines (selected and highlighted with a red box), Environments, Releases, Library, Task groups, and Deployment groups. The main content area is titled 'Pipelines' and displays the 'Recent' view. It includes a search bar, filter options, and a table of recently run pipelines. The table has columns for Pipeline name, Last run, and timestamp. Two entries are shown: 'pipelines-dotnet-core' (last run 32m ago, triggered manually) and 'FabrikamFiber' (last run 1h ago, triggered manually). A 'New pipeline' button is located in the top right corner.

Pipeline	Last run
pipelines-dotnet-core	#20191209.2 • Set up CI with Az... Manually triggered 32m ago
FabrikamFiber	#20191209.3 • Set up CI with Az... Manually triggered 1h ago

From the pipelines landing page you can view pipelines and pipeline runs, create and import pipelines, manage security, and drill down into pipeline and run details.

Choose **Recent** to view recently run pipelines (the default view), or choose **All** to view all pipelines.

This screenshot shows the same Pipelines landing page as above, but with the 'All' tab selected instead of 'Recent'. The interface is identical, featuring a navigation bar, search/filter, and a table of pipelines. The table shows the same two recent runs: 'pipelines-dotnet-core' and 'FabrikamFiber', each with its build number, description, trigger type, and timestamp.

Pipeline	Last run
pipelines-dotnet-core	#20191209.2 • Set up CI with Az... Manually triggered 36m ago
FabrikamFiber	#20191209.3 • Set up CI with Az... Manually triggered 1h ago

Select a pipeline to manage that pipeline and [view the runs](#). Select the build number for the last run to view the results of that build, select the branch name to view the branch for that run, or select the context menu to run the pipeline and perform other management actions.

Recently run pipelines

Pipeline	Last run	
pipelines-dotnet-core	#20191209.2 • Set up CI with Azure Pip... Manually triggered ⚡ main 1h ago 42s	<span>⋮</span>
FabrikamFiber	#20191209.3 • Set up CI with Azure Pip... Manually triggered ⚡ main 2h 1n	<span>⋮</span>

The context menu for the first pipeline run is open, showing options: Edit, Run pipeline, Manage security, Rename/move, and Delete. The '⋮' button at the top right of the table row is also highlighted with a red box.

Select **Runs** to view all pipeline runs. You can optionally filter the displayed runs.

**Pipelines**

Recent All **Runs** ⋮ Filter

New pipeline

All pipeline runs

Description	Stages	Time
Set up CI with Azure Pipelines #20191209.2 on pipelines-dotnet-core ⚡ main d4964...	✓	44m ago 42s
Set up CI with Azure Pipelines #20191209.1 on pipelines-dotnet-core ⚡ main d4964...	✓	53m ago 46s
Set up CI with Azure Pipelines #20191209.3 on FabrikamFiber ⚡ main 2b4b23c	✓-✓	1h ago 1m 13s
Set up CI with Azure Pipelines #20191209.2 on FabrikamFiber ⚡ main 2b4b23c	✓-✓	1h ago 1m 55s
Set up CI with Azure Pipelines #20191209.1 on FabrikamFiber ⚡ main 2b4b23c	✓-✓	1h ago 1m 6s

Select a pipeline run to view information about that run.

You can choose to **Retain** or **Delete** a run from the context menu. For more information on run retention, see [Build and release retention policies](#).

A screenshot of the Azure Pipelines interface showing a list of stages. The first stage has a green checkmark icon and a timestamp of '51m ago'. The second stage has a green checkmark icon and a timestamp of '42s'. The third stage has a green checkmark icon followed by a minus sign and another green checkmark icon, with a timestamp of '2h ago' and '1m 13s'. A context menu is open over the second stage, showing options 'Retain' and 'Delete'.

## View pipeline details

The details page for a pipeline allows you to view and manage that pipeline.

A screenshot of the Azure DevOps Pipeline details page for the 'FabrikamFiber' pipeline. The top navigation bar includes the Azure DevOps logo, a search bar, and user profile icons. The pipeline name 'FabrikamFiber' is displayed with a back arrow and a 'Run pipeline' button. Below the pipeline name are tabs for 'Runs', 'Branches', and 'Analytics'. The 'Runs' section displays three recent pipeline runs:

Description	Stages	Timestamp
#20191209.3 Set up CI with Azure Pipelines Manually triggered   main   2b4b23c	✓ - ✓	54m ago 1m 13s
#20191209.2 Set up CI with Azure Pipelines Manually triggered   main   2b4b23c	✓ - ✓	55m ago 1m 55s
#20191209.1 Set up CI with Azure Pipelines Individual CI   main   2b4b23c	✓ - ✓	56m ago 1m 6s

Choose **Edit** to edit your pipeline. For more information, see [YAML pipeline editor](#). You can also edit your pipeline by modifying the `azure-pipelines.yml` file directly in the repository that hosts the pipeline.

## View pipeline run details

From the pipeline run summary you can view the status of your run, both while it is running and when it is complete.

#20191210.2 Update azure-pipelines.yml for Azure Pipe... [Run new](#) [:](#)

[Summary](#) [Environments](#)

Triggered by Steve Danielson

FabrikamFiber ➔ main b2f795e

Today at 12:56 PM

Duration: 1m 9s

Tests: [Get started](#)

Changes: 2 commits

Work items: 1 linked

Artifacts: 1 published

[Stages](#) [Jobs](#)

Build Deploy

1 job completed 41s 1 job completed 13s

1 artifact

From the summary pane you can view job and stage details, download artifacts, and navigate to linked commits, test results, and work items.

## Jobs and stages

The jobs pane displays an overview of the status of your stages and jobs. This pane may have multiple tabs depending on whether your pipeline has stages and jobs, or just jobs. In this example, the pipeline has two stages named **Build** and **Deploy**. You can drill down into the pipeline steps by choosing the job from either the **Stages** or **Jobs** pane.

<a href="#">Stages</a>	<a href="#">Jobs</a>		
Name	Status	Stage	Duration
Build	Success	Build	40s
DeployWeb	Success	Deploy	10s

Choose a job to see the steps for that job.

The screenshot shows the Azure Pipelines interface. On the left, there's a sidebar with a back arrow and the text "Jobs in run #20191...". Below it, under the "Build" section, is a list of steps:

- Build (status: green checkmark, duration: 40s)
- Initialize job (status: green checkmark, duration: 1s)
- Checkout (status: green checkmark, duration: 3s)
- CmdLine (status: green checkmark, duration: 2s)
- Component Detect (status: green checkmark, duration: 32s)
- Post-job: Checkout (status: green checkmark, duration: <1s)
- Finalize Job (status: green checkmark, duration: <1s)

Below this, under "Deploy", is a single step:

- > DeployWeb (status: green checkmark, duration: 10s)

At the bottom, under "Finalize build", is one step:

- Report build status (status: green checkmark, duration: <1s)

On the right, the main content area is titled "Build" with a green checkmark icon. It displays the following details:

- Pool: [Azure Pipelines](#)
- Image: [Ubuntu-16.04](#)
- Agent: Hosted Agent
- Started: Today at 1:13 PM
- Duration: 40s
- (empty line)
- 7 ► [Job preparation parameters](#)

From the steps view, you can review the status and details of each step. From the **More actions** you can toggle timestamps or view a raw log of all steps in the pipeline.

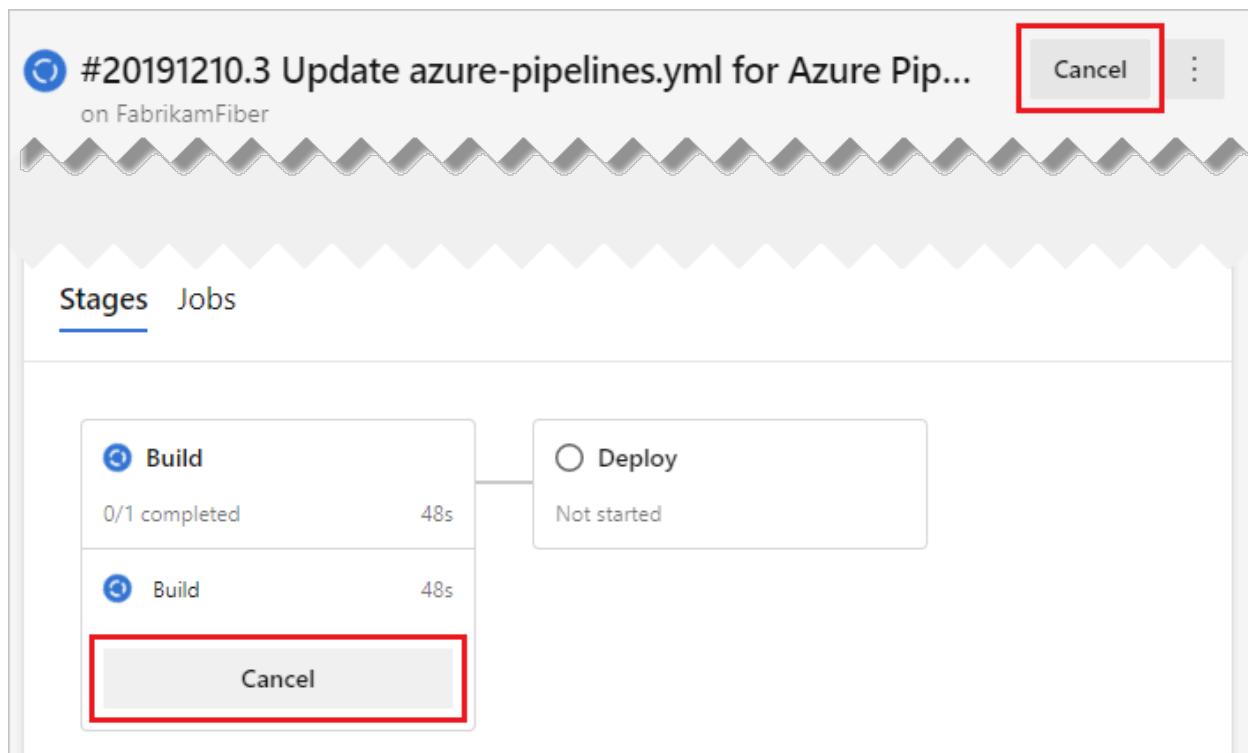
The screenshot shows the same Azure Pipelines interface as above, but with a context menu open over the "Build" summary details. The menu has two items:

- View job raw log
- Toggle timestamps

A red box highlights the three-dot More actions icon in the top right corner of the summary details area.

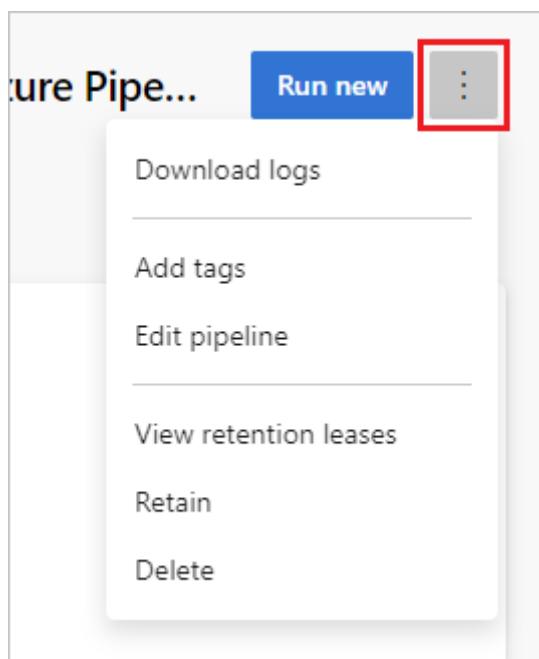
## Cancel and re-run a pipeline

If the pipeline is running, you can cancel it by choosing **Cancel**. If the run has completed, you can re-run the pipeline by choosing **Run new**.



## Pipeline run more actions menu

From the **More actions** menu you can download logs, add tags, edit the pipeline, delete the run, and configure [retention](#) for the run.



### Note

You can't delete a run if the run is retained. If you don't see **Delete**, choose **Stop retaining run**, and then delete the run. If you see both **Delete** and **View retention releases**, one or more configured retention policies still apply to your run. Choose

View retention releases, delete the policies (only the policies for the selected run are removed), and then delete the run.

## Add a status badge to your repository

Many developers like to show that they're keeping their code quality high by displaying a status badge in their repo.



To copy the status badge to your clipboard:

1. In Azure Pipelines, go to the **Pipelines** page to view the list of pipelines. Select the pipeline you created in the previous section.
2. Select , and then select **Status badge**.
3. Select **Status badge**.
4. Copy the sample Markdown from the Sample markdown section.

Now with the badge Markdown in your clipboard, take the following steps in GitHub:

1. Go to the list of files and select `Readme.md`. Select the pencil icon to edit.
2. Paste the status badge Markdown at the beginning of the file.
3. Commit the change to the `main` branch.
4. Notice that the status badge appears in the description of your repository.

To configure anonymous access to badges for private projects:

1. Navigate to **Project Settings** in the bottom left corner of the page
2. Open the **Settings** tab under **Pipelines**
3. Toggle the **Disable anonymous access to badges** slider under **General**

### Note

Even in a private project, anonymous badge access is enabled by default. With anonymous badge access enabled, users outside your organization might be able

to query information such as project names, branch names, job names, and build status through the badge status API.

Because you just changed the `Readme.md` file in this repository, Azure Pipelines automatically builds your code, according to the configuration in the `azure-pipelines.yml` file at the root of your repository. Back in Azure Pipelines, observe that a new run appears. Each time you make an edit, Azure Pipelines starts a new run.

## Next steps

You learned how to create your first pipeline in Azure. Now, Learn more about configuring pipelines in the language of your choice:

- [.NET Core](#)
- [Go](#)
- [Java](#)
- [Node.js](#)
- [Python](#)
- [Containers](#)

Or, you can proceed to [customize the pipeline](#) you created.

To run your pipeline in a container, see [Container jobs](#).

For details about building GitHub repositories, see [Build GitHub repositories](#).

To learn how to publish your Pipeline Artifacts, see [Publish Pipeline Artifacts](#).

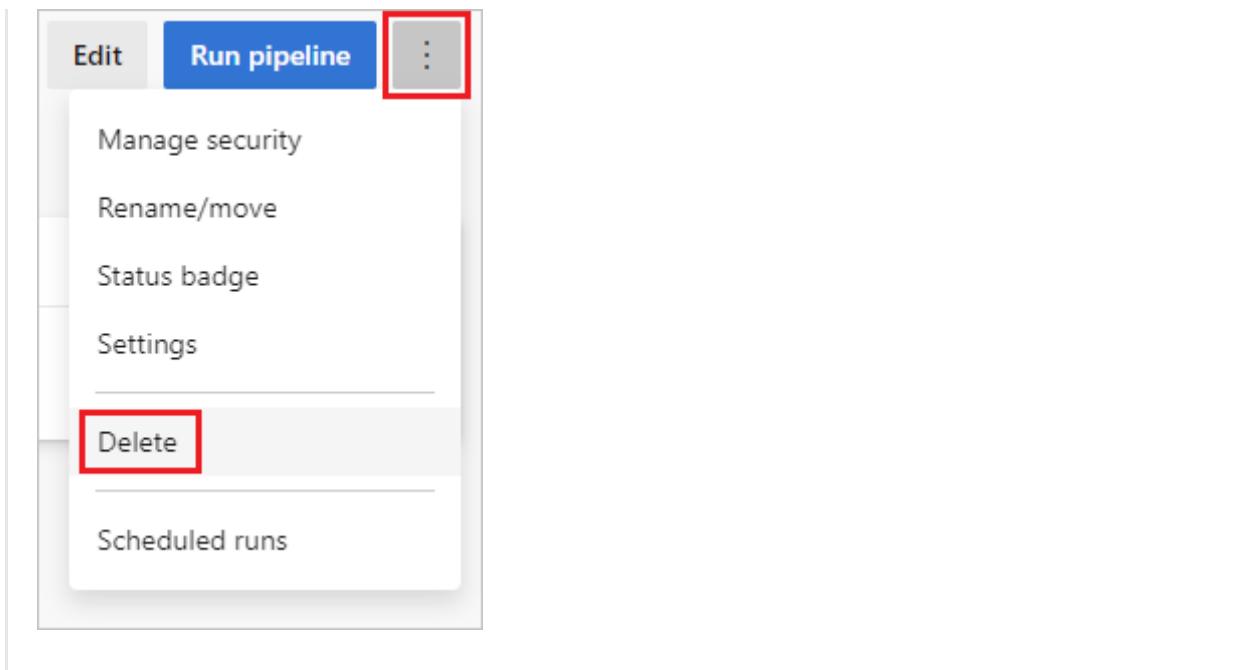
To find out what else you can do in YAML pipelines, see [YAML schema reference](#).

## Clean up

If you created any test pipelines, they're easy to delete when you finish with them.

### Azure Pipelines UI

To delete a pipeline, navigate to the summary page for that pipeline, and choose **Delete** from the ... menu at the top-right of the page. Type the name of the pipeline to confirm, and choose **Delete**.



## FAQ

### Where can I read articles about DevOps and CI/CD?

[What is Continuous Integration?](#)

[What is Continuous Delivery?](#)

[What is DevOps? ↗](#)

### What version control system can I use?

When you're ready to get going with CI/CD for your app, you can use the version control system of your choice:

- Clients
  - [Visual Studio Code for Windows, macOS, and Linux ↗](#)
  - [Visual Studio with Git for Windows or Visual Studio for Mac ↗](#)
  - [Eclipse](#)
  - [Xcode](#)
  - [IntelliJ](#)
  - [Command line](#)
- Services
  - [Azure Pipelines ↗](#)
  - Git service providers such as Azure Repos Git, GitHub, and Bitbucket Cloud
  - Subversion

## How can I delete a pipeline?

To delete a pipeline, navigate to the summary page for that pipeline, and choose **Delete** from the ... menu in the top-right of the page. Type the name of the pipeline to confirm, and choose **Delete**.

## What else can I do when I queue a build?

You can queue builds [automatically](#) or manually.

When you manually queue a build, you can, for a single run of the build:

- Specify the [pool](#) into which the build goes.
- Add and modify some [variables](#).
- Add [demands](#).
- In a Git repository
  - Build a [branch](#) or a [tag ↗](#).
  - Build a [commit](#).

## Where can I learn more about pipeline settings?

To learn more about pipeline settings, see:

- [Getting sources](#)
- [Tasks](#)
- [Variables](#)
- [Triggers](#)
- [Retention](#)
- [History](#)

## How do I programmatically create a build pipeline?

[REST API Reference: Create a build pipeline](#)

 **Note**

You can also manage builds and build pipelines from the command line or scripts using the [Azure Pipelines CLI](#).

---

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Plan and track work in Azure Boards

Article • 01/30/2025

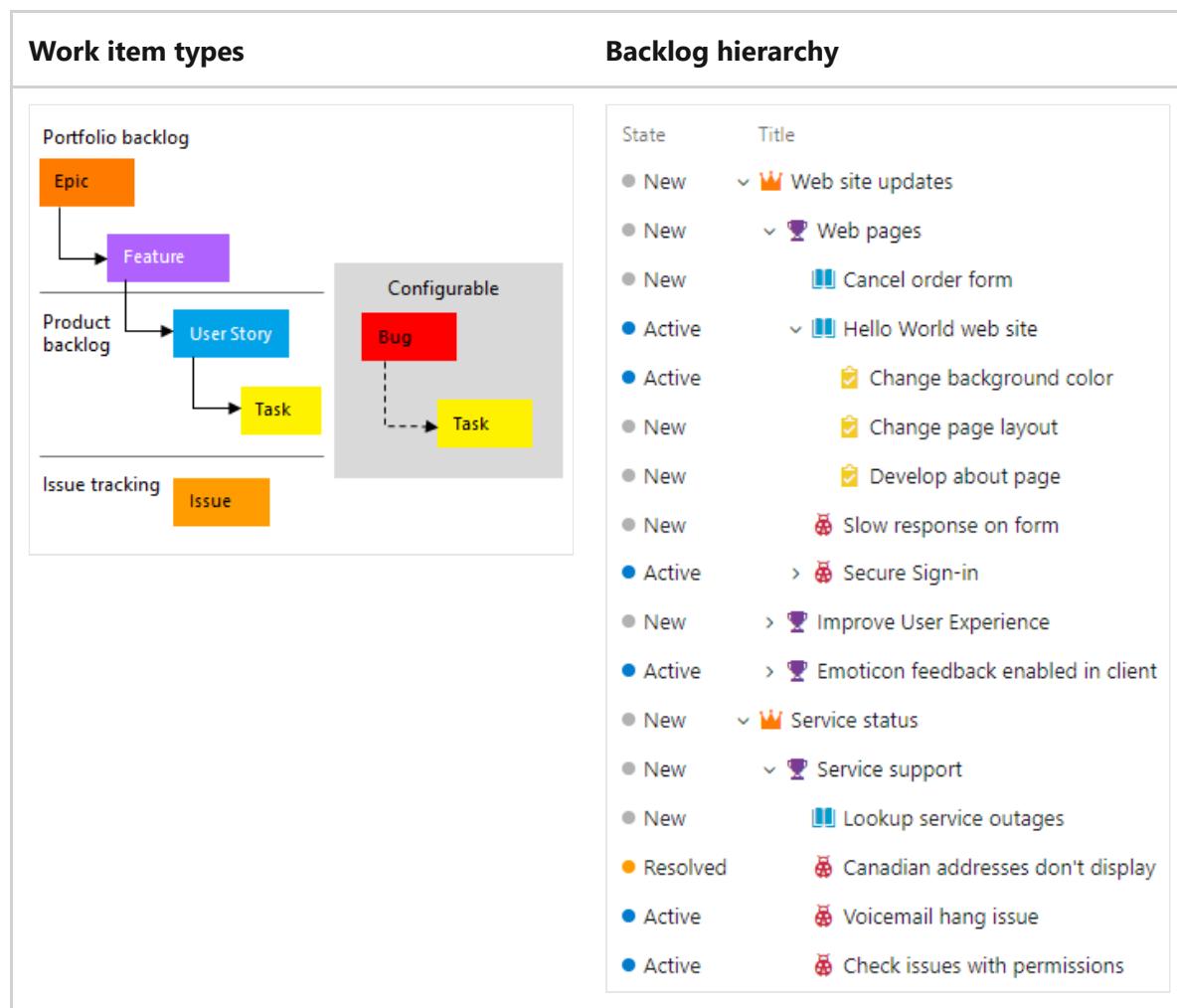
Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

In this article, learn how to use Azure Boards to plan and track your work using an *Agile*, *Basic*, *Scrum*, or *Capability Maturity Model Integration (CMMI)* process. For more information, see [About processes and process templates](#).

## Agile process

The Agile process uses various work item types such as user stories, tasks, bugs, features, and epics to plan and track work. Begin by adding user stories and grouping them into features if needed. You can add tasks to a user story to track more details.

[+] Expand table



In each work item form, you can describe the work to be done, assign work to project contributors, track status, and collaborate with others through the

Discussion section. This article describes how to add user stories and child tasks from the web portal and add details to those work items.

# Prerequisites

[+] Expand table

Category	Requirements
Access levels	<ul style="list-style-type: none"><li>- To add work items to a board and use all other board features: At least <a href="#">Basic access</a>.</li><li>- Private project: To view boards, open and modify work items, and add child tasks to a checklist: At least <a href="#">Stakeholder</a> access. You can't reorder or reparent a backlog item using drag-and-drop. You can't update a field on a card.</li><li>- Public project: For full access to all Boards features: At least <a href="#">Stakeholder</a> access.</li></ul>
Permissions	Member of the <a href="#">Contributors</a> or <a href="#">Project Administrators</a> group.

For more information, see [Default permissions and access for Azure Boards](#).

## Open your board

A board is provisioned with the addition of each project and each team. You can only create or add boards to a project by adding another team. For more information, see [About teams and Agile tools](#).

1. Sign in to your organization ([https://dev.azure.com/{Your\\_Organization}](https://dev.azure.com/{Your_Organization})) and go to your project.
2. Select **Boards > Boards**.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The top navigation bar includes 'Azure DevOps', the organization name 'fabrikamprime', and project names 'Fabrikam Fiber', 'Overview', and 'Summary'. On the left, a sidebar lists project management sections: Overview, Summary, Dashboards, Wiki, Boards (highlighted with a red box), Repos, Pipelines, and Test Plans. The main content area is titled 'Fabrikam Fiber' and displays 'About this project' and 'Agile process template'. A dropdown menu for 'Boards' is open, showing options: Work items, Boards (highlighted with a red box), Backlogs, Sprints, and Queries.

3. Select a board from the All Team Boards dropdown menu.

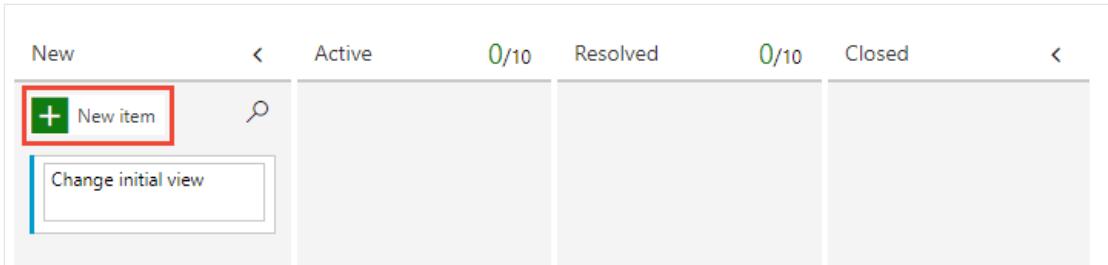
The screenshot shows the 'Boards' page for the 'Fabrikam Fiber' project. The sidebar includes 'Overview', 'Boards' (highlighted with a red box), 'Work items', 'Backlogs', 'Sprints', and 'Queries'. The main area shows a dropdown menu for selecting a board. The 'Fabrikam Fiber Team' option is listed under 'My Team Boards'. Under 'All Team Boards', 'Fabrikam Fiber Team' is also listed, highlighted with a red box. Other options include 'New area', 'New team', and 'Phone'.

## Add work items to your board

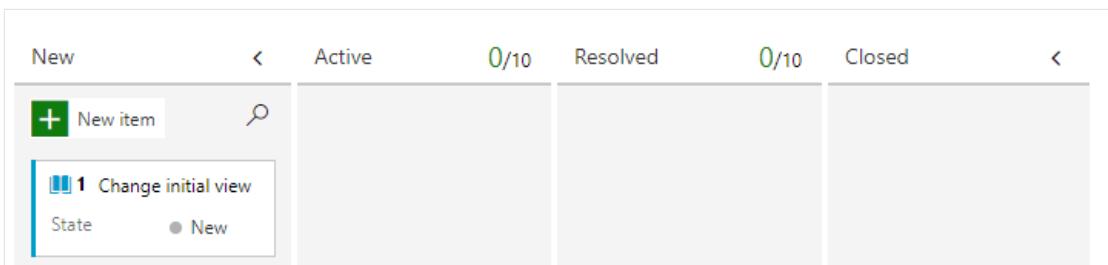
Work items on your board are automatically assigned the default **Area Path** and **Iteration Path** assigned to the team. For more information, see [Manage and configure team tools](#).

## Agile process

1. From the Stories board, choose **New item** and the stories you want to track.



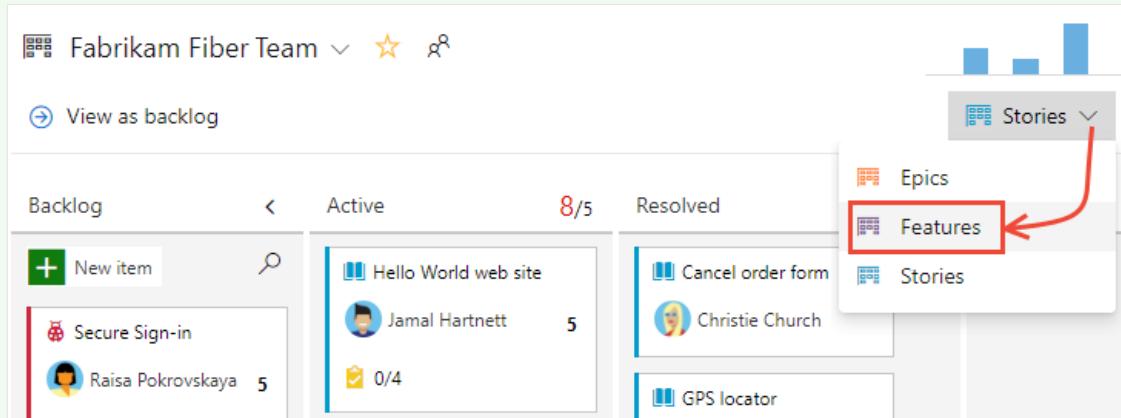
2. Select **Enter**. The system assigns a work item ID to the user story.



3. Add as many user stories as you need.

### Tip

To quickly add features and child user stories, choose **Features** from the board selector.



## Add details to a board item

To open an issue or user story, select its title. Change one or more field values, add a description, or make a note in the **Discussion** section. You can also choose the **Attachments** tab and drag-and-drop a file to share the file with others.

## Agile process

For example, assign the story to Raisa Pokrovskaya and add a discussion note, mentioning Raisa.

The screenshot shows the 'USER STORY 1\*' creation screen. At the top, there's a header with a back arrow, a save icon, and a close icon. Below the header, the title '1 Change initial view' is displayed. On the left, there's a user profile for 'Raisa Pokrovskaya' and a 'Save & Close' button. To the right of the title, there are fields for 'State' (New), 'Reason' (New), 'Area' (Fabrikam Fiber), and 'Iteration' (Fabrikam Fiber). Below these are tabs for 'Details' and 'Related Work items'. The main content area is divided into sections: 'Description' (containing the text 'Switch initial view to the updated design.'), 'Acceptance Criteria' (with a placeholder 'Click to add Acceptance Criteria'), 'Discussion' (containing a message from Raisa: '@Raisa Pokrovskaya - Can you make this happen in the next week?' and a rich text editor toolbar), 'Planning' (with 'Story Points' and 'Priority' set to 2), 'Classification' (with 'Value area' set to 'Business'), 'Development' (with a dropdown menu), and 'Related Work' (with a dropdown menu). The bottom right corner of the window has a '...' button.

When you're done, select **Save & Close**.

## Field descriptions

### Field

### Usage

### Title

Enter a description of 255 characters or less. You can always modify the title later.

## Assigned To

Assign the work item to the team member responsible for performing the work. Depending on the context you're working in, the drop-down menu lists only team members or contributors to the project.

### ⓘ Note

You can only assign work to a single user. If you need to assign work to more than one user, add a work item for each user and distinguish the work to be done by title and description. The Assigned To field only accepts user accounts that have been [added to a project or team](#).

## State

When the work item is created, the State defaults to the first state in the workflow. As work progresses, update it to reflect the current status.

## Reason

Use the default first. Update it when you change state as need. Each State is associated with a default reason.

## Area (Path)

Choose the area path associated with the product or team, or leave blank until assigned during a planning meeting. To change the dropdown list of areas, see [Define area paths and assign to a team](#).

## Iteration (Path)

Choose the sprint or iteration in which the work is to be completed, or leave it blank and assign it later during a planning meeting. To change the drop-down list of iterations, see [Define iteration paths and configure team iterations](#).

## Description

Provide enough detail to create shared understanding of scope and support estimation efforts. Focus on the user, what they want to accomplish, and why. Don't describe how to develop the product. Do provide sufficient details so that your team can write tasks and test cases to implement the item.

---

## Acceptance Criteria

Provide the criteria to be met before the work item can be closed. Define what "Done" means by describing the criteria for the team to use to verify whether the backlog item or bug fix is fully implemented. Before work begins, describe the criteria for customer acceptance as clearly as possible. Have conversations between the team and customers to determine the acceptance criteria. These criteria help ensure a common understanding within the team to meet customers' expectations. Also, this information provides the basis for acceptance testing.

---

## Priority

A subjective rating of the issue or task it relates to the business. You can specify the following values:

- 1: Product can't ship without the successful resolution of the work item, and it should be addressed as soon as possible.
  - 2: Product can't ship without the successful resolution of the work item, but it doesn't need to be addressed immediately.
  - 3: Resolution of the work item is optional, based on resources, time, and risk.
  - 4: Resolution of the work item isn't required.
- 

## Value Area

A subjective rating of the issue or task it relates to the business. You can specify the following values:

- **Architectural:** Technical services to implement business features that deliver solution.
  - **Business:** Services that fulfill customers or stakeholder needs that directly deliver customer value to support the business (Default).
-

## Effort, Story Points, Size

Provide a relative estimate of the amount of work required to complete an issue. Most Agile methods recommend that you set estimates for backlog items based on relative size of work. Such methods include powers of 2 (1, 2, 4, 8) and the Fibonacci sequence (1, 2, 3, 5, 8, etc.). Use any numeric unit of measurement your team prefers.

The estimates you set are used to calculate [team velocity](#) and [forecast sprints](#).

## Update work status

The State field tracks the status of a work item. With the board, you can quickly update the status of backlog items by dragging and dropping them to a different column.

Agile process

As work begins, drag the user story card from the **Backlog** column to the **Active** column. When work is ready for review, move it to the **Resolved** column. After a team member reviews and accepts it, move it to the **Closed** column.

Backlog	Active	Resolved	Closed
<a href="#">New item</a>	<a href="#">Change initial view</a> Raisa Pokrovskaya 5	<a href="#">Cancel order form</a> Christie Church	
<a href="#">Welcome back page</a> Jamal Hartnett 8	<a href="#">Hello World web site</a> Jamal Hartnett 5 0/4	<a href="#">GPS locator</a> Jamal Hartnett 8	

### Tip

To add or rename columns as needed, see [About configuring and customizing Azure Boards](#).

## Add tasks

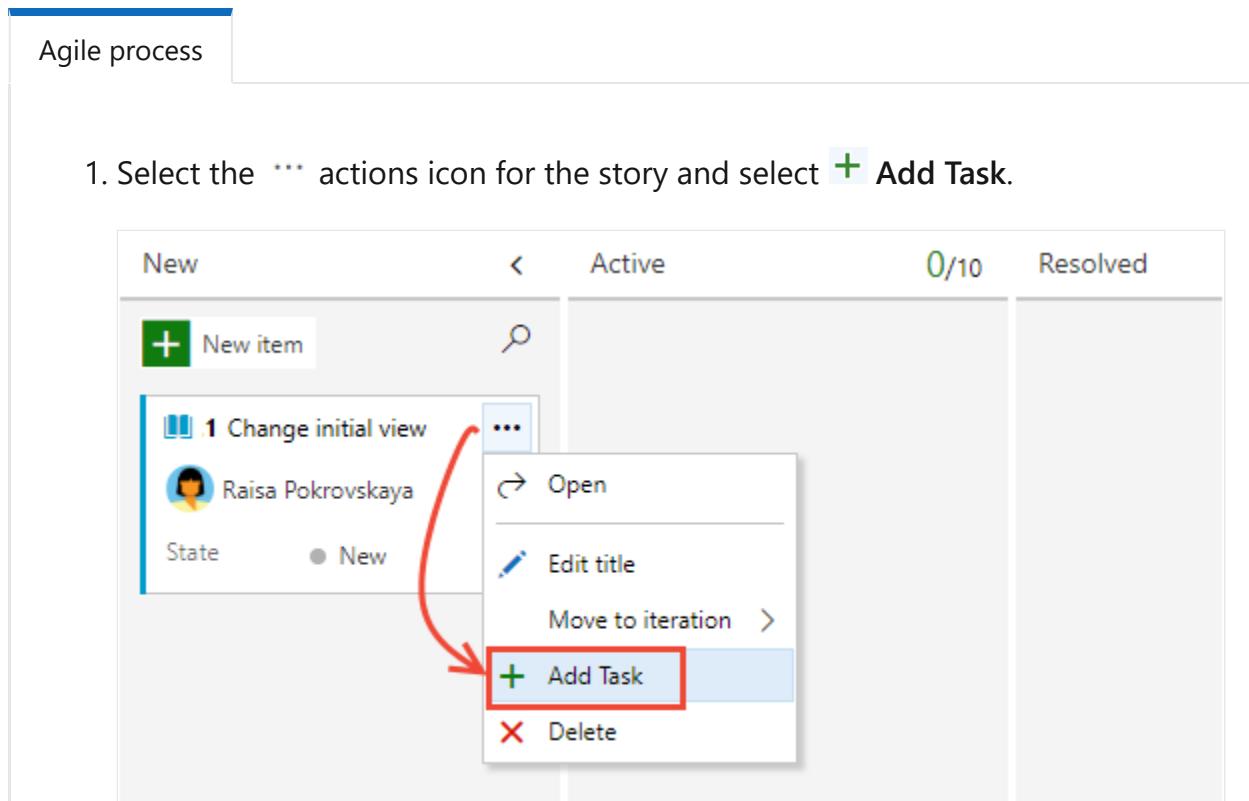
Task checklists provide a quick and easy way to track elements of work that are important to complete a backlog item. Also, you can assign individual tasks to different

team members.

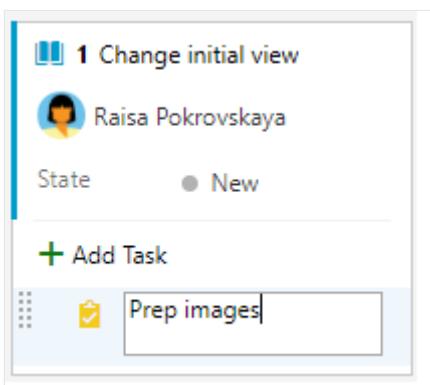
### Tip

Tasks that you create from the board are automatically assigned the **Area Path** and **Iteration Path** of their parent work item and show up on your sprint taskboard.

Tasks that you create from the [sprint backlog](#) or [taskboard](#) show up in tasks checklists on the board.



2. Enter a title for the task and select **Enter**.



3. If you have many tasks to add, keep entering your task titles and select **Enter**.

**1 Change initial view**

Raisa Pokrovskaya

State ● New

0/4

**Add Task**

- Prep images
- Change colors
- Standard form factors
- About screen

4. You can mark a task as done, expand or collapse the task checklist, reorder, and reparent tasks.

Expand table

Mark a task as done	Reorder and reparent tasks	Expand or collapse the checklist
To mark a task as complete, select the task checkbox. The task State changes to Done.	To reorder a task, drag it in the checklist. To reparent a task, drag it to another issue on the board.	To expand or collapse a task checklist, choose the task annotation.

**Mark a task as done**

To mark a task as complete, select the task checkbox. The task State changes to Done.

**Reorder and reparent tasks**

To reorder a task, drag it in the checklist. To reparent a task, drag it to another issue on the board.

**Expand or collapse the checklist**

To expand or collapse a task checklist, choose the task annotation.

## Add details to a task

If you have details you want to add about a task, select the title to open it. Change one or more field values, add a description, or make a note in the **Discussion** section. Choose **Save & Close**.

## Agile process

This example assigns the task to Christie Church.

The screenshot shows a task card for 'Prep images' assigned to 'Christie Church'. The card includes fields for State (New), Reason (New), Area (Fabrikam Fiber), Iteration (Fabrikam Fiber), and various planning and effort details. The 'Description' section contains a rich text editor with a preview of the text 'Prep new images for use on web site.' The 'Discussion' section has a placeholder for comments. The 'Planning' section shows priority 2, activity Design, and effort of 8 hours. The 'Development' and 'Related Work' sections are also visible.

## Field descriptions

You can assign these fields for a backlog item: user story, issue, product backlog item, and requirement. You can specify the following fields for a task to support capacity and time tracking.

### ⓘ Note

There are no inherent time units associated with this field even though the taskboard always shows "h" for hours in relationship to Remaining Work. You can specify work in any unit of measurement your team chooses.

## Field

## Usage

---

### Activity

The type of activity that's required to do a task. For more information, see [Determine and set sprint capacity](#). Allowed values are:

- Deployment
- Design
- Development
- Documentation
- Requirements
- Testing

### Discipline (CMMI process)

The type of activity that's required to do a task. For more information, see [Determine and set sprint capacity](#). Allowed values are:

- Analysis
- Development
- Test
- User Education
- User Experience

### Original Estimate

The amount of estimated work required to complete a task. Typically, this field doesn't change after you assign the task.

### Remaining Work

The amount of work that remains to finish a task. You can specify work in hours or in days. As work progresses, update this field. It's used to calculate [capacity charts](#) and the [sprint burndown chart](#). If you divide a task into subtasks, specify Remaining Work for the subtasks only.

### Completed Work

The amount of work spent implementing a task. Enter a value for this field when you complete the task.

## Task Type (CMMI only)

Select the kind of task to implement from the allowed values:

- Corrective Action
- Mitigation Action
- Planned

## Capture comments in the Discussion section

Use the **Discussion** section to add and review comments made about the work being performed.

### Discussion

 Add a comment. Use # to link a work item, ! to link a pull request, or @ to mention a person.

 **Jamal Hartnett** commented just now  
@**Christie Church** - Assigning this to you

 **Christie Church** commented less than a minute ago  
I've updated the storyboard per our discussions yesterday.

 **Helena Petersen** commented 9 minutes ago  
@**Christie Church, @Jamal Hartnett** - Let's do an A/B test on the colors used in the form.

 **Jamal Hartnett** commented 21 hours ago  
Make sure the standards guidelines are written in a similar manner to those done for account setup.

The rich text editor toolbar appears under the text entry area when you place your cursor in any text box that supports text formatting.

### Discussion

 @**Jamal Hartnett** note that this work item is dependent on [Product Backlog Item 358: Research architecture changes](#)

B / U ≡ ≡ ab v A v ☺ ↶ ↷ ≈ AA v </> @ # ⚭ A 🖼 🗃

### ① Note

A Discussion work item field doesn't exist. To query work items with comments from the Discussion area, filter on the [History field](#). The full content of the text entered in the Discussion text box is added to the History field.

## Mention someone, a group, work item, or pull request

Select one of the following icons to open a menu of recent entries where you mentioned someone, linked to a work item, or linked to a pull request. Alternatively, you can open the same menu by entering @, #, or !.

- @
- #
- !!

The screenshot shows a 'Discussion' interface with a search dropdown menu. The menu is triggered by an '@' symbol and lists recent entries. The entries include user profiles and their names and email addresses. The list starts with 'Christie Church fabrikamfiber1@hotmail.com' and continues with 'Jamal Hartnett fabrikamfiber4@hotmail.com', 'Raisa Pokrovskaya fabrikamfiber5@hotmail.com', and 'Johnnie McLeod fabrikamfiber2@hotmail.com'. Below the list, it says 'Showing 9 results'. The interface has a clean, modern design with blue and white colors.

Enter a name or number to filter the menu list to match your entry. Select the entry you want to add. To bring a group into the discussion, enter @ followed by the group name, such as a team or security group.

## Edit or delete a comment

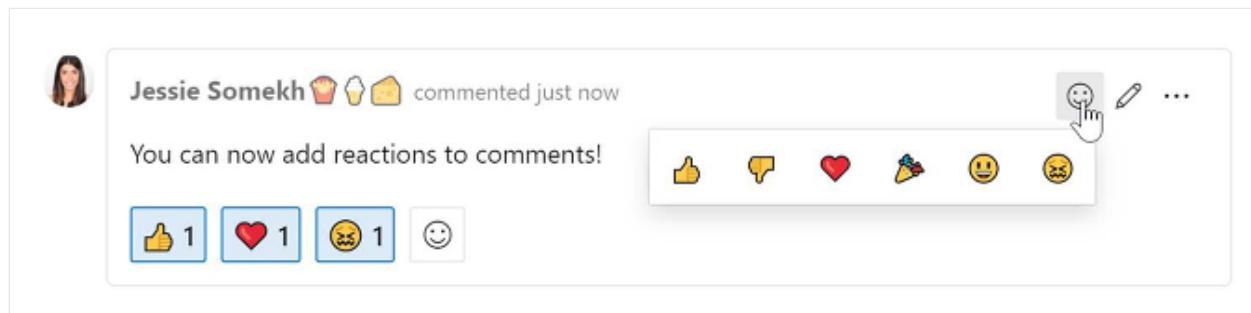
To edit or delete any of your discussion comments, choose [Edit](#) or choose the actions icon and then choose [Delete](#).

The screenshot shows a comment card for 'Raisa Pokrovskaya' from January 7, 2019. The comment text is '@Jamal Hartnett note that this work item is dependent on 358 Research architecture changes'. Below the comment, there is a 'New' button. To the right of the comment, there is a 'More options' icon (three dots) and a 'Delete' button, both of which are highlighted with red boxes. The overall layout is consistent with the 'Discussion' interface shown earlier.

After you update the comment, select **Update**. To delete the comment, confirm that you want to delete it. The **History** tab on the work item form maintains a full audit trail of all edited and deleted comments.

## Add a reaction to a comment

Add one or more reactions to a comment by choosing a smiley icon at the upper-right corner of any comment. Choose from the icons at the bottom of a comment next to any existing reactions. To remove your reaction, choose the reaction on the bottom of your comment. The following image shows an example of the experience of adding a reaction, and the display of reactions on a comment.



## Save a comment without saving the work item

### ⓘ Note

This feature is available starting in Azure DevOps Server 2022.1.

If you only have permissions to add to the **Discussion** of a work item, then you can do so by saving comments. This permission is controlled by Area Path nodes and the **Edit work item comments in this node** permission. For more information, see [Set work tracking permissions](#), [Create child nodes](#), [modify work items under an area or iteration path](#).

When you save the comments, you don't need to save the work item.

A screenshot of the "Discussion" editor. It shows a comment from "@Jamal Hartnett" with the text "Please note the change in the discussion." Below the comment is a rich text toolbar with various icons for bold, italic, underline, etc. At the bottom right are "Cancel" and "Save" buttons.

 Note

When you save changes made to the **Discussion** control, only the comment gets saved. No work item rules defined for the work item type are executed.

## Related articles

### Customize your board

- [Review Azure Boards FAQs](#)
- [Add tags to issues or tasks](#)

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Add, run, update inline tests

Article • 07/24/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Learn how to add, run, update, and expand and collapse inline tests in Azure DevOps.

To start manual testing, add the test to the user story or bug that you want to test. From the board, you can define inline tests or a set of manual tests for a backlog item. You also can run these tests and update their status. If you're new to working with the board, see the [Board quickstart](#).

Tests you create from the board are automatically linked to the user story or backlog item.

## Open your board

1. From your web browser, open the project for your organization and select **Azure Boards**. If you don't have a project, [create one now](#). If you haven't been added as a team member, [get invited now](#).

The URL follows this pattern: `https://dev.azure.com/fabrikamfiber/_boards/board`

If you don't see the team or project you want, select  **Azure DevOps** to [browse all projects and teams](#).

2. Select **Boards** to open the board.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' team. The left sidebar has a 'Boards' section selected. The main area displays the 'Stories backlog' for the 'FabrikamFiber Team'. The backlog is filtered to show 'Active' stories, with 3/5 stories resolved. There are three stories listed:

- Technician can report busy/late on Windows Phone**: Status: Active, 3 tests.
- Technician can see service tickets on Windows Phone**: Status: Active, 0/2 tests.
- Add an information form**: Status: Resolved, 1 test.
- Welcome back page**: Status: Resolved.
- Secure sign in**: Status: Resolved.

## Add tests

1. To add tests, open the menu for a work item.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. On the left, the 'Boards' menu is selected. In the main area, a user story titled 'Technician can see service tickets on Windows Phone' is listed under the 'Stories backlog'. A context menu is open next to the story, with the 'Add Test' option highlighted by a red box.

New < Active

+ New item

...

Open

Edit title

Move to iteration >

Add Task

**Add Test**

Delete

New branch...

Add to dashboard >

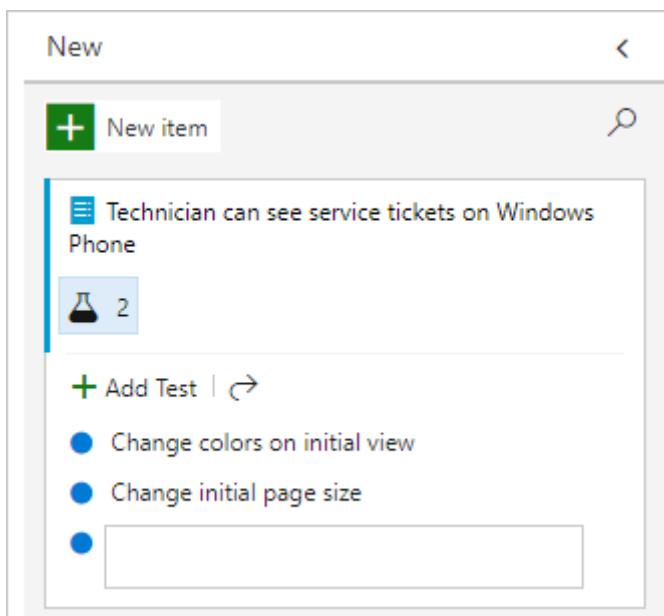
Inline tests are the same as test cases in a test suite. A default test plan and test suite automatically get created under which the manual test cases are grouped.

For example, a test suite is created for the following user story, and inline tests are added to that suite. User story 314 is highlighted. It has two manual tests defined with the IDs 337 and 341.

The screenshot shows the 'Test Plans' section of the Azure DevOps interface. A test suite named '314 : Technician can see service tickets on Windows Phone' is selected. The 'Tests' tab is active, displaying two manual test cases with IDs 337 and 341, both marked as 'Active'.

Outcome	Order	ID	Title
Active	1	337	Change colors on initial view
Active	2	341	Change initial page size

2. If you have a number of tests to add, enter each title and select **Enter**.



To add details to the test case, open it. You can select the title, double-select the inline item, or open the context menu and choose **Open**.

**TEST CASE 337**

337 Change colors on initial view

Author: Jamal Hartnett | Comments: 0 | Tags: Add tag | Save & Close | Follow | ...

State: Design | Area: FabrikamFiber  
Reason: New | Iteration: FabrikamFiber\Release 1\Sprint 3

Steps | Summary | Associated Automation | (1) |

**Steps**

Click or type here to add a step

**Development**

+ Add link  
Development hasn't started on this item.

**Related Work**

+ Add link | Tests  
314 Technician can see serv... Updated 2/28/2013, New

**Details**

Priority: 2  
Automation status: Not Automated

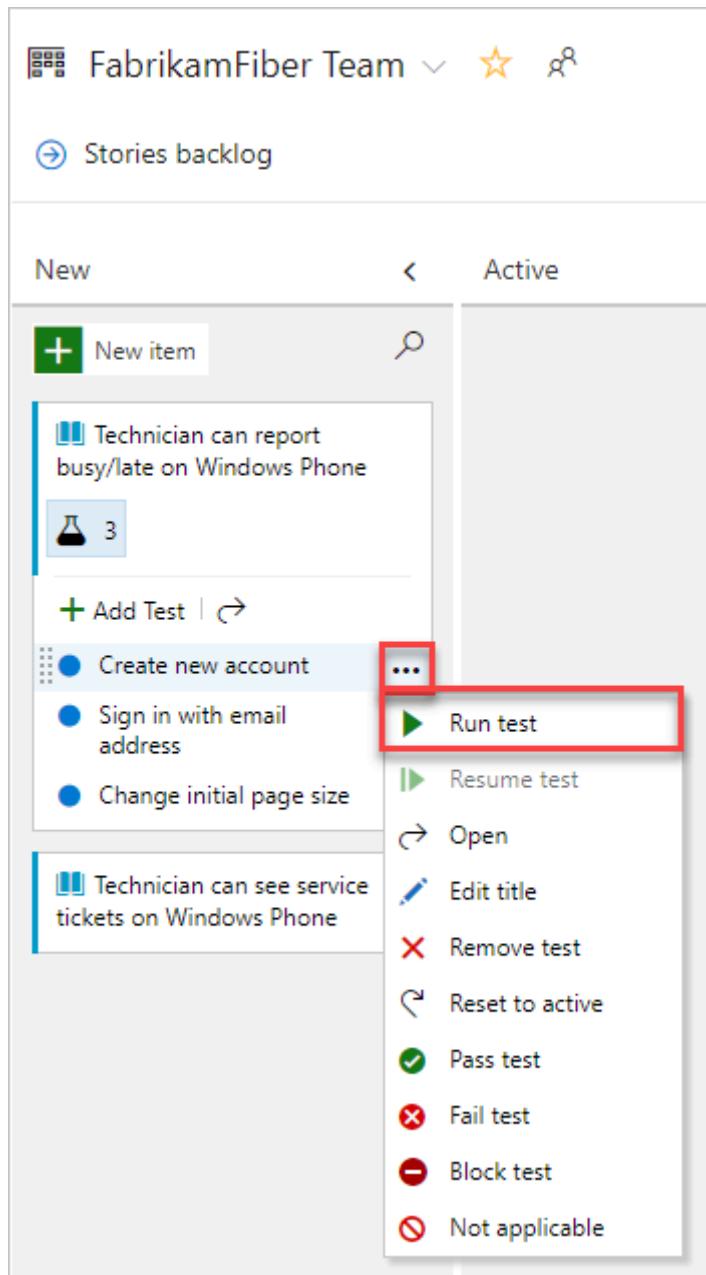
Parameter values

For more information about how to define tests, see [Create manual tests](#).

Before you run the test, you must add details.

## Run a test

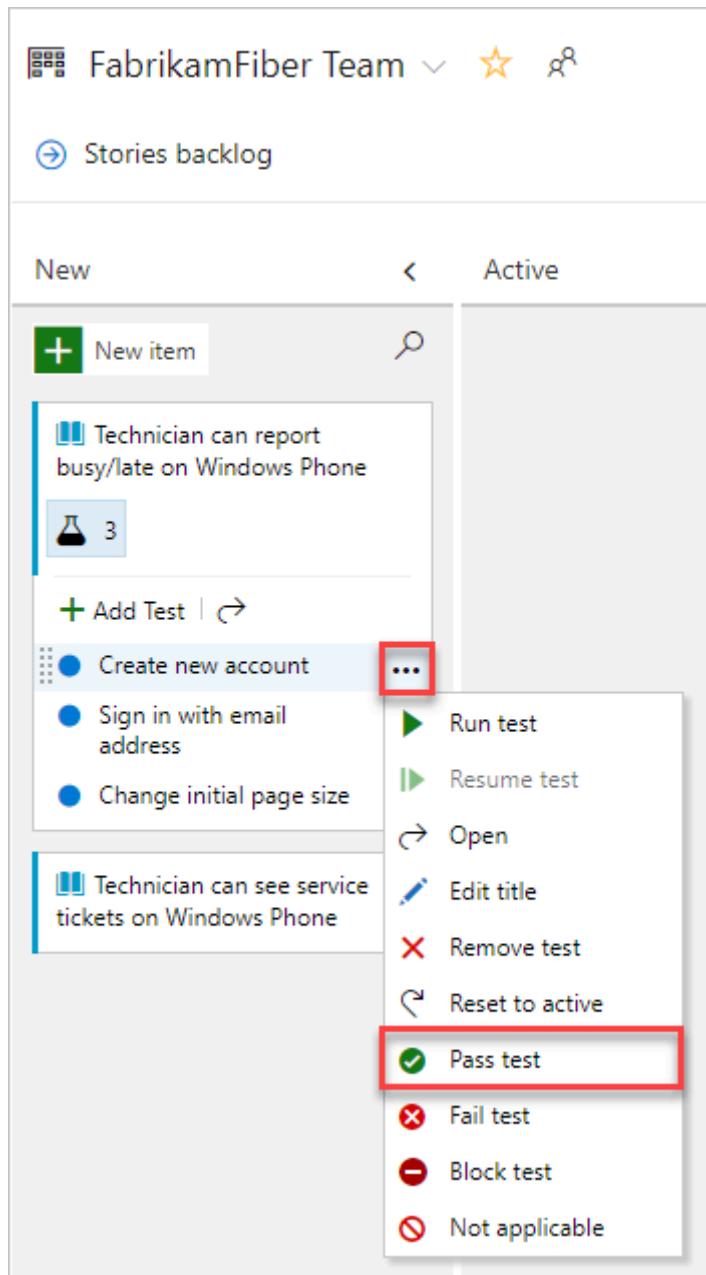
Run the test by selecting ► Run test from the \*\*\* actions menu for the inline test.



Microsoft Test Runner starts in a new browser instance. For information on how to run a test, see [Run manual tests](#).

## Update the status of a test

You can update the status of the test from the \*\*\* actions menu.



When you update the status of tests, you can [track test results](#).

## Expand or collapse inline tests

When you first open the board, you'll see an unexpanded view of checklists and tests.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' team. The left sidebar has 'Boards' selected. The main area displays the 'Stories backlog' for the 'FabrikamFiber Team'. A card for a story titled 'Technician can report busy/late on Windows Phone' is expanded, showing two test cases (indicated by a flask icon with the number 2) and a summary for 'Technician can see service tickets on Windows Phone' assigned to 'Jamal Hartnett'. Other cards visible include 'Add an information form', 'Welcome back page', and 'Secure sign in'.

Select the inline test summary to expand a collapsed set of tests. Select the same summary to collapse an expanded list.

This comparison illustrates the interaction with a test summary. On the left, a card for a story is shown with a red box highlighting the flask icon containing the number '2'. On the right, after selecting the summary, a red arrow points to the 'Add Test' button, which has expanded the list of test cases below it.

## Next steps

[Board quickstart](#)

## Related articles

- [Learn more about test case management](#)
- [Exploratory test your web app directly in your browser](#)
- [Essential services](#)
- [Client-server tools](#)
- [Software development roles](#)

---

# Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Tutorial: Follow changes made to a user story, bug, or other work item or pull request

Article • 11/22/2024

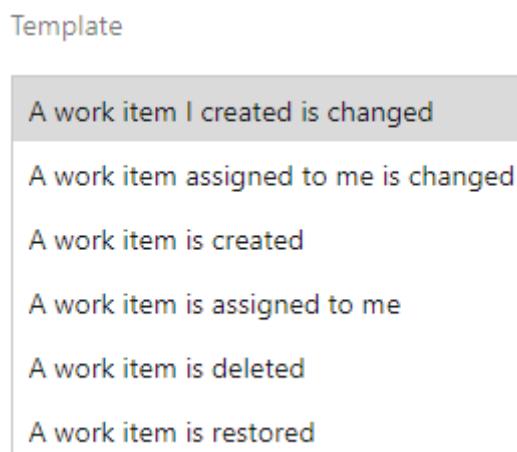
Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

To get notified of changes made to a specific work item or a pull request, you can choose to follow them. The Follow feature provides an improvised way of getting notified on a case-by-case basis.

If you want to subscribe to receive notifications automatically based on changes that occur based on your targeted set of criteria, see [Manage personal notifications](#). For example, you can create a subscription to automatically get notified whenever a work item that you created or that was assigned to you is modified.

## Note

Notification subscriptions allow you to personalize the notifications you receive automatically based on additional criteria you specify for [yourself](#), a team, or a project. For example, you can create a subscription and add field criteria to receive changes based on one or more of the following templates.



This article shows you how to:

- ✓ Follow a work item
- ✓ Follow a pull request
- ✓ Manage work items that you're following

# Prerequisites

- **Permissions:**
  - To view, follow, and edit work items, have **View work items in this node** and **Edit work items in this node** permissions set to **Allow**. By default, the **Contributors** group has these permissions. For more information, see [Set work tracking permissions](#).
- To add tags to work items, have the project-level **Create new tag definition** permission set to **Allow**. By default, the **Contributors** group has this permission.
- **Access levels:**
  - Be a [project member](#).
  - To add new tags to work items or to view or follow pull requests, have at least **Basic** access.
  - To view or follow work items, have at least **Stakeholder** access. For more information, see [About access levels](#).
  - All project members, including those in the **Readers** group, can send emails containing work items.

## ① Note

- Provide [\*\*Stakeholder access\*\*](#) to members who want to contribute to the discussion and review progress. These are typically members who don't contribute to code, but want to view work items, backlogs, boards, and dashboards.

- By default, all **Contributors** and **Stakeholders** in public projects can add new and existing tags. In private projects, Stakeholders can only add existing tags. To control the ability to create new tags, set the **Create tag definition** permission at the project level. For more information, see [Change project-level permissions](#).

## Follow a work item

When you want to track the progress of a single work item, choose the  [Follow](#) follow icon. This signals the system to notify you when changes are made to the work item.

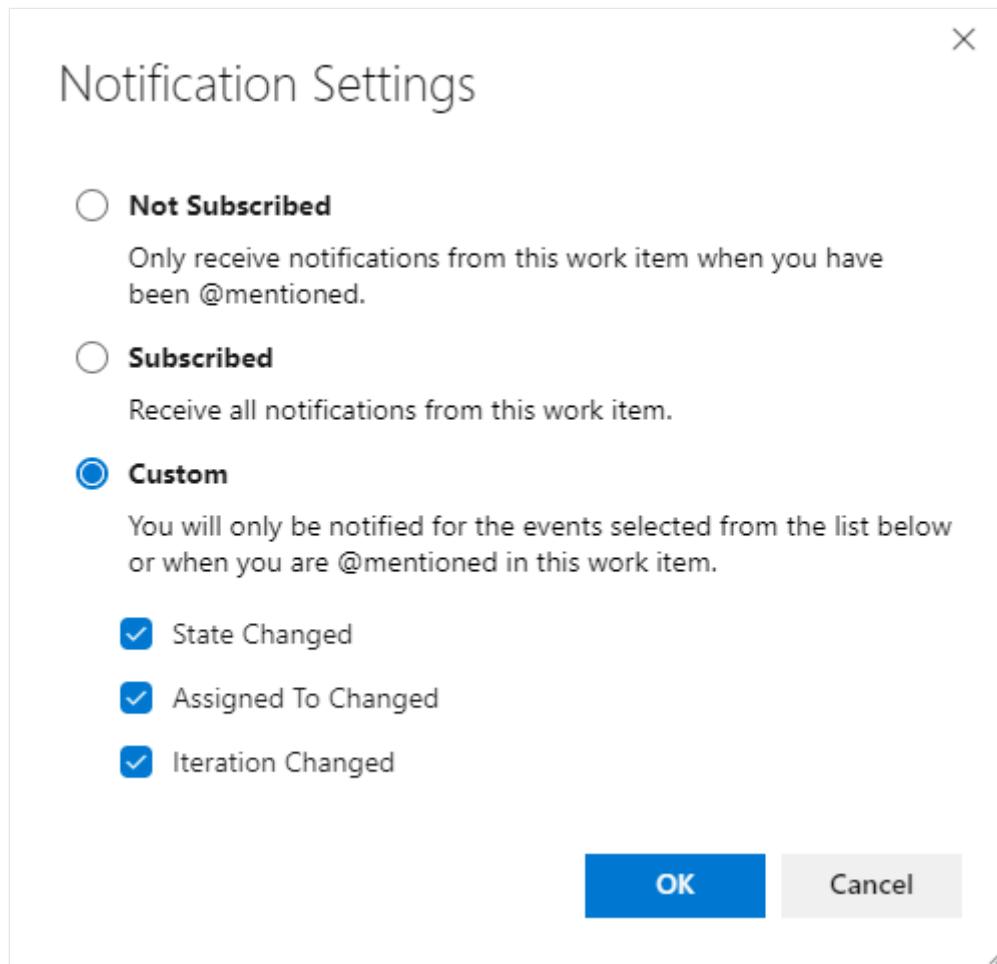
BUG 31  
31 Cancel order form

Jamal Hartnett 0 Comments Add Tag Save Follow

Approved Area FabrikamFiber Updated by Jamal Hartnett: Yesterday

Work stopped Iteration FabrikamFiber Details Scans 0 0

If you want to specify conditions on when you'll get notified of changes, choose the gear icon and choose from the options provided.



By default, you're **Subscribed** to receive a notification when any change is made to the work item. Choose **Not Subscribed** to receive notification only when you're @mentioned. Or choose **Custom** to receive notifications when one of the checked fields changes, **State**, **Assigned To**, or **Iteration Path**.

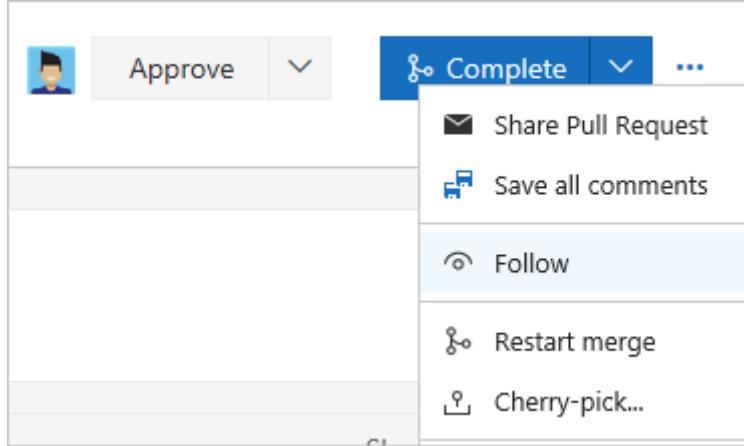
You'll only receive notifications when other members of your team modify the work item, such as adding to the discussion, changing a field value, or adding an attachment.

Notifications are sent to your preferred email address, which [you can change from your user profile](#)

To stop following changes, choose the following icon.

# Follow a pull request

To track the progress of a single pull request, choose the  actions icon for the pull request, and select the  [Follow](#) option. This signals the system to notify you when changes are made to the PR.



You'll only receive notifications when other members of your team modify the PR, such as adding to the discussion or adding an attachment.

Notifications are sent to your preferred email address, which [you can change from your user profile](#).

To stop following changes, open the PR context menu and choose the  Following icon.

## Manage work items that you're following

You can review and manage all the work items you've selected to follow.

Open **Boards>Queries**, choose **All**, and under **My Queries**, choose **Followed work items**.

The screenshot shows the 'Queries' page in the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar has 'Queries' selected. At the top, there are tabs for 'Favorites' and 'All', with 'All' highlighted. Below is a search bar labeled 'Title'. A section titled 'My Queries' contains several items: 'Active bugs', 'All Items', 'Assigned to me', 'Closed bugs', 'Fabrikam Fiber Team - Backlog items', 'Followed work items' (which is also highlighted with a red box), and 'Following - my query'. Each item has a small icon and a yellow star rating.

From this view, you can view all items you're following across all projects. Also, you can complete similar actions supported with a query results view, such as:

- Refresh the view
- Add or remove visible columns
- Sort the order of specific columns
- Filter results by text or tags
- Set work item pane
- Enter full screen mode.

You can also view and manage work that you're following from **Boards>Work Items** and pivot to **Following**.

The screenshot shows the 'Work Items' page in the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar has 'Work Items' selected. At the top, there is a dropdown labeled 'Following' with a red box around it, followed by buttons for 'New Work Item', 'Open in Queries', and 'Column Op'. Below is a table with columns: ID, Assigned To, State, and Title. The table lists several work items:

ID	Assigned To	State	Title
375	Jamal Hartnett	Committed	Check service status
361	Christie Church	Approved	Interim save on long form
384	Christie Church	Committed	Secure sign-in
360	Raisa Pokrovskaya	New	Change initial view
436	Jamal Hartnett	Committed	Hello World Web Site

# Query work items that you're following

You can use the `@Follows` macro in a work item query to filter a list based on work items you're following along with other query filters.

For example, the following query shows how to query across all projects for active work items that you're following. You use the `ID` field and the `In` operator with the `@Follows` macro.

The screenshot shows the Azure DevOps Query Editor interface. At the top, it says "Queries > My Queries" and "3 work items 1 selected". Below that, there are tabs for "Results", "Editor" (which is selected), "Charts", "GANTT", and "Export". There's also a "Run query" button and a "..." button. On the right, there's a refresh icon. Under "Type of query", it says "Flat list of work items" and "Query across projects" with a checked checkbox. The main area is titled "Filters for top level work items" and contains a table with three clauses:

And/Or	Field*	Operator	Value
+ X	Work Item Type	=	[Any]
+ X	State	=	Active
+ X	ID	In	@Follows

At the bottom left of the query editor, there's a link "Add, update, and follow a work item".

## Next steps

[Add, update, and follow a work item](#)

## Related articles

- [Manage personal notifications](#)
- [View and update work items via the mobile work item form](#)

## Q: Can I add someone else to follow a work item or PR?

A: No, you can't add another team member to follow a work item or pull request at this time. You can subscribe them to get notified based on select criteria, such as when a work item is created or modified, or a pull request is created. For more information, see [Manage team notifications](#).

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# Get started as a Stakeholder

Article • 02/07/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

*Stakeholders* are users with free but limited access to Azure DevOps features and functions. With Stakeholder access, you can add and modify work items, manage build and release pipelines, and view dashboards. You can check project status and provide direction, feedback, feature ideas, and business alignment to a team. For more information, see [Create your first pipeline](#) and [Supported source repositories](#).

For more information, see the [Stakeholder access quick reference](#) and the [feature matrix](#).

## Prerequisites

[ ] [Expand table](#)

Category	Requirements
Private project:	
Access levels	Stakeholder access. To get access as a Stakeholder, ask your organization owner or Project Collection Administrator to add you to a project with Stakeholder access. For more information, see <a href="#">Add organization users and manage access</a> .
Permissions	Member of the <b>Contributors</b> or <b>Project Administrators</b> group. You can view boards, open and modify work items, and add child tasks to a checklist. You can't reorder or reparent a backlog item by using the drag-and-drop method. You can't update a field on a card.
Public project:	
Access levels	Stakeholder access.
Permissions	Member of the <b>Contributors</b> or <b>Project Administrators</b> group for full access. For more information, see <a href="#">Default permissions quick reference</a> .

## Sign in to a project

1. Select the link provided in your email invitation or open a browser window and enter the URL for the web portal.

<https://dev.azure.com/OrganizationName/ProjectName>

2. Enter your credentials. If you can't sign in, ask the organization owner or Project Administrator to add you as a member of the project with Stakeholder access.

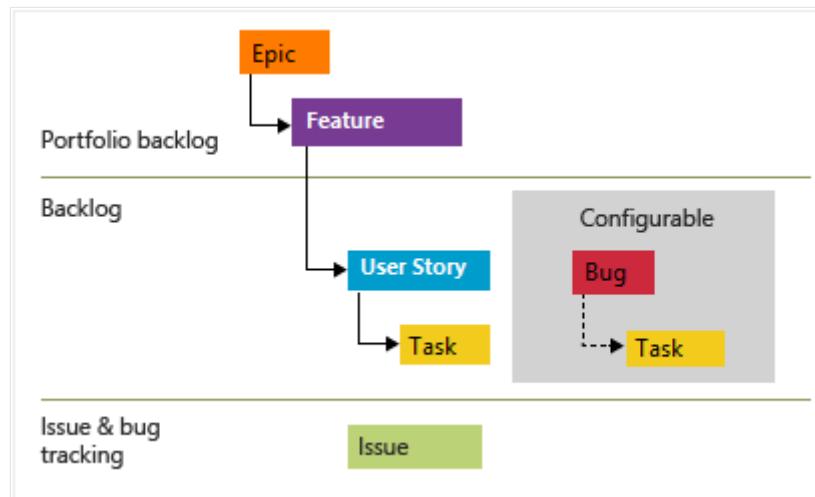
## Understand work items and types

Work items support planning and tracking work. Each work item is based on a work item type. Each work item is assigned an identifier, which is unique in an organization or project collection.

Different work items track different types of work. The work item types available are based on the [process that was used when your project was created](#). The options are *Agile*, *Basic*, *Scrum*, or *Capability Maturity Model Integration (CMMI)*, as illustrated in the following images. For more information, see [About work items and work item types](#).

### Agile process

The following image shows the hierarchy for the Agile process backlog work item:



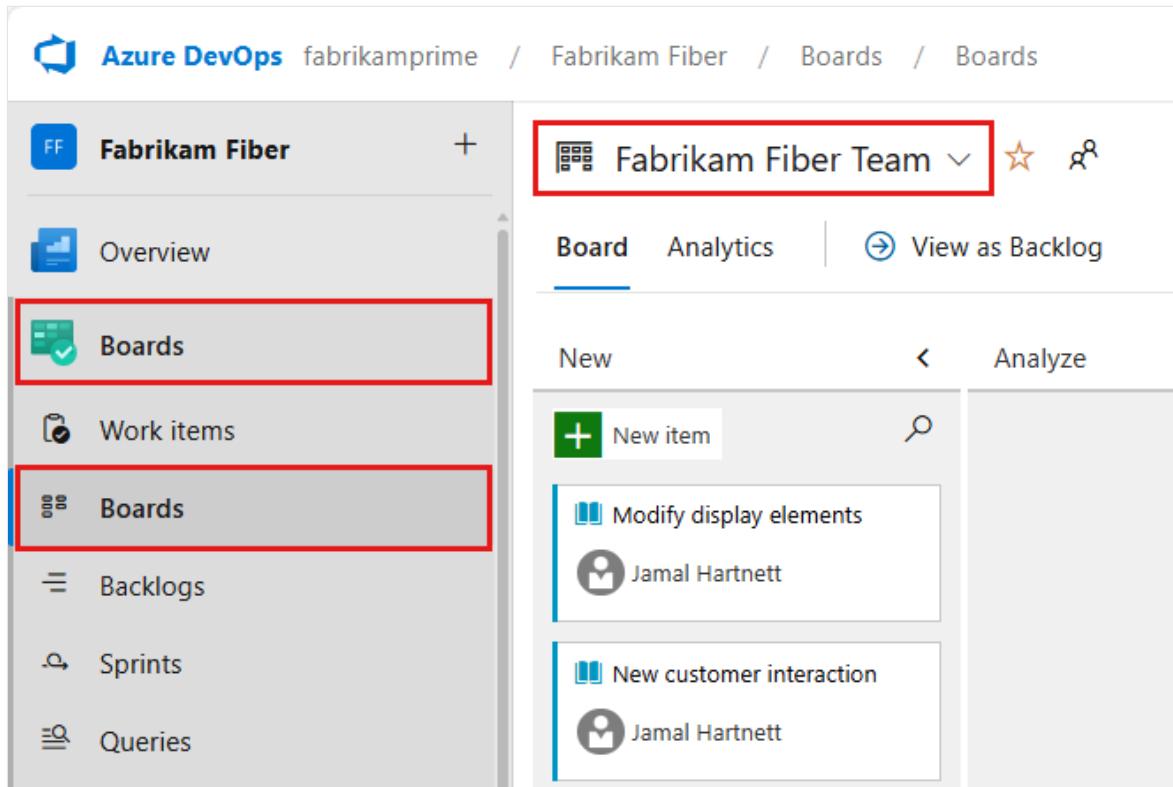
- User Stories and tasks are used to track work.
- Bugs track code defects.
- Epics and features are used to group work under larger scenarios.

Each team can configure how they manage Bug work items at the same level as User Story or Task work items. Use the [Working with bugs](#) setting. For more information about using these work item types, see [Agile process](#).

# Open your board

After you connect to a project, you can view work items.

1. In your project, select **Boards > Boards**. From the dropdown menu, select a team board.



You can also enter a keyword in the search box or select **View Board directory** to see a list of available team boards.

Fabrikam Fiber Team

Search team boards

My Team Boards

- Fabrikam Fiber Team
- New team

All Team Boards

- Fabrikam Fiber Team
- New area
- New team
- Phone

**View Board directory**

**Tip**

Select the star icon to make a team board a favorite. Favorite artifacts ( favorite icon) appear at the top of the team selector list.

2. Ensure that for the backlog level, you select:

- Stories for Agile.
- Issues for Basic.
- Backlog items for Scrum.
- Requirements for CMMI.

Fabrikam Fiber Team

+ New Work Item    Backlog items Board    ...

**Backlog items**

Filter    Settings    Refresh

## Add work items

From your board, select the plus sign, enter a title, and then select **Enter**.

The screenshot shows the Microsoft Azure DevOps Board view for the 'Fabrikam Fiber Team'. The board has columns for 'New', 'Active', 'Resolved', and 'Closed'. In the 'New' column, there is a card for 'Hello World' with the status 'User Story'. A red box highlights the '+ New item' button. Below the cards, there is a search bar and a section for 'Elements'. The 'Hello World' card is currently selected, and a blue box highlights the 'Add to top' button.

For more information, see [View and add work items](#).

## Update work items

Your work item forms might differ from the following images, but the functionality is the same.

### Change status

Drag a work item downstream as you finish work.

The screenshot shows the Microsoft Azure DevOps Board view with four columns: Backlog, Analyze, Develop, and Test. A red arrow points from the 'Resume' work item in the 'Analyze' column to the 'Show response on welcome page' work item in the 'Develop' column, indicating it is being moved downstream.

## Add details

To open a work item, double-click the title or highlight it, and then select **Enter**. This example shows how to assign work. You can only assign work to a user who was added to the project.

The screenshot shows a work item details page. At the top, there is a tab for 'Agile process'. Below the tabs, there is a note: 'This example assigns the story to Raisa Pokrovskaya and at-mentions Raisa in a discussion note. When you're finished, select Save & Close.'

The screenshot shows the 'USER STORY 1\*' work item in Azure Boards. At the top, there's a header with the title, a save button ('Save & Close'), and other navigation links. Below the header, there are sections for 'State' (New), 'Reason' (New), 'Area' (Fabrikam Fiber), and 'Iteration' (Fabrikam Fiber). A toolbar below these includes 'Details', 'Related Work items', and other icons. The 'Description' section contains the text: 'Switch initial view to the updated design.' The 'Planning' section shows 'Story Points' and 'Priority' (2). The 'Acceptance Criteria' section has a placeholder: 'Click to add Acceptance Criteria'. The 'Discussion' section shows a comment from '@Raisa Pokrovskaya': 'Can you make this happen in the next week?'. The 'Classification' section lists 'Value area' (Business) and 'Development'. The 'Related Work' section is also present.

To add more details, change field values, add a description or tags, and add comments. For more information, see:

- Plan and track work in [Azure Boards](#).
- Add tags to work items. As a Stakeholder, you can add existing tags to a work item, but you can't add new tags.
- Capture comments in the [Discussion section](#).

## View as backlog

Check the product backlog to see how the team prioritized their work. Backlog items appear in priority order. Work item types might include bugs, depending on the process used when your project was created. For more information, see [About default processes and process templates](#).

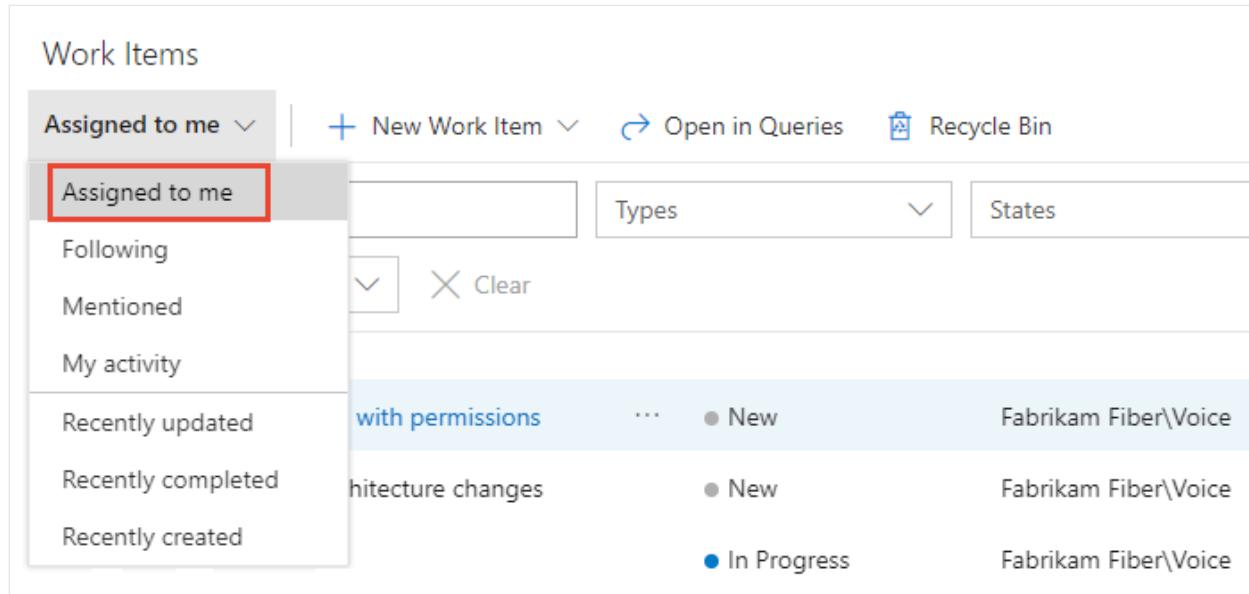
From the board, select **View as backlog**.

The screenshot shows the navigation bar of the Azure Boards interface. It includes links for 'Board', 'Analytics', 'View as Backlog' (which is highlighted with a red box), 'Stories', and other settings. The 'Fabrikam Fiber Team' is selected in the top left.

The list of backlog items appears in priority order. You can add a backlog item, which goes to the bottom of the list. With Stakeholder access, you can't reprioritize work.

## Find work items

Select **Boards > Work Items**. Then select an option from the dropdown menu. For example, select **Assigned to me**.



The screenshot shows the 'Work Items' page with the 'Assigned to me' dropdown menu open. The menu includes options like 'Following', 'Mentioned', 'My activity', 'Recently updated', 'Recently completed', and 'Recently created'. The 'Assigned to me' option is highlighted with a red box. The main area displays work items with columns for 'with permissions', '...', 'New', and 'States'. One item is listed under 'with permissions' with 'hitecture changes' and 'New' status, and another item is listed with 'In Progress' status.

For more information, see:

- [View, run, or email a work item query](#)
- [View and add work items](#)

## Next steps

[Create your product backlog](#)

## Related articles

- [Add work items](#)
- [Get started with Kanban boards](#)
- [Learn about access levels](#)
- [Change access levels](#)

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# View permissions for yourself or others

Article • 02/07/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

In this article, learn how to view your permissions or the permissions for other users in Azure DevOps. If you don't have permission to access a feature or function, you can request it from the right resource.

You can set and view permissions at the following three levels:

- [Project-level](#)
- [Organization or Collection-level](#)
- [Object-level](#)

For more information, see [Get started with permissions, access, and security groups](#).

## Prerequisites

[ ] [Expand table](#)

Category	Requirements
Project access	<a href="#">Project member</a> .
Permissions	Member of the <a href="#">Project Valid Users group</a> or <a href="#">Project Collection Valid Users group</a> .

## View project-level permissions

Do the following steps to view project-level permissions for you or other users.

### ! Note

To get the new user interface for the [Project Permissions Settings Page](#), [enable the preview feature](#).

[Preview page](#)

1. Sign in to your project  
([https://dev.azure.com/{Your\\_Organization}/{Your\\_Project}](https://dev.azure.com/{Your_Organization}/{Your_Project})).
2. Select **Project settings > Permissions**.

The screenshot shows the Azure DevOps interface for the project 'Fabrikam Fiber'. The left sidebar lists various project management features: Overview, Boards, Repos, Pipelines, Test Plans, Artifacts, Compliance, and Start Right. At the bottom of the sidebar, the 'Project settings' button is highlighted with a red box. The main content area is titled 'Project Settings' for 'Fabrikam Fiber'. It is organized into several sections: 'General' (Overview, Teams, Permissions - which is also highlighted with a red box), 'Boards' (Project configuration, Team configuration, GitHub connections), 'Pipelines' (Agent pools, Parallel jobs, Settings, Test management, Release retention, Service connections, XAML build services), 'Repos' (Repositories), and 'Artifacts'. A 'Project settings' button is located at the bottom right of the main content area.

## Project Settings

Fabrikam Fiber

### General

- Overview
- Teams
- Permissions**
- Notifications
- Service hooks
- Dashboards

### Boards

- Project configuration
- Team configuration
- GitHub connections

### Pipelines

- Agent pools
- Parallel jobs
- Settings
- Test management
- Release retention
- Service connections
- XAML build services

### Repos

- Repositories

### Artifacts

3. Select **Users**. To filter the list, enter a name into the *Search users* box.

## Permissions

The screenshot shows the 'Permissions' page in Azure DevOps. At the top, there are tabs for 'Groups' and 'Users', with 'Users' being the active tab and highlighted by a red box. A search bar at the top right contains the name 'Jamal'. Below the search bar, a list of users is displayed with columns for 'Name' and 'Email'. The user 'Jamal Hartnett' is highlighted with a larger callout bubble containing their profile picture, name, and email address. Other users listed include AB (Azure Boards), MS (MyPublicProject Build Service (fabrikam)), DS (Demo 11 Build Service (fabrikam)), Christie Church, Chuck Reinhart, and another Jamal Hartnett.

Name	Email
AB	Azure Boards
MS	MyPublicProject Build Service (fabrikam)
DS	Demo 11 Build Service (fabrikam)
Christie Church	fabrikamfiber1@hotmail.com
Chuck Reinhart	fabrikamfiber3@hotmail.com
Jamal Hartnett	fabrikamfiber4@hotmail.com

If your project administration is done using groups, **Expand search** after you begin to enter the user name.

4. Choose the user you want. The project-level permissions for that user display. These permissions are based on the groups the user belongs to or the permissions set specifically for the user's account.

Permission	Setting
Delete team project	Not set
Edit project-level information	Not set
Manage project properties	Not set
Rename team project	Not set
Suppress notifications for work item updates	Not set
Update project visibility	Not set
View project-level information	Allow (inherited)
Bypass rules on work item updates	Not set
Change process of team project.	Not set

5. Select **Member of** to see which security groups and teams that the user belongs to.

In the following example, *Jamal Hartnett* belongs to several teams and the Project Collection Administrators group for several projects.

Name	Scope
Web	[Fabrikam Git]
Fabrikam Team	[Fabrikam]

Tip

If there's an asterisk (\*) next to a 'Deny' permission, it indicates that the denial applies to all child objects or resources under the specified scope. This means that if a user is denied a permission at a higher level, they're also denied that permission for all related resources, regardless of any other permissions that might be granted at lower levels.

For example, if a user has 'Deny' permission for 'View project' with an asterisk (\*) at the project level, they can't view any of the repositories, boards, or pipelines within that project, even if they are granted 'Allow' permissions at those lower levels.

## View organization or collection-level permissions

Do the following steps to view organization or collection-level permissions for you or other users.

1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Select **Organization settings**.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber01' organization. On the left sidebar, under 'Organizations', 'FabrikamFiber01' is selected and highlighted with a blue background. Below it are other organizations: 'fabrikamfiber02' (purple) and 'fabrikamffiber' (pink). There are also links for '14 more organizations' and 'New organization'. The main content area is titled 'FabrikamFiber01' and shows a summary card for 'Fabrikam Fiber' with the letters 'FF' on it. At the bottom of the sidebar, there is a 'What's new' section featuring 'Sprint 162 release notes' which mention the return of the Sprint Burndown. A red box highlights the 'Organization settings' link at the bottom of the sidebar.

3. Select Permissions > Project Collection Administrators > Members.

Name	Type	Username or scope
Christie Church fabrikamfiber1@hotmail.com	user	fabrikamfiber1@hotmail.com
PA Project Collection Service Accounts	group	[mseng]
Jamal Hartnett fabrikamfiber4@hotmail.com	user	fabrikamfiber4@hotmail.com
Raisa Pokrovskaya fabrikamfiber5@hotmail.com	user	fabrikamfiber5@hotmail.com
Helena Petersen fabrikamfiber8@hotmail.com	user	fabrikamfiber8@hotmail.com

4. View the user's permissions and group membership. For more information, see the previous steps in [View project-level permissions](#).

## View object-level permissions

Do the following steps to view object-level permissions for you or other users.

1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Go to the object and open the Security dialog for the object. For specific instructions, see the following articles:

### Area

### Task

#### Wiki & dashboard permissions

- [README & wiki](#)
- [Dashboards](#)

#### Azure Repos, Azure Pipelines/DevOps (code, build, test, release) permissions

- [Git branch](#)
- [Git repository](#)
- [TFVC](#)
- [Builds](#)
- [Release pipeline security](#)
- [Approvals and approvers](#)

Azure Boards & work tracking permissions

- [Area and iteration paths](#)
- [Work item query and folder](#)
- Plan permissions

## Next steps

[Look up a member of the Project Administrators group](#)

## Related articles

- [Troubleshoot permissions](#)
- [Look up permissions and roles](#)

 **Note:** The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

# Sign up for Azure DevOps

Article • 03/13/2025

## Azure DevOps Services

Sign up for Azure DevOps and get the [free tier of services](#). For more information, see [What is Azure DevOps?](#)

## Prerequisites

[+] [Expand table](#)

Category	Requirements
Browser	Latest version of one of the following web browsers: Microsoft Edge, Internet Explorer, Safari (Mac), Firefox, or Chrome.

## Sign up

Sign up for Azure DevOps with either a Microsoft account or GitHub account.

Microsoft account

### Sign up with a personal Microsoft account

1. If you don't have one, [create a Microsoft account](#).
2. Go to [Azure DevOps](#) and select **Get started with Azure**.
3. Select either **Try Azure for free** or **Pay as you go**.
4. Enter your Microsoft account credentials and go through the sign-up process.

Azure DevOps creates an organization:

- If you signed up with a newly created Microsoft account, Azure DevOps creates a project named after your account.
- If you signed up with an existing Microsoft account, [create a project](#) next.

Sign in to your organization at any time:

[https://dev.azure.com/{Your\\_Organization}](https://dev.azure.com/{Your_Organization}).

## Next steps

[Create a project](#)

## Related articles

- Plan your organizational structure in Azure DevOps
- Change the location of your organization
- Add users to your organization
- Add users or groups to a team or project
- Connect to GitHub, FAQs

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Create an organization

Article • 02/06/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Use an organization to connect groups of related projects and help scale up your enterprise. You can use a personal Microsoft account, GitHub account, or a work or school account. Using your work or school account *automatically connects* your organization to your Microsoft Entra ID.

## ⓘ Note

All organizations must be manually created via the web portal. Automated creation of organizations is not supported. However, we do support automated organization configuration, project creation, and resource provisioning via the [REST API](#).

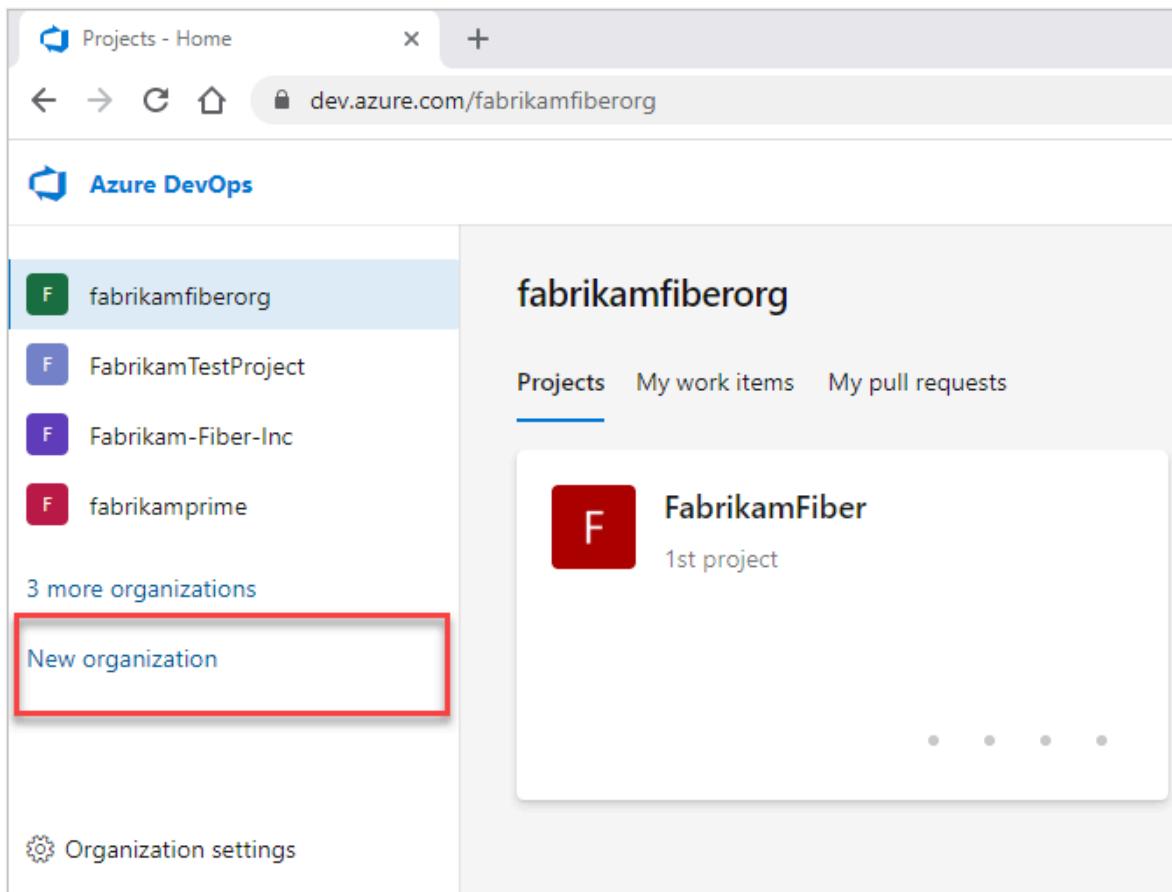
## Prerequisites

expand Expand table

Category	Requirements
Authentication	Determine whether you want to use only Microsoft accounts or authenticate users with Microsoft Entra ID. For more information, see <a href="#">Choosing your organization administrator account type</a> .
Planning	Understand how to <a href="#">plan your organizational structure</a> .

## Create an organization

1. Sign in to [Azure DevOps](#).
2. Select **New organization**.



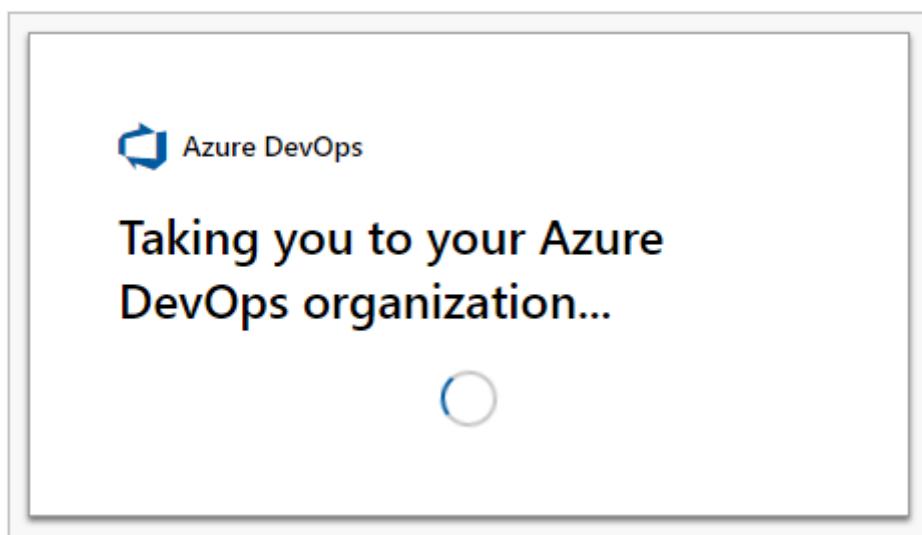
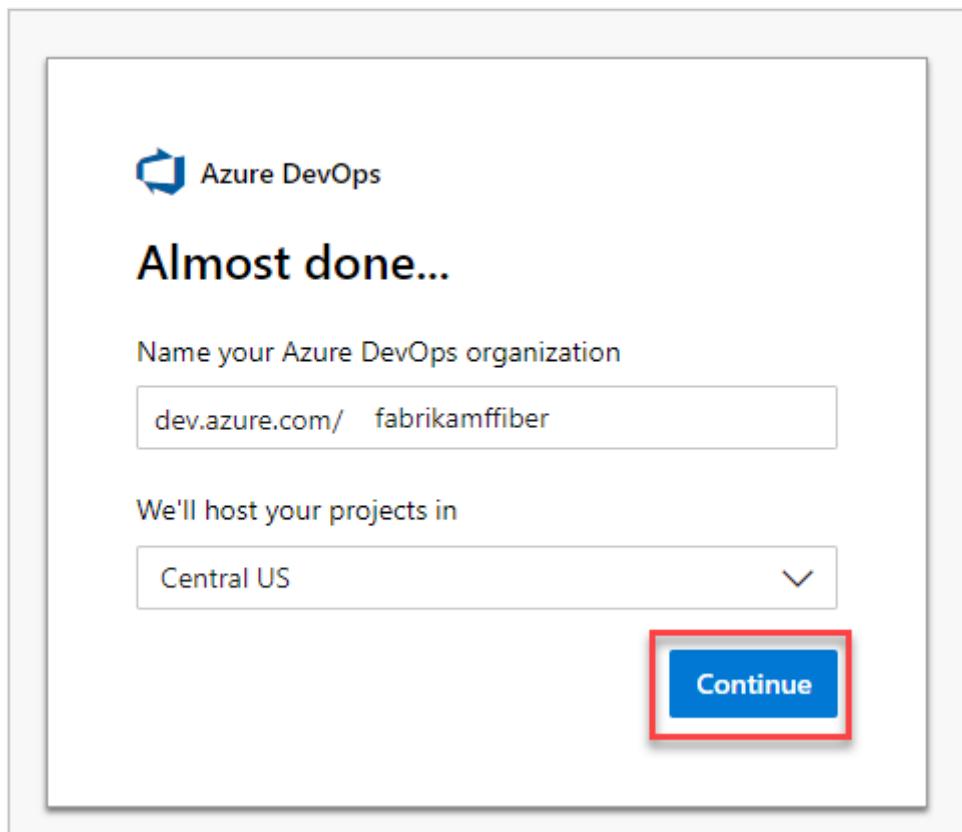
3. Enter the name for your organization, select its hosting geography, and then select **Continue**.

#### *(i)* Important

Adhere to the following guidelines when you create an organization name.

- Use only letters from the English alphabet
- Start your organization name with a letter or number
- Use letters, numbers, or hyphens after the initial character
- Ensure that your organization doesn't exceed 50 Unicode characters
- End with a letter or number

If you use any of the disallowed characters, you get the following error message: VS850015: The specified name is not allowed to be used: {Organization name}.



Congratulations, you're an organization owner!

Sign in to your organization at any time, <https://dev.azure.com/{yourorganization}>.

With your organization, the following aspects are included in the free tier:

- First five users free (Basic license)
- **Azure Pipelines:**
  - One Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month)
  - One self-hosted CI/CD concurrent job
- **Azure Boards:** Work item tracking and boards
- **Azure Repos:** Unlimited private Git repos
- **Azure Artifacts:** Two GiB free per organization

# Next steps

[Create a project](#)

## Related articles

- [Get started with Azure Repos and Visual Studio](#)
- [Rename an organization](#)
- [Change organization time-zone](#)
- [Change organization owner](#)
- [Delete an organization](#)
- [Resolve orphaned organization](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Get started managing your project

Article • 05/02/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

With most Azure DevOps Services, you can start using the service and configure resources as you go. No up-front work is required. Most settings define defaults.

If you created a project or you're added to the **Project Administrators** group, get familiar with the administrative tasks you're charged with. There are a few tasks you might want to do to ensure a smooth operational experience.

## Prerequisites

[ ] [Expand table](#)

Category	Requirements
Permissions	Member of the <b>Project Administrators</b> security group.

### ! Note

This article provides an overview of tasks a member of the **Project Administrators** group should review and attend to. For information on tasks to be performed by members of the **Project Collection Administrators** group, see [Manage your organization or project collection](#).

## Add users to your project

You add users to a team or project so they can contribute to the team and project. Users can be added to multiple teams and projects.

Users who are added to an organization, can easily be added to a project by adding them to a team or inviting them to contribute to a project.

Team administrators can add users to their team, which automatically adds them to the project. By adding users to a team, the users become visible to team-specific tools like the team security group, Team Members widget, and sprint capacity planning tools. To learn more about teams, see [About teams and Agile tools](#).

Members of the **Project Administrators** group can add users to a project. Adding users to a team or project automatically adds them to the project's **Contributors** group. Members of this group have permissions to most features needed to contribute to work items, code, builds, and releases. For an overview of default permissions, see [Default permissions quick reference](#).

After users are added to a project or organization, you can browse for their display name or user name (email alias) from any people-picker tool. Users can connect to a project and access features available through a supported client or the web portal.

For more information, see the following articles:

- [Add users or groups to a team or project](#)
- [Manage your organization or project collection, Add users to your organization](#)
- [Connect to a project](#)

## Share your project vision, set up a project wiki

Each project has a summary page that's useful for sharing information through **README** files. You can also redirect users to a project Wiki. For users who are new to your project, a good approach is to [set up your project summary page](#) or [prepare a Wiki](#). Use these features to share established processes and procedures for your project.

## Remove unused services

To simplify the web portal user interface, you can disable specific services. Suppose you use a project only to log bugs. In this scenario, you might disable all services except for **Boards**. For more information, see [Turn a service on or off](#).

The following example shows the **Test Plans** service disabled:

## Project Settings > Overview

### General

#### Overview

Teams

Security

Notifications

Service hooks

Dashboards

### Boards

Project configuration

Team configuration

GitHub connections

## Azure DevOps services



### Boards

Flexible agile planning with boards and cross-product issues

On



### Repos

Repos, pull requests, advanced file management and more

On



### Pipelines

Build, manage, and scale your deployments to the cloud

On



### Artifacts

Continuous delivery with artifact feeds containing NuGet, npm, Maven, Universal, and Python packages

On



### Test Plans

Structured manual testing at any scale for teams of all sizes

Off

# Manage security and permissions

Permissions and security groups control access to specific tasks. To quickly understand the defaults configured for your project, see [Default permissions and access](#).

The following table lists the permissions assigned at the project-level. All these permissions are granted to members of the **Project Administrators** group, except for the **Delete shared Analytics views** and **Edit shared Analytics views** permissions. For a description of each permission, see [Permissions and groups reference, Groups](#).

### ! Note

Permissions associated with Analytics require that the Inherited process model is selected for an on-premises project collection.

## General

- Delete team project
- Edit project-level information
- Manage project properties
- Rename team project
- Suppress notifications for work item updates
- Update project visibility

- View project-level information

## Boards

- Bypass rules on work item updates
- Change process of team project
- Create tag definition
- Delete and restore work items
- Move work items out of this project
- Permanently delete work items

## Analytics

- Delete shared Analytics views
- Edit shared Analytics views
- View analytics

## Test Plans

- Create test runs
- Delete test runs
- Manage test configurations
- Manage test environments
- View test runs

For more information about security and setting permissions at the project-level, review the following articles:

- [Get started with permissions, access, and security groups](#)
- [Change permissions at the project-level](#)

## Add members to the Project Administrators group

The person who creates a project is automatically added as a member to the **Project Administrators** group. Members of this group have permissions to manage project configuration, repositories, pipeline resources, teams, and all project-level permissions.

It's a good practice to assign administrative privileges to more than one team member. You can add a user to this group by following the instructions in [Change permissions at the project level, Add members to the Project Administrators group](#).

## Grant or restrict permissions

Permissions are managed at the following three levels and through role-based assignments:

- object

- project
- organization or collection

As a member of the **Project Administrators** group, you can grant or restrict permissions for all objects at the project-level. To delegate specific tasks to others, a good approach is to add the users to a built-in or custom security group, or add them to a specific role. For more information, see the following articles:

- [Use role-based permissions](#)
- [Add/remove users or groups, manage security groups](#)
- [Manage access to specific features and functions](#)
- [Set object-level permissions](#)

## Review and update notifications

Several notifications are predefined for each project you add. Notifications are based on subscription rules. Subscriptions arise from the following areas:

- [Out-of-the-box or default subscriptions.](#)
- [Team, project, and organization or collection subscriptions](#) defined by a team administrator or member of the **Project Administrators** or **Project Collection Administrators** groups.

If users report receiving too many notifications, you can direct them to [opt out of a subscription](#).

Notifications > Mine		<a href="#">New subscription</a>	<a href="#">Help</a>
Description	Type	Notifies	State
<b>Build</b>			
 Build completes Notifies you when a build you queued or that was queued for you compl...	Build completed (any project)	 You	<input checked="" type="checkbox"/> On
<b>Code (Git)</b>			
 Pull request reviewers added or removed Notifies you when you are added to a pull request or when a user is add...	Pull request (any project)	 You	<input checked="" type="checkbox"/> On
 Pull request completion failures Notifies you when a pull request you created fails to complete	Pull request (any project)	 You	<input checked="" type="checkbox"/> On
 Pull request changes Notifies you when changes are made to a pull request you created or are...	Pull request (any project)	 You	<input checked="" type="checkbox"/> On
 A comment is left on a pull request Notifies you about comments made to a pull request you created or a di...	Pull request comment (any project)	 You	<input checked="" type="checkbox"/> On

## Determine traceability requirements

If you use most Azure DevOps Services, such as Azure Boards, Azure Repos, Azure Pipelines, and Azure Test Plans, you probably want to alert your teams to the features that support end-to-end traceability. You can get started by reviewing the following articles:

- [Cross-service integration and collaboration overview](#)
- [End-to-end traceability](#)

## Set DevOps policies

Set policies to support collaboration across your teams and automatically remove obsolete files. To set policies that govern Azure Repos, Azure Pipelines, and Azure Test Plans, review the following articles:

- [Manage branch policies](#)
- [Add Team Foundation Version Control \(TFVC\) check-in policies](#)
- [Set build and release pipeline retention policies](#)
- [Set test retention policies](#)

## Configure and customize Azure Boards

You can configure and customize Azure Boards to support many business requirements for planning and tracking work. At a minimum, you should configure the following elements:

- **Area paths** to group work items by team, product, or feature area
- **Iteration paths** to group work into sprints, milestones, or other event-specific or time-related periods

If you're new to Azure Boards and want an in-depth overview of what you can configure and customize, see [Configure and customize Azure Boards](#).

## Define area and iteration paths for tracking work

If you support several products, you can assign work items according to feature area by defining [area paths](#). To assign work items to specific time intervals, also known as *sprints*, you configure [iteration paths](#). To use the Scrum tools like sprint backlogs, taskboards, and team capacity, you need to configure several sprints. For an overview, see [About areas and iteration paths](#).

The following image shows default iteration paths for Scrum processes:

The screenshot shows the 'Iterations' tab selected in the 'Areas' section of the Project Settings. A red box highlights the 'Iterations' tab. The main content area displays information about iterations for the project, including a table showing releases, sprints, start dates, and end dates.

This project is currently using the Agile process. To customize your work item types, go to the process customization page.

Create and manage the iterations for this project. These iterations will be used by teams for iteration planning (sprint planning). Learn more about customizing areas and iterations ↗

To select iterations for the team, go to the default team's settings.

Iterations	Start Date	End Date
Release 1		
Sprint 1	1/6/2020	1/10/2020
Sprint 2	1/13/2020	1/17/2020
Sprint 3	1/20/2020	1/24/2020
Release 2		

The following image shows a set of sample area paths:

The screenshot shows the 'Areas' tab selected in the 'Areas' section of the Project Settings. A red box highlights the 'Areas' tab. The main content area displays information about areas for the project, including a table showing areas and their corresponding teams.

This project is currently using the Agile process. To customize your work item types, go to the process customization page.

Create and manage the areas for this project. These areas will be used by teams to determine what shows up on the team's backlog and what work items the team is responsible for. Learn more about customizing areas and iterations ↗

To select areas for the team, go to the default team's settings.

Areas	Teams
Customer Service	Customer Service
Phone	
Voice	
Web	...

## Customize work-tracking processes

You and your team can start using all work-tracking tools immediately after you create a project. But often, some users want to customize the experience to meet various business needs. You can customize the process easily through the user interface. It's a good practice to establish a methodology for which users can manage the updates and evaluate requests.

### Note

By default, organization owners and users added to the **Project Collection Administrators** security group are granted permission to create, edit, and manage processes used to customize the work-tracking experience. If you want to lock down who is able to perform these tasks, you can set permissions at the organization-level to **Deny**.

For more information, see the following articles:

- [About process customization and inherited processes](#)
- [Customize a project](#)
- [Add and manage processes](#)

## Integrate with other services

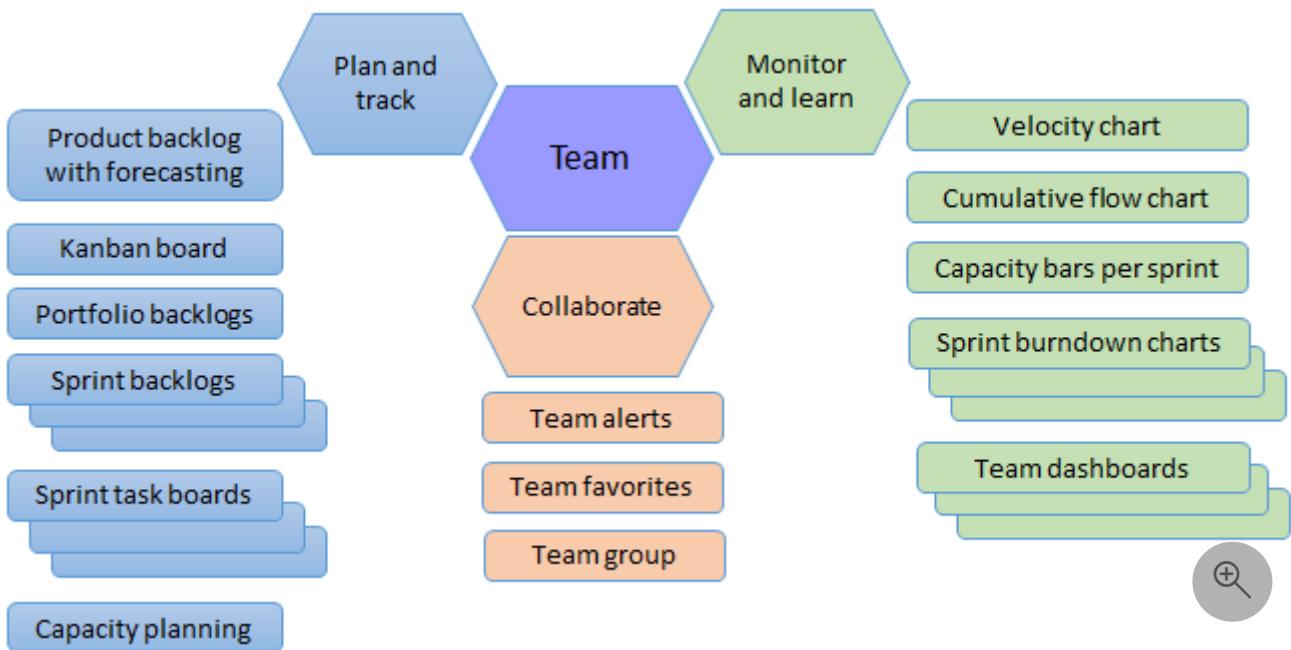
Azure DevOps supports integration with Azure, GitHub, and many other services. As a member of the **Project Administrators** group, you can configure integration with many of these services. For more information, see the following articles.

 [Expand table](#)

Service integration	Resources
Azure DevOps and GitHub	<a href="#">Azure DevOps and GitHub integration overview</a>
Azure Boards and GitHub	<a href="#">Azure Boards and GitHub integration</a>
Microsoft Teams	<ul style="list-style-type: none"><li>- <a href="#">Azure Boards with Microsoft Teams</a></li><li>- <a href="#">Azure Repos with Microsoft Teams</a></li><li>- <a href="#">Azure Pipelines with Microsoft Teams</a></li></ul>
Slack	<ul style="list-style-type: none"><li>- <a href="#">Azure Boards with Slack</a></li><li>- <a href="#">Azure Repos with Slack</a></li><li>- <a href="#">Azure Pipelines with Slack</a></li></ul>
Azure DevOps service hooks	<a href="#">Integrate with service hooks</a>

## Add teams and scale your project

As your organization grows, it's a good practice to add teams to scale your project. Each team gets [access to their own set of customizable Agile tools](#).



For more information, see the following articles:

- [About projects and scaling your organization](#)
- [Add a team, move from one default team to several teams](#)
- [Add a team administrator](#)

## Related content

- [View and update project summary page](#)
- [Get started managing your organization or project collection](#)
- [About user, team, project, and organization-level settings](#)

# Manage your organization or collection

Article • 02/05/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

After you create an organization or project collection, add contributors and configure policies, settings, and other options available to you. This article provides an overview of tasks to ensure you set up your organization or collection to get maximal use of your services.

Each organization is associated with one and only one collection. If you need to create another organization, see [Plan your organizational structure](#) and [Create an organization](#).

## Prerequisites

[+] Expand table

Category	Requirements
Permissions	Member of the <a href="#">Project Collection Administrators group</a> . Organization owners are automatically members of this group.

### ⓘ Note

This article provides an overview of tasks that require membership in the **Project Collection Administrators** group. For information on tasks performed by members of a **Project Administrators** group, see [Manage your project](#).

## Add users to your organization

For large enterprises, connect Azure DevOps to Microsoft Entra ID and use its security groups to control user access. This way, you can sync users and groups between Microsoft Entra ID and Azure DevOps, and reduce the overhead of managing permissions and user access.

You can add users and security groups to your organization through the web portal **Organization settings > Users** interface, regardless of the size of your enterprise. You can also assign these users and groups to one or more projects within your organization.

When you add users, you specify their *access level*, which determines the features they can use through the web portal. For more information, review these resources:

- Get started with permissions, access, and security groups
- About access levels
- Add organization users and manage access
- Connect your organization to Microsoft Entra ID

ⓘ Note

If the **Limit user visibility and collaboration to specific projects** preview feature is turned on the organization, users added to the **Project-Scoped Users** group can't access projects that they aren't added to. For more information including important security-related call-outs, see [Limit user visibility for projects and more](#), later in this article.

## Set up billing

Azure DevOps charges for the following services as described in [Pricing for Azure DevOps](#).

- Individual services:
  - Microsoft-hosted CI/CD parallel jobs
  - Self-hosted CI/CD parallel jobs
  - Storage of Azure Artifacts feeds
- User licenses for **Basic** or **Basic + Test Plans**.

All organizations are granted five free **Basic** licenses and unlimited users with **Stakeholder** access. For information on each access level, see [About access levels](#).

If your organization requires more than five contributors, then you need to set up billing. Users that have a Visual Studio subscription can be added without incurring any further billing charges. Billing is based on the access level, **Basic** or **Basic + Test Plans**, that you assign to the user. For more information, see [Set up billing](#).

## Manage security and permissions

Permissions and security groups control access to specific tasks.

The following table lists the permissions assigned at the organization or collection level. All permissions, except for **Make requests on behalf of others**, are granted to members

of the **Project Collection Administrators** group. For more information, see [Permissions and groups reference, Groups](#).

## General

- Alter trace settings
- Create new projects
- Delete team project
- Edit instance-level information
- View instance-level information

## Service Account

- Make requests on behalf of others
- Trigger events
- View system synchronization information

## Boards

- Administer process permissions
- Create process
- Delete field from organization or account
- Delete process
- Edit process

## Repos (TFVC)

- Administer shelved changes
- Administer workspaces
- Create a workspace

## Pipelines

- Administer build resource permissions
- Manage build resources
- Manage pipeline policies
- Use build resources
- View build resources

## Test Plans

- Manage test controllers

## Auditing

- Delete audit streams
- Manage audit streams
- View audit log

## Policies

- Manage enterprise policies

For more information about security and setting permissions at the collection-level, review the following articles:

- [Get started with permissions, access, and security groups](#)
- [Change permissions at the organization or collection-level.](#)

## Add members to the Project Collection Administrators group

When you create an organization, you become a member of the **Project Collection Administrators** group. This group has the authority to manage the organization's settings, policies, and processes. It can also create and manage all the projects and extensions in the organization.

It's always a good idea to have more than one person who has administrative privileges. Look up a [Project Collection Administrator](#) and then ask them to add you to the group.

## Set security policies

Configure the security policies for your organization through the [Organization settings](#) > **Policies** page. These policies let you grant or restrict the following features:

- Non-microsoft application access via OAuth
- SSH authentication
- Creation of public projects
- Invitation of GitHub user accounts

## Policies

### Application connection policies

On    Third-party application access via OAuth [🔗](#)

On    SSH authentication [🔗](#)

### Security policies

On    Log Audit Events [🔗](#)

Off    Allow public projects [🔗](#)

On    Enterprise access to projects

On    Additional protections when using public package registries [🔗](#)

Off    Enable IP Conditional Access policy validation on non-interactive flows [🔗](#)

### User policies

On    External guest access [🔗](#)

On    Allow team and project administrators to invite new users [🔗](#)

On    Request access [🔗](#)    [Edit Url](#)

For more information, see [Change application connection & security policies for your organization](#).

## Limit user visibility

### ⚠️ Warning

Consider the following limitations when using this preview feature:

- The limited visibility features described in this section apply only to interactions through the web portal. With the REST APIs or `azure devops` CLI commands, project members can access the restricted data.

- Users in the limited group can only select users who are explicitly added to Azure DevOps and not users who have access through Microsoft Entra group membership.
- Guest users who are members in the limited group with default access in Microsoft Entra ID, can't search for users with the people picker.

## Organizations and projects

By default, users added to an organization can view all organization and project information and settings. You can restrict specific users, such as Stakeholders, Microsoft Entra users, or member sof a particular security group, with the **Limit user visibility and collaboration to specific projects** preview feature for the organization. Once the feature [gets turned on](#), any user or group that [gets added to the Project-Scope Users group](#) is restricted in the following ways:

- Access is confined to only the projects to which they're explicitly added.
- Views displaying lists of users, projects, billing details, usage data, and more accessed through **Organization settings** are restricted.
- The set of people or groups that appear in people-picker search selections and the ability to **@mention** people is limited.

## Identity search and selection

With Microsoft Entra ID, you can use people pickers to search for any user or group in your organization, not just the ones in your current project. People pickers support the following Azure DevOps functions:

- Selection of a user identity from a work tracking identity field such as **Assigned To**
- Selection of a user or group using **@mention** in a work item discussion or rich-text field, a pull request discussion, commit comments, or changeset or shelveset comments
- Selection of a user or group using **@mention** from a wiki page

As shown in the following image, start entering a user or security group name into a people picker box until you find a match.

The screenshot shows a search interface for users and groups. A search bar at the top contains the text '@C'. Below it, two user results are displayed: 'Christie Church' (fabrikamfiber1@hotmail.com) and 'Chuck Reinhart' (fabrikamfiber3@hotmail.com). Each result has a small circular profile picture and a 'Select' button to the right. Below the results is a search bar with the placeholder 'Search' and a note 'Showing 2 results'.

Users and groups who get [added to the Project-Scope Users group](#) can only see and select users and groups in the project they're connected to from a people picker.

## Turn on the preview feature and add users to the security group

Do the following steps to turn on the preview feature and add users and group to the Project-Scope Users group:

1. Turn on the [Limit user visibility and collaboration to specific projects](#) [preview feature](#) for the organization.
2. Add the users to your project as described in [Add users to a project or team](#). Users added to a team are automatically added to the project and team group.
3. Open [Organizations settings > Security > Permissions](#) and choose **Project-Scope Users**. Select the **Members** tab.
4. Add all users and groups that you want to scope to the project they're added to. For more information, see [Set permissions at the project- or collection-level](#).

The **Project-Scope Users** group only appears under the **Permissions > Groups** when the [Limit user visibility and collaboration to specific projects](#) preview feature is turned on.

All security groups in Azure DevOps are considered organization-level entities, even if they only have permissions for a specific project. This means that security groups get managed at the organization level.

From the web portal, the visibility of some security groups might be restricted based on the user's permissions. However, you can still discover the names of all security groups within an organization by using the `azure devops` CLI tool or the REST APIs. For more information, see [Add and manage security groups](#).

# Manage extensions

An extension is an installable unit that adds new capabilities to your projects. Azure DevOps extensions support the following functions:

- Planning and tracking of work items, sprints, scrums, and so on
- Build and release flows
- Code testing and tracking
- Collaboration among team members

For example, to support [code search](#), install the [Code Search extension](#).

You want to tell your users about extensions and that they can [request an extension](#). To install and manage extensions, be an organization Owner, a member of the [Project Collection Administrators](#) group. Or, you can get added to the [Manager role for extensions](#).

## Install Code Search

Code Search is a free Marketplace extension that lets you search across all your source repositories. For more information, see [Install and configure Search](#).

## Adjust time zone and other organization settings

When you create an organization, you specify the name of your organization and select the region where your organization is hosted. The default **Time zone** is set to *UTC*. You can update the **Time zone** and specify a Privacy URL from the [Organization settings](#)>[Overview](#) page. For more information about these settings, see the following articles:

- [Time zone settings and usage](#)
- [Add a privacy policy URL for your organization](#)

## Configure DevOps settings

Use the following settings, which get defined at the organization-level, to support your work.

- [Add agent pools](#)
- [Define pipeline retention settings](#)

- Define repository settings:
  - [Default branch name for new repositories](#)
  - [Gravatar images](#).

## Customize work-tracking processes

All work-tracking tools are available immediately after you create a project. Often, one or more users might want to customize the experience to meet one or more business needs. Processes are easily customized through the user interface. However, you might want to establish a methodology for who manages the updates and evaluates requests.

For more information, see the following articles:

- [About process customization and inherited processes](#)
- [Customize a project](#)
- [Add and manage processes](#)

## Alert users with information banners

Communicate with your Azure DevOps users quickly through information banners. Use banners to alert your Azure DevOps users to upcoming changes or events without sending mass emails. For more information, see [Add and manage information banners](#).

## Review and update notifications

Many notifications are predefined at the organization or collection level. You can [manage subscriptions or add new subscriptions](#).

## Scale your organization or collection

To learn about scaling your organization, see the following articles.

- [About projects and scaling your organization](#)
- [Plan your organizational structure](#)

## Related articles

- [About projects](#)
- [FAQs about signing up and getting started](#)
- [Organization management](#)

- About user, team, project, and organization-level settings
- 

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Add users or groups to a team or project

Article • 11/28/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

In this article, learn how to add users or groups to a team or project. For organizations with large user bases, we recommend you use Microsoft Entra ID to add and manage new users through security groups. However, to enable flexibility for all size organizations, Azure DevOps supports the following operations.

## Prerequisites

[ ] Expand table

Category	Requirements
Project access	Member of a <a href="#">project</a> .
Permissions	<ul style="list-style-type: none"><li>- To add users to or remove users from a team: <a href="#">Team Administrator</a> or member of one of the administrative groups.</li><li>- To add users to or remove users from a project: Member of the <a href="#">Project Administrators group</a>.</li><li>- To add users or manage users for an organization: Member of the <a href="#">Project Collection Administrators group</a>. Organization owners are automatically members of this group.</li></ul>
Policies	If your organization is connected to Microsoft Entra ID: Enable the <a href="#">Allow team and project administrators to invite new users</a> policy for team administrators or members of the Project Administrators group for adding new users.

**Recommended:** If you're new to Azure DevOps, familiarize yourself with the information in the following articles:

- [Get started with permissions, access levels, and security groups](#)
- [About projects and scaling your organization](#)
- [Default permissions and access quick reference](#)
- [About teams and Azure Boards tools](#)

## Supported options for adding users

Depending on your administrator level and interface, you can add new or existing users to teams or projects in the following ways.

## Administrator level

### Interface

### Supported tasks

Team administrators

#### [Team Members dashboard widget](#)

- Add new or existing users to a team.
- Send new users an invitation.

#### [Project settings > Teams > Team > Members](#)

Add existing users or groups to a team.

Project Administrators

#### [Project Summary page > Invite](#)

- Add new or existing users.
- Send new users an invite.
- Optionally add users to one or more teams.

#### [Project settings > Permissions > Groups > Group > Members](#)

- Add existing users or groups to a security group. By adding to a team group, you effectively add them to the team.
- Optionally remove a user from a group.

Project Collection Administrators

#### [Organization settings > Users](#)

- Add new users to an organization and send an invite. Must specify the access level.
- Optionally add users to select projects.
- Use [Group rules](#) to further manage groups.

#### [az devops user CLI](#)

Add new users to an organization and send an invite. Must specify the access level.

Microsoft Entra Administrators

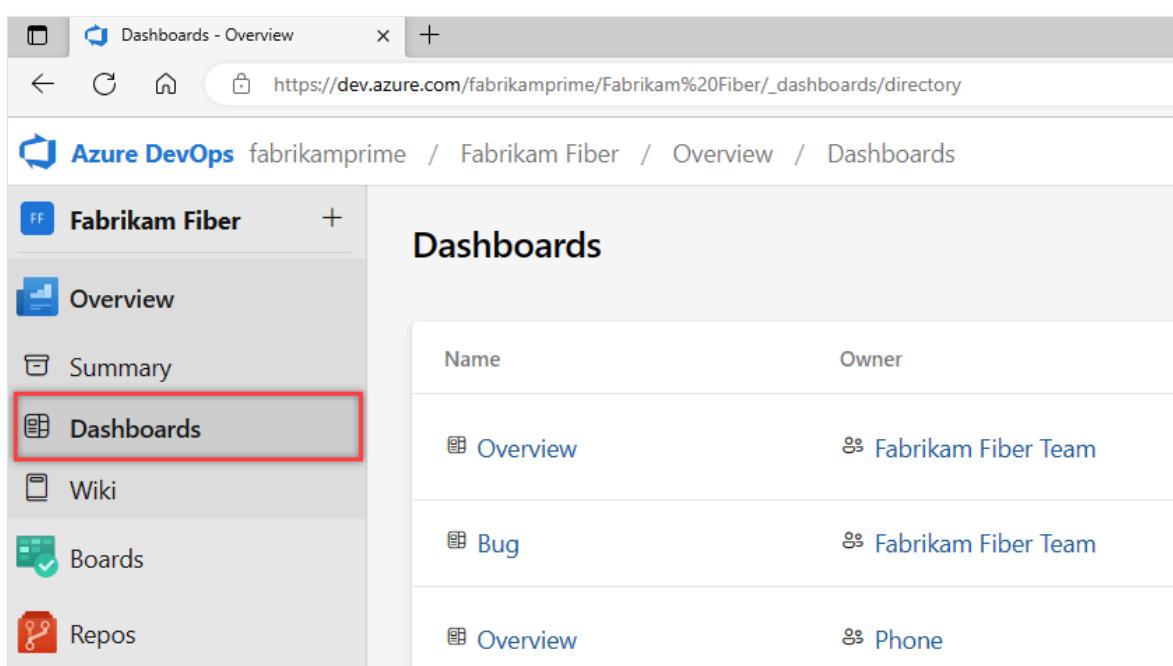
Microsoft Entra ID

Add users to Microsoft Entra, connected to Azure DevOps Services. These users get added to the Project Collection Valid Users group. For more information, see [Connect your organization to Microsoft Entra ID](#).

## Add a user from the Team Members widget

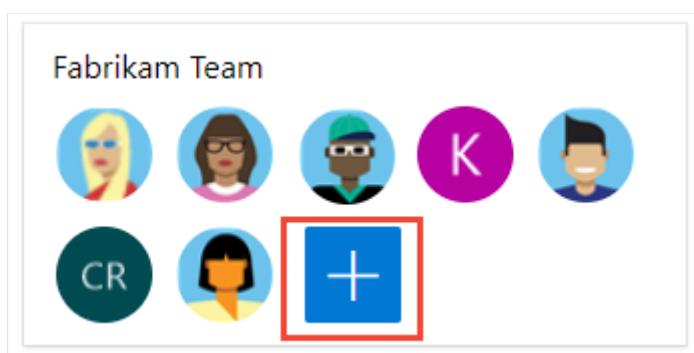
As a team administrator, you can add new or existing members from the **Team Members** dashboard widget. For more information, see [Add widgets to a dashboard](#).

1. Sign in to your project ([https://dev.azure.com/{Your\\_Organization}/Your\\_Project](https://dev.azure.com/{Your_Organization}/Your_Project)).
2. Select **Dashboards** and then choose your dashboard.



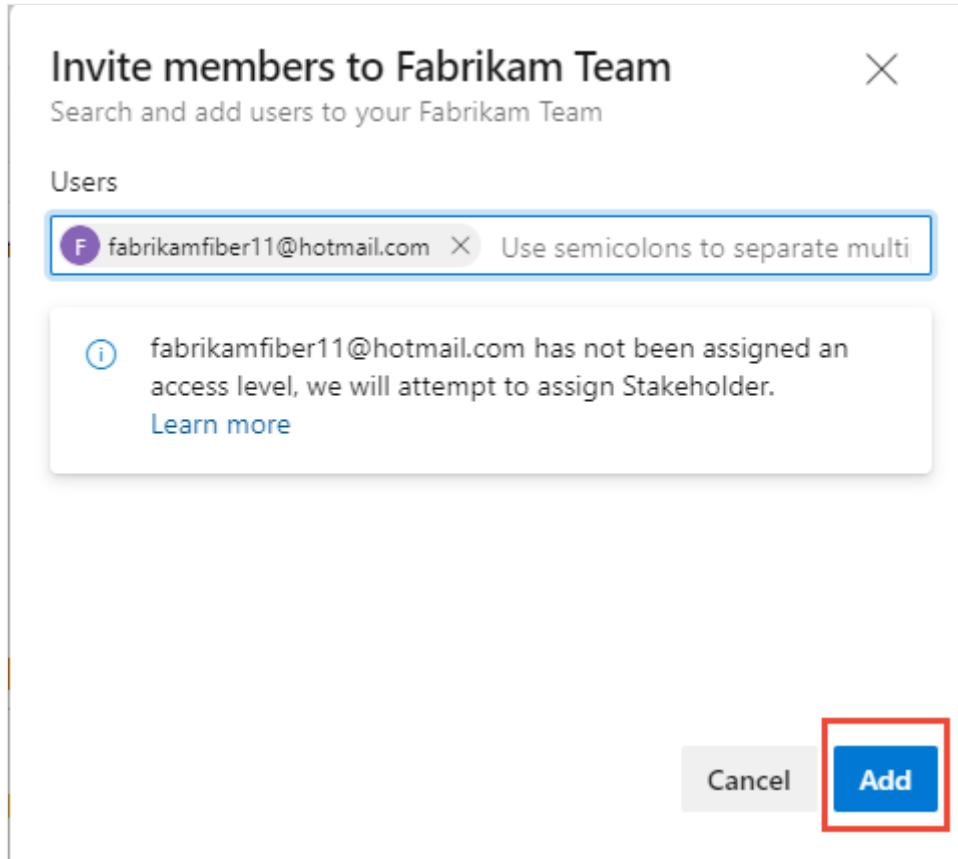
The screenshot shows the Azure DevOps Dashboards page for the 'Fabrikam Fiber' project. On the left, there's a sidebar with links: Overview, Summary, Dashboards (which is highlighted with a red box), Wiki, Boards, and Repos. The main area is titled 'Dashboards' and lists three dashboards: 'Overview' (owner: Fabrikam Fiber Team), 'Bug' (owner: Fabrikam Fiber Team), and another 'Overview' (owner: Phone). The URL in the browser is https://dev.azure.com/fabrikamprime/Fabrikam%20Fiber/\_dashboards/directory.

3. Select  **Manage team members** on the Team Members widget.



4. Enter email addresses for new users. For existing users, enter their name until it resolves as a known name to the system. Separate multiple entries with a semicolon (;). Select **Add**.

When the user's unknown, a notification advises that an access level must be assigned. To complete the invitation, select **Add**.



When you add a new user, the system assigns Stakeholder as the access level when all free five Basic access levels are already assigned. Active contributors to a project need to have Basic access as a minimum. A Project Collection Administrator can change the access level and resend invitations from the [Organization Settings > Users page](#).

**!** Note

Users with limited access, such as Stakeholders, can't access select features even if granted permissions to those features. For more information, see [Permissions and access](#).

5. (Optional) A notification briefly displays to indicate success or failure. Select **Details** to open the notification and review details.

Success: Added 1 user to 2 teams  
and assigned an access level to 1 user.

[Details](#)

Failed: Added 1 user to 1 team and  
assigned an access level to 1 user.

[Details](#)

## Notifications



System issues are problems in the system that require admin attention. Session notifications are triggered by user activities in this session.

Session notifications 3

[Dismiss all](#)

Added 1 user to 1 team and assigned an access level to 1 user.

Just now

Less details

User

Message

Success 1

fabrikamfiber11@hotmail.com

"..."

## Notifications



System issues are problems in the system that require admin attention. Session notifications are triggered by user activities in this session.

### Session notifications 1

[Dismiss all](#)

Add 1 user

Just now

Less details

User

Message

Failed 1

fabrikamfiber11@hotmail.com

You are trying to invite a user from outside your directory, but the security setting of this organization doesn't allow it. [Learn more](#)

6. New users receive an email invitation to sign in to the project. Existing users don't receive a formal notification.

## Add users or groups to a team

Do the following steps to add existing users or security groups to a team. To add a custom security group, see [Manage security groups](#).

### Note

To enable the new user interface for managing teams, enable the [New Teams Page](#) from the [Preview features](#) tool. To learn how, see [Manage or enable features](#).

[Preview page](#)

1. Select **Boards > Boards > Show team profile > Team Settings**.

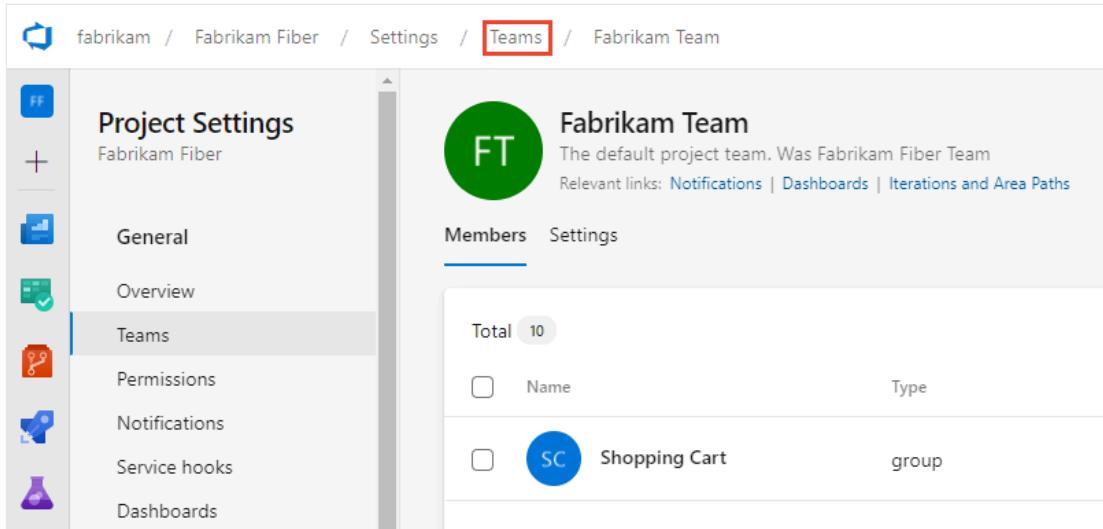
2. If you need to switch the team context, use the team selector within the breadcrumbs.

3. Select Add.

Total	Name	Type	Username or scope
9	Christie Church	user	fabrikamfiber1@hotmail.com
	Chuck Reinhart	user	fabrikamfiber3@hotmail.com
	Jamal Hartnett	user	fabrikamfiber4@hotmail.com

You can toggle between direct or expanded membership views. The **Direct Members** view displays users and groups added to the team. The **Expanded Members** view replaces any Azure DevOps groups with the members who belong to those groups. Microsoft Entra ID or Active Directory groups don't expand.

4. Enter the sign-in address or display name one at a time or all together, separated by commas. You can also add a project security group--such as another team group, custom group, or Microsoft Entra group if used by the organization.



The screenshot shows the 'Project Settings' page for 'Fabrikam Fiber'. The left sidebar has icons for General, Overview, Teams (which is selected), Permissions, Notifications, Service hooks, and Dashboards. The main area is titled 'Fabrikam Team' with a green circular icon containing 'FT'. It says 'The default project team. Was Fabrikam Fiber Team' and provides links for Notifications, Dashboards, and Iterations and Area Paths. Below this, there are tabs for 'Members' and 'Settings', with 'Members' being the active tab. It shows a total of 10 members. A table lists two members: 'Name' (checkbox) and 'SC Shopping Cart' (checkbox). The 'Type' column indicates 'group' for the second member.

Select  Refresh if you don't see your updates.

5. To [add an account as a Team administrator](#), go to the **Settings** page and select Add in the Administrators section.

### Tip

The total count display stops incrementing at 500, but you can still add more users.

[Members](#) [Settings](#)

Total 10

## Remove users or groups from a team

Do the following steps to remove a user or group from a team.

Preview UI

1. Select **Project settings > Teams > Members > Direct Members**. For the user to be removed, select  More options >**Remove**.

Fabrikam Fiber Team  
The default project team.  
Want links: [Notifications](#) | [Dashboards](#) | [Iterations and Area Paths](#)

Members Settings

Total 13

Name	Type
fabrikamfiber2@hotmail.com	user
fabrikamfiber3@hotmail.com	user
fabrikamfiber5@hotmail.com	user

Direct Members Add

⋮ Remove

### Tip

To remove a team administrator as a team member, you must first remove them as an administrator.

2. Select **Delete** to confirm.

### Delete Member

Are you sure you want to remove "fabrikamfiber11@hotmail.com" from the "Fabrikam Team" team?

Cancel

Delete

## Add users or groups to a project

As a member of the **Project Administrators** group, you can add users or groups to a project from the **Project settings > Permissions** page by adding them to a security group. To add a custom security group, see [Add or remove users or groups, manage security groups](#).

### Note

To enable the **Project Permissions Settings Page** preview page, see [Enable preview features](#).

1. Sign in to your project  
([https://dev.azure.com/{Your\\_Organization}/Your\\_Project](https://dev.azure.com/{Your_Organization}/Your_Project)).

2. Select **Project settings > Permissions**.

The screenshot shows the 'Permissions' page in Azure DevOps. On the left, under 'Project Settings' for the 'FabrikamFiber' project, the 'Permissions' link is highlighted with a red box. On the right, the 'Permissions' section displays two groups: 'Build Administrators' and 'Contributors'. The 'Build Administrators' group is currently selected.

Name	Description
BA	Build Administ... Member create, m... build def queued a...
C	Contributors Member add, mo... within th...

3. Under **Groups**, choose one of the following options:

- **Readers**: To add users who require read-only access to the project, choose.
- **Contributors**: To add users who contribute fully to this project or have Stakeholder access.
- **Project Administrators**: To add users who need to administrate the project. For more information, see [Change project-level permissions](#).

Or, you can choose any team group to add users to a specific team.

Here we choose the **Contributors** group.

## Permissions

Groups    Users

Name	Description
[Fabrikam Fiber]\Build Administrators	Members of this group can create, modify and delete build definitions and manage queued and completed builds.
C [Fabrikam Fiber]\Contributors	Members of this group can add, modify, and delete items within the team project.

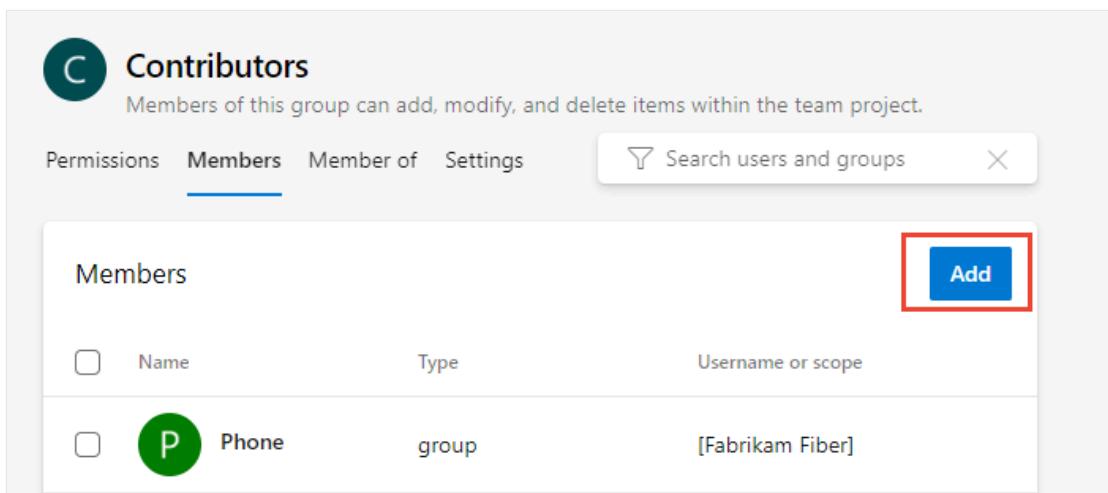
4. Next, choose the **Members** tab.

The default team group, and any other teams you add to the project, get included as members of the **Contributors** group. Add a new user as a member of a team instead, and the user automatically inherits Contributor permissions.

 **Tip**

Managing users is much easier [using groups](#), not individual users.

5. Choose **Add** to add a user or a user group.



The screenshot shows the 'Contributors' page. At the top, there's a heading 'Contributors' with a green circular icon containing a white letter 'C'. Below it, a sub-header says 'Members of this group can add, modify, and delete items within the team project.' There are four tabs: 'Permissions', 'Members' (which is selected and highlighted in blue), 'Member of', and 'Settings'. To the right of the tabs is a search bar with a magnifying glass icon and a close button ('X'). Below the tabs is a table with a header row: 'Members', 'Name', 'Type', and 'Username or scope'. Under the 'Members' column, there's a blue button labeled 'Add' with a red rectangular box drawn around it. In the table, there's one existing entry: a green circular icon with a white letter 'P', followed by 'Phone' in bold, 'group', and '[Fabrikam Fiber]'.

6. Enter the name of the user account into the text box. You can enter several identities into the text box, separated by commas. The system automatically searches for matches. Choose the match(es) that meets your requirements.

## Invite members to Contributors

X

Search and add users and/or groups to your group

Add users and/or groups



Ch



Christie Church

fabrikamfiber1@hotmail.com



Chuck Reinhart

fabrikamfiber3@hotmail.com



Cancel

Save

### ⚠ Note

The first time you add a user or group to Azure DevOps, you can't browse to it or check the friendly name. After the identity has been added, you can just enter the friendly name.

Choose **Save** when done.

7. You might customize user permissions for other functionality in the project.  
For example, in [areas and iterations](#) or [shared queries](#).

## Invite users from the Summary page

As a member of the Project Administrators group, you can add members to a project from the [Summary page](#) and optionally add them to one or more teams.

1. Open your **Project > Summary** page, and select **Invite**.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, there's a sidebar with options like Overview, Summary, Dashboards, Analytics views\*, Wiki, and Boards. The 'Summary' option is selected. At the top right, there are buttons for 'Private', 'Invite' (which is highlighted with a red box), and a star icon. Below the header, there's a section titled 'About this project' with a description: 'Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber.' It also lists 'Fabrikam Fiber / README.md' and 'minor modification to test development section in mobile form'. There are 'Like' and '0' buttons next to the description.

2. For new users, enter their email address. For existing users, enter their name until it resolves as a known name to the system. You can add several email addresses or account names by separating them with a semicolon (;).

Choose the entry listed under **Add users** to complete the entry.

If you're adding a user known by the organization or collection, enter the name or email address and then choose the name that appears to complete the entry.

This screenshot shows a modal dialog titled 'Invite members to Fabrikam Fiber'. It has a search bar at the top with the placeholder 'Search and add users to your Fabrikam Fiber'. Below it, there's a section labeled 'Users' containing a text input field with the email 'fabrikamfiber11@hotmail.com'. Underneath, there's a 'Add users' section with another input field containing the same email, which is also highlighted with a red box. At the bottom of the dialog are 'Cancel' and 'Add' buttons.

## Invite members to Fabrikam Fiber



Search and add users to your Fabrikam Fiber

Users

 fabrikamfiber9	Jia-hao Tseng fabrikamfiber9@hotmail.com	
--	---	---

[Cancel](#)

[Add](#)

### ⓘ Note

Any valid email address is acceptable. When the user accepts the invitation and signs into Azure DevOps, they register their email address as a Microsoft account and choose a password.

3. Optionally, select the teams you want to add the user to and then choose **Add** to complete the invitation.

When the user is unknown, a notification alerts that an access level must be assigned. To complete the invitation, choose **Add**.

Choose **Add** to complete the invitation.

## Invite members to Fabrikam Fiber

X

Search and add users to your Fabrikam Fiber

### Users



fabrikamfiber12@hotmail.com X

Use semicolons to separate multi

Add to team(s)

Fabrikam Team



- i fabrikamfiber12@hotmail.com has not been assigned an access level, we will attempt to assign Stakeholder.
- [Learn more](#)

Cancel

Add

**Invite members to Fabrikam Fiber** X

Search and add users to your Fabrikam Fiber

Users

Johnnie McLeod X +

Add to team(s)

Service Delivery (+3) ▼

Search

- Shopping Cart
- Service Delivery
- Service Status
- Fabrikam Team
- Customer Profile
- Voice
- Organization Management
- TV
- Phone

[Add all](#)

Cancel Add

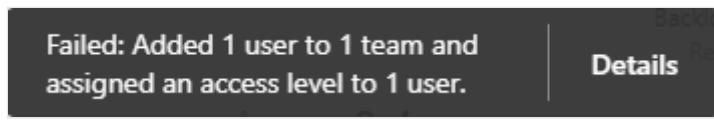
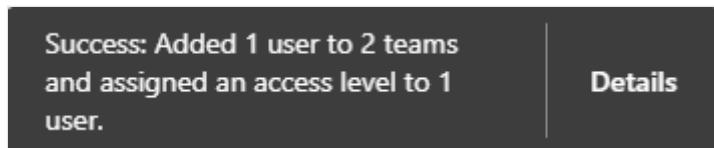
When you add a new user, the system assigns Stakeholder as the access level when all free five Basic access levels get assigned. Active contributors to a project need to have Basic access as a minimum. A Project Collection Administrator can change the access level from the [Organization settings > Users page](#).

! Note

Users with limited access, such as Stakeholders, can't access select features even if granted permissions to those features. For more information, see [Permissions and access](#).

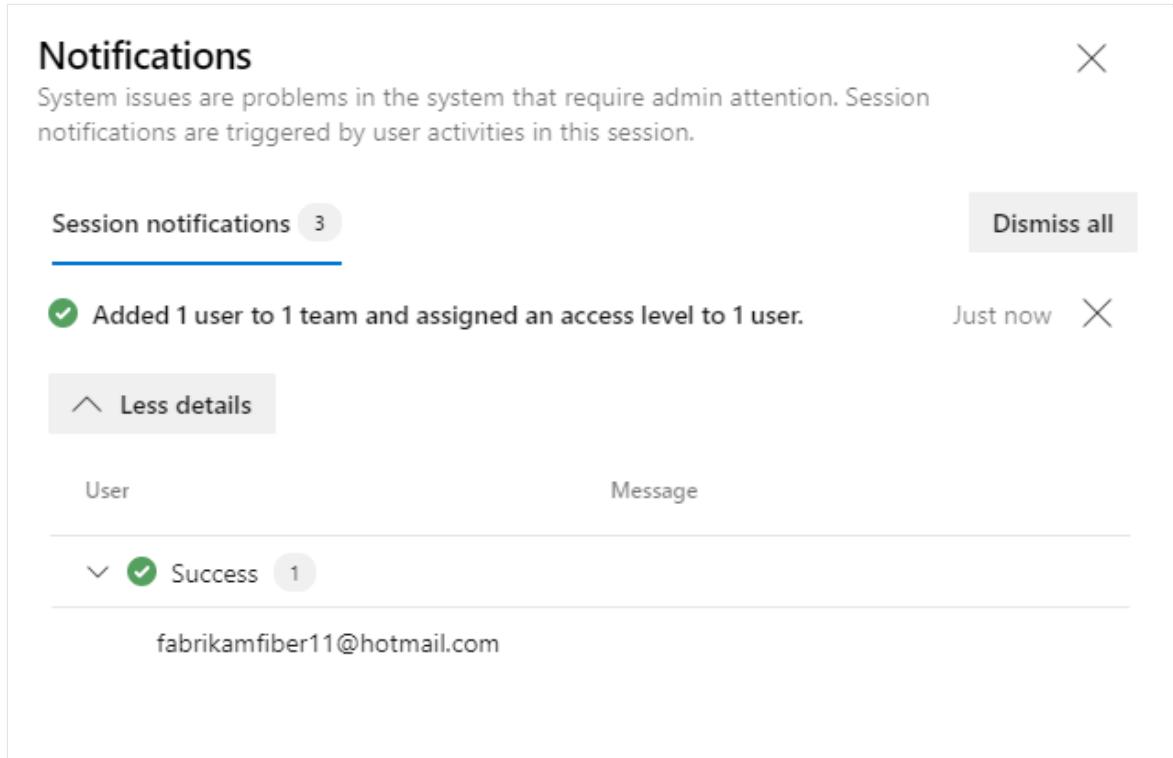
4. (Optional) A message briefly displays on the screen to indicate success or failure.

Select **Details** to open the notification and review details.



A success message indicates the status of adding the user to the system.

A failure message indicates why the addition of the user failed.



The image shows a "Notifications" dialog box. At the top, it says "Notifications" and "System issues are problems in the system that require admin attention. Session notifications are triggered by user activities in this session." Below this, there is a "Session notifications" section with a count of 3, a "Dismiss all" button, and a "Less details" button. The main area lists a single notification: "Added 1 user to 1 team and assigned an access level to 1 user." It includes a timestamp "Just now" and a close button. Below this, there is a table with columns "User" and "Message", showing "fabrikamfiber11@hotmail.com" under "User".

User	Message
fabrikamfiber11@hotmail.com	

"..."

## Notifications



System issues are problems in the system that require admin attention. Session notifications are triggered by user activities in this session.

### Session notifications 1

[Dismiss all](#)

Add 1 user

Just now

Less details

User

Message

Failed 1

fabrikamfiber11@hotmail.com

You are trying to invite a user from outside your directory, but the security setting of this organization doesn't allow it. [Learn more](#)

5. New users receive an email inviting them to sign in to the project. Existing users don't receive any formal notification.

## Manage users or resend invitations

Project Collection Administrators can update user assignments and resend invitations. For more information, see [Add account users for Azure DevOps](#).

Users

All users Group rules

Export users

Filter users Access Level License Source X

Total 16 Selected 1

Summary Add users

Name	Access Level	License Source	Date Added	Last Accessed
<input checked="" type="checkbox"/> fabrikamfiber11@hotmail.com fabrikamfiber11@hotmail.com	Stakeholder	Direct	6/16/2021	Never
<input type="checkbox"/> fabrikamfiber12@hotmail.com fabrikamfiber12@hotmail.com	Stakeholder	Direct	6/16/2021	Never
<input type="checkbox"/> CR Chuck Reinhart fabrikamfiber3@hotmail.com	Stakeholder	Direct	2/23/2018	8/7/2021
<input type="checkbox"/> Francis Totten fabrikamfiber7@hotmail.com	Stakeholder	Direct	2/23/2018	1/2/2021
<input type="checkbox"/> Johnnie McLeod fabrikamfiber2@hotmail.com	Stakeholder	Group Rule	2/23/2018	4/1/2021

⋮

Change access level  
Manage user  
Resend invite  
Remove direct assignments  
Remove from organization

## List team members or team details

From the Azure DevOps CLI command, you can see details about a team or list the individual members of that team. To first see a list of all teams in your organization, use the [az devops team list](#) command.

[List team members](#) | [Show team details](#)

### ⓘ Note

You can use the [az devops user](#) command to add users to an organization. There is no comparable command for adding users to a team or project.

## List team members

You can list the individual members of a team in your organization with the [az devops team list-member](#) command. To get started, see [Get started with Azure DevOps CLI](#).

### Azure CLI

```
az devops team list-member --team  
    [--org]  
    [--project]  
    [--skip]  
    [--top]
```

## Parameters

- **team**: Required. Name or ID of the team to show.
- **org**: Azure DevOps organization URL. You can configure the default organization using `az devops configure -d organization=ORG_URL`. Required if not configured as default or picked up using `git config`. Example: `--org https://dev.azure.com/MyOrganizationName/`.
- **project**: Name or ID of the project. You can configure the default project using `az devops configure -d project=NAME_OR_ID`. Required if not configured as default or picked up using `git config`.
- **skip**: Optional. Number of members to skip.
- **top**: Optional. Maximum number of members to return.

## Example

The following command lists the first five members of the team named **Fabrikam Team** and returns the details in table format.

```
Azure CLI

az devops team list-member --team "Fabrikam Team" --top 5 --output table

ID           Name          Email
-----
3b5f0c34-4aec-4bf4-8708-1d36f0dbc468 Christie Church
fabrikamfiber1@hotmail.com
19d9411e-9a34-45bb-b985-d24d9d87c0c9 Johnnie McLeod
fabrikamfiber2@hotmail.com
8c8c7d32-6b1b-47f4-b2e9-30b477b5ab3d Chuck Reinhart
fabrikamfiber3@hotmail.com
d291b0c4-a05c-4ea6-8df1-4b41d5f39eff Jamal Hartnett
fabrikamfiber4@hotmail.com
bd30c189-db0f-4dd6-9418-5d8b41dc1754 Raisa Pokrovskaya
fabrikamfiber5@hotmail.com
```

## Show team details

You can view details about a team in your organization with the `az devops team show` command. To get started, see [Get started with Azure DevOps CLI](#).

```
Azure CLI

az devops team show --team
                     [--org]
```

## Parameters

- **team**: Required. Name or ID of the team to show.
- **org**: Azure DevOps organization URL. You can configure the default organization using `az devops configure -d organization=ORG_URL`. Required if not configured as default or picked up using `git config`. Example: `--org https://dev.azure.com/MyOrganizationName/`.
- **project**: Name or ID of the project. You can configure the default project using `az devops configure -d project=NAME_OR_ID`. Required if not configured as default or picked up using `git config`.

## Example

The following command shows information about the team in your organization named **Fabrikam Team** and returns the details in table format.

```
Azure CLI

az devops team show --team "Fabrikam Team" --output table

ID           Name          Description
-----       -----
a48cb46f-7366-4f4b-baf5-b3632398ed1e  Fabrikam Team  The default project
team. Was Fabrikam Fiber Team
```

## Next steps

[Manage your project](#)

## Related articles

- [Add users and manage access](#)
- [Resources granted to project members](#)
- [Manage permissions with command line tool](#)
- [Change project visibility to public or private](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage and configure team tools

Article • 02/07/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

If you're a team administrator, you have the flexibility to tailor your backlogs and boards to align with your team's workflow. In case you require a new team, you can ask a Project Administrator group member to create one for you, which takes only a minute. Team administrators have the ability to set up and oversee all team tools.

Team administrators perform the following tasks for team tools:

- [Add team members](#)
- [Add another team administrator](#)
- [Configure areas and iteration paths](#)
- [Configure backlogs, boards, and general settings](#)
- [Configure and manage team dashboards](#)
- [Configure team notifications](#)

## Prerequisites

[+] [Expand table](#)

Category	Requirements
Permissions	<ul style="list-style-type: none"><li>- To manage teams: <a href="#">Team administrator</a> or member of the <a href="#">Project Administrators</a> group.</li><li>- To add a team: Member of the <a href="#">Project Administrators</a> group. For more information, see <a href="#">Add teams</a>.</li></ul>

### ⓘ Note

For more information, see the following articles:

- [Use backlogs to manage projects](#)
- [Configure and customize Azure Boards](#)
- [Create a project using the process of your choice](#)
- [Customize your work tracking experience](#)
- [Create and manage inherited processes](#)

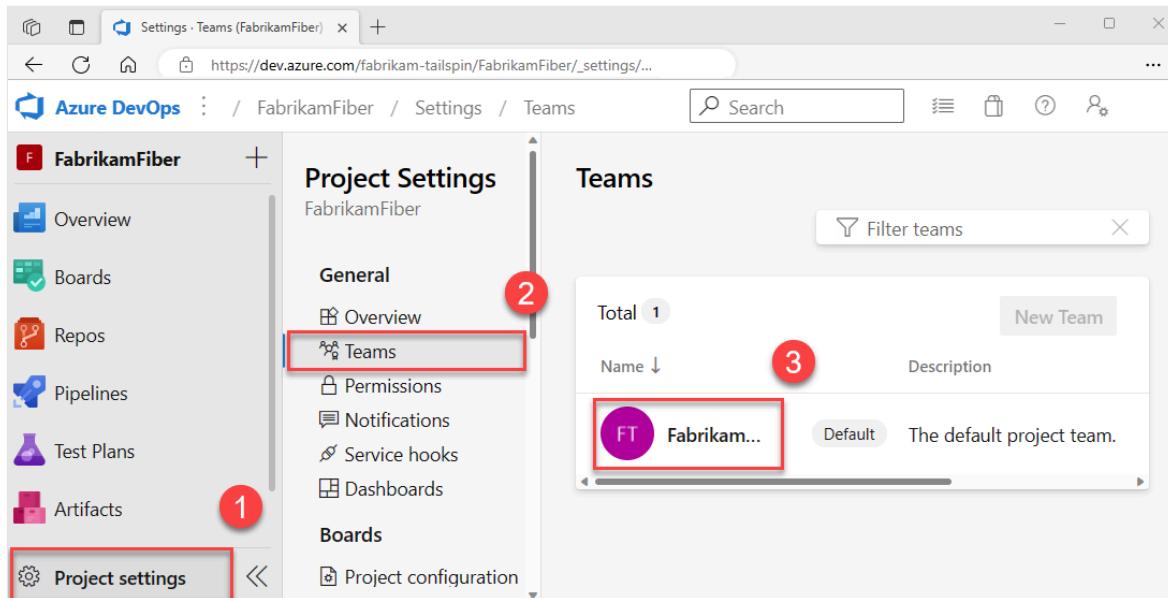
# Open your team profile

Open your team profile to quickly access items defined for your team.

## 1. Sign in to your project

([https://dev.azure.com/{Your\\_Organization}/{Your\\_Project}](https://dev.azure.com/{Your_Organization}/{Your_Project})).

## 2. Select Project settings > Teams > your team.



# Add users to a team

Tools like capacity planning, team alerts, and dashboard widgets operate within the scope of a team. They automatically access the user information of team members to facilitate planning tasks or issue alerts.

To add users to a team, see [Add users to a project or specific team](#).

The screenshot shows the 'Fabrikam Fiber Team' page. The top navigation bar includes a team icon, the team name, a description ('The default project team.'), and links for Notifications, Dashboards, and Iterations and Area Paths. Below is a 'Members' tab (selected) and a 'Settings' tab. The 'Members' table shows a total of 13 members, with 1 filtered. A search bar and a 'Direct Members' dropdown are at the top of the table. The table lists members with checkboxes for selecting them: 'JH Jamal Hartnett' (user type). An 'Add' button is highlighted with a red box.

All members of a team can favorite team artifacts and define work item templates. For more information, see:

- Set personal or team favorites
- Use templates to add and update work items.

If team members don't have access to all the features they want, make sure they have the permissions needed for those features.

## Add an administrator

When you add a team to a project, a Project Administrator should [add one or more team administrators](#).

The screenshot shows the 'FabrikamFiber Team' settings page. At the top, there's a breadcrumb navigation: Fiber / Settings / Teams / FabrikamFiber Team. Below the breadcrumb, there are two tabs: 'Members' and 'Settings', with 'Settings' being the active tab. The main content area is titled 'Team Details'. It contains two fields: 'Team name' with the value 'FabrikamFiber Team' and 'Description' with the value 'The default project team.'. A 'Save' button is located below these fields. Below the 'Team Details' section is another section titled 'Administrators' with the sub-instruction 'All teams need to have an Administrator.' A red-bordered 'Add' button is visible in this section.

## Configure team areas and iterations

Many Agile tools rely on the team's configured area and iteration paths. For more information, see [About teams and Agile tools](#).

After project administrators add the project's area and iteration paths using [Set area paths](#) and [Set iteration paths](#), team administrators can choose the relevant area and iteration paths for their team. These settings influence a wide range of Agile tools that the team can access.

The screenshot shows the 'FabrikamFiber Team' settings page. At the top, there's a purple circular icon with 'FT' in white. Next to it is the team name 'FabrikamFiber Team' and a description 'The default project team.'. Below this, a red box highlights the 'Iterations and Area Paths' link in the 'Relevant links' section. The 'Settings' tab is selected. The 'Team Details' section contains fields for 'Team name' (FabrikamFiber Team) and 'Description' (The default project team.). A 'Save' button is visible. The 'Administrators' section notes that all teams need an administrator and has an 'Add' button. The 'Iterations and Area Paths' section is also visible.

Settings include making the following associations for each team:

- **Select team area paths**  
Can select the default area paths associated with the team. These settings affect many Agile tools available to the team.
- **Select team iteration paths or sprints** Can select the default area paths associated with the team. These settings affect many Agile tools available to the team.

For more information, see [Define area paths and assign to a team](#) and [Define iteration paths and configure team iterations](#).

## Configure team backlogs, boards, and general settings

As a team administrator, you have the flexibility to customize your team's workflow to suit your needs. One way to do so is by choosing which backlog levels are active for your team. For instance, a feature team might only want to display the product backlog, while a management team might prefer to show the feature and epic backlogs only.

Also, you can choose how to treat bugs within your workflow, either as user stories and requirements or as tasks.

Another way to customize your team's workflow is by selecting nonworking days for the team. By doing so, sprint planning and tracking tools can automatically take these days off into account when calculating capacity and sprint burndown.

Most of these team settings can be easily configured from the common configuration dialog, providing a convenient way to manage your team's workflow in one central location. You can also [set team automation rules to update work items when child item states change](#).

 **Note**

For more information, see [Backlogs, boards, and plans](#). In case you don't see the desired work items on your backlog or board, see [Set up your backlogs and boards](#).

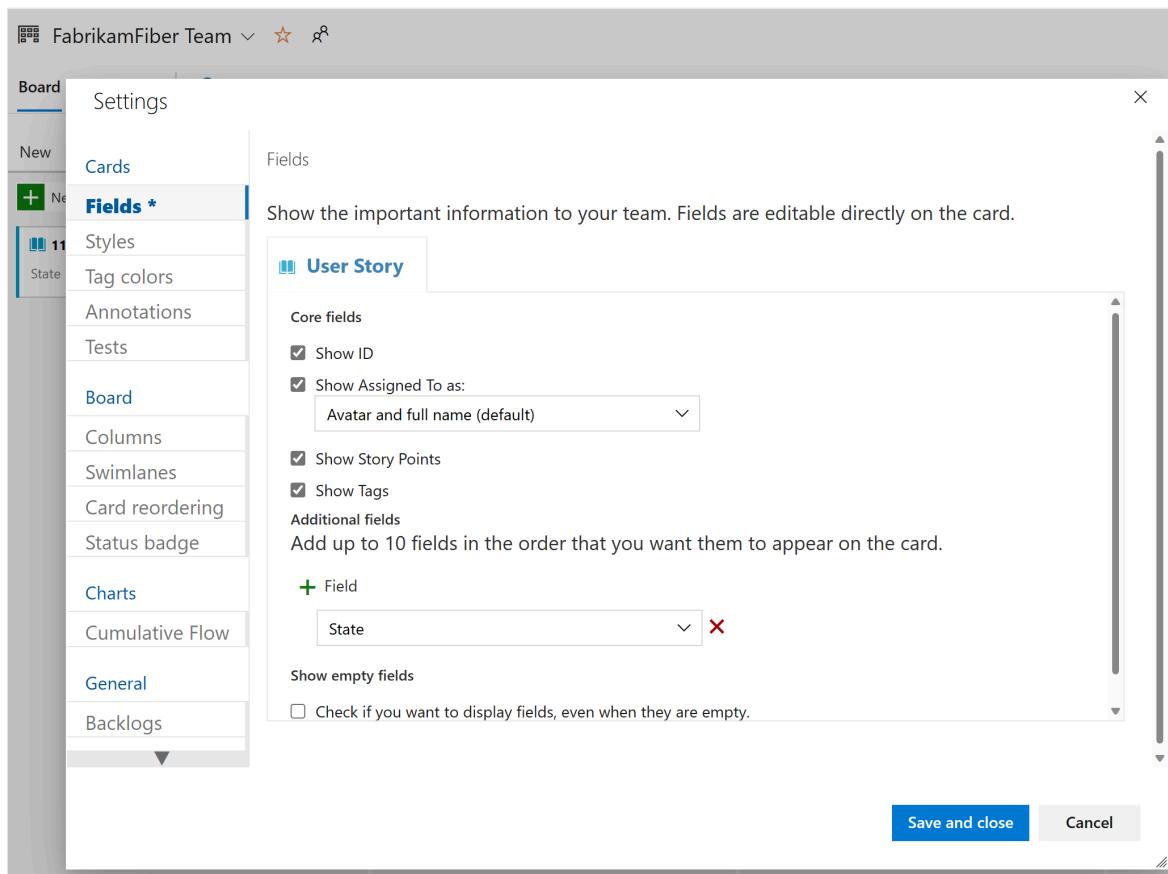
1. Check that you selected the correct project, and then choose **Boards > Boards**, and select the correct team from the team selector dropdown menu. For more information, see [Use breadcrumbs and selectors to navigate and open artifacts](#).

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, a sidebar lists various sections: Overview (1), Boards (highlighted with a red box), Work items, Boards (highlighted with a red box) (2), Backlogs, Sprints, Queries, Repos, Pipelines, Test Plans, and Artifacts. The main area is titled 'Fabrikam Fiber Team' (3). It displays a Kanban board with two columns: 'To Do' and 'Doing'. Under 'To Do', there is a card for '1 Bug' with the state 'To Do'. A 'New item' button and a search icon are also present.

2. Choose **Team settings**  to configure the board and set general team settings.

This screenshot shows the 'Team settings' page for the 'Fabrikam Fiber Team'. At the top, it shows the team name and some navigation links: 'Board' (selected), 'Analytics', 'View as Backlog', 'Stories' (with a dropdown arrow), a filter icon, and a gear icon (highlighted with a red box). Below these are several configuration tabs: Cards, Board, Charts, General, Analytics, Stories, Filter, and Save and close.

3. Choose a tab under any of the sections—**Cards, Board, Charts, and General**—to configure the cards or boards, the cumulative flow chart, or other team settings. When you're done configuring the settings, select **Save and close**.



Team administrators have complete control over customizing their team's boards for both the product and portfolio backlogs. To set up a board, you can define the columns and work-in-progress (WIP) limits through the common configuration dialog. For more information, see [Board overview](#) and [Board quickstart](#).

For detailed information on each configuration option, see the following articles:

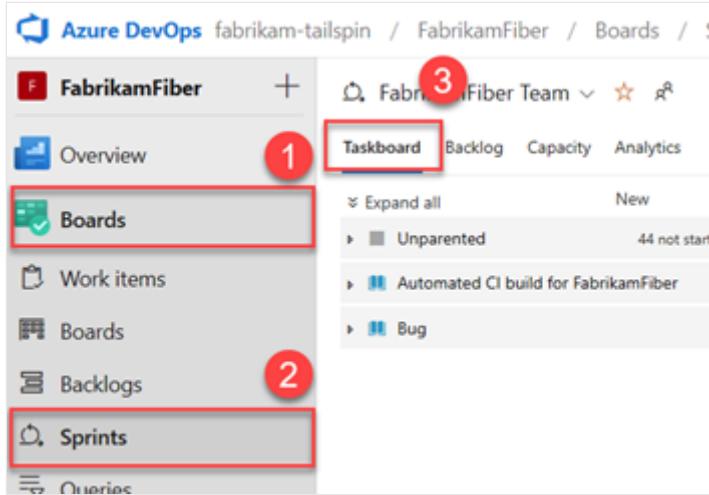
[+] [Expand table](#)

Category	Articles
General	<ul style="list-style-type: none"><li>- <a href="#">Backlogs</a></li><li>- <a href="#">Working with bugs</a></li></ul>
Cards	<ul style="list-style-type: none"><li>- <a href="#">Add fields</a></li><li>- <a href="#">Define styles</a></li><li>- <a href="#">Add tag colors</a></li><li>- <a href="#">Enable annotations</a></li><li>- <a href="#">Configure inline tests</a></li></ul>
Chart	<ul style="list-style-type: none"><li>- <a href="#">Configure cumulative flow chart</a></li></ul>
Boards	<ul style="list-style-type: none"><li>- <a href="#">Add columns</a></li><li>- <a href="#">Split columns</a></li><li>- <a href="#">WIP limits</a></li><li>- <a href="#">Definition of Done</a></li><li>- <a href="#">Add swimlanes</a></li></ul>

Category	Articles
	<ul style="list-style-type: none"> <li>- <a href="#">Card reordering</a></li> <li>- <a href="#">Configure status badges</a></li> </ul>

## Configure sprint taskboards

Similar to boards, you can customize each sprint Taskboard to support information-rich color-coded cards and columns. For more information, see [Customize sprint taskboards](#).



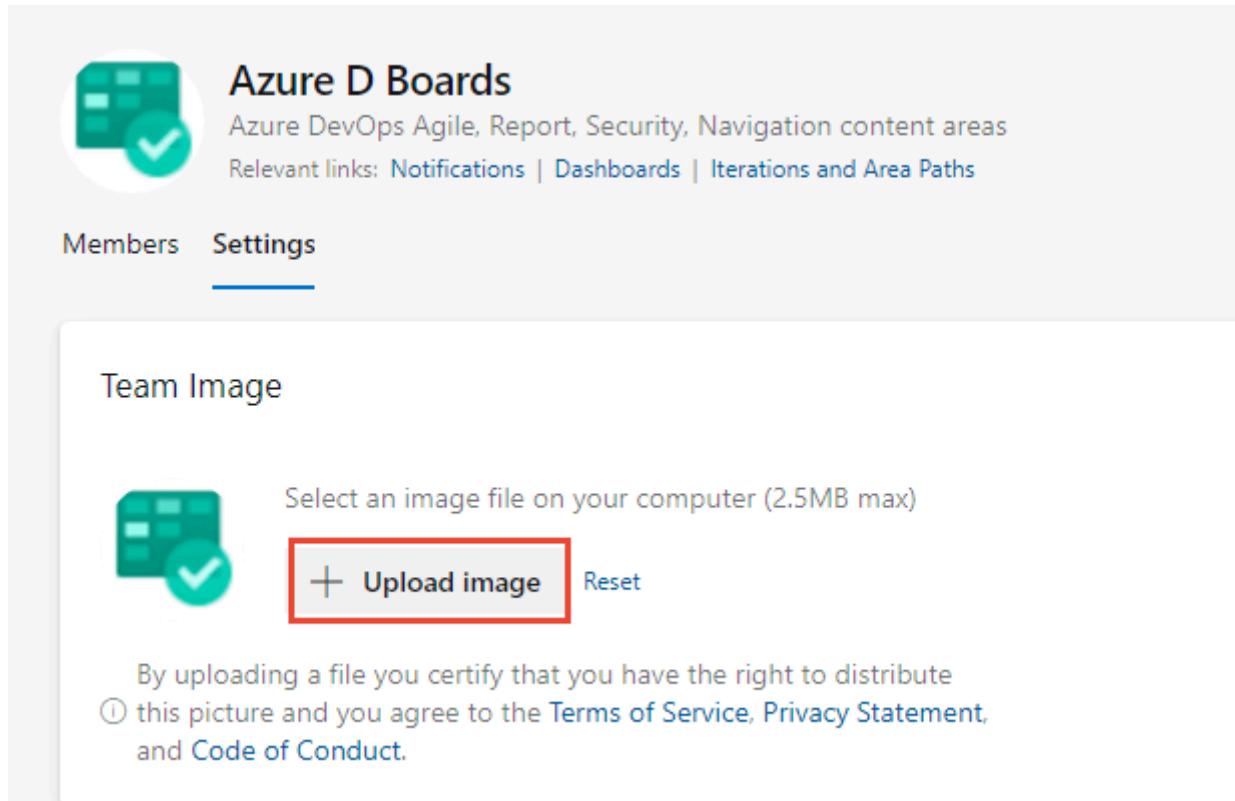
## Add and manage team dashboards

By default, all team members can add and edit team dashboards. In addition, team administrators can manage permissions for team dashboards. For more information, see [Add and manage dashboards](#).

The screenshot shows the 'Teams' settings page for the 'FabrikamFiber Team'. It features a purple circular icon with 'FT' and the team name 'FabrikamFiber Team'. Below it, the text 'The default project team' and 'Relevant links: Notifications, Dashboards, Iterations and Area Paths' are displayed. A red box highlights the 'Dashboards' link. The 'Settings' tab is selected. The 'Team Details' section contains fields for 'Team name' (set to 'FabrikamFiber Team') and 'Description' (set to 'The default project team.'), both with placeholder text. A blue 'Save' button is at the bottom.

# Update team name, description, and image

Team settings also include the team name, description, and team profile image. To add a team picture, select the image icon. The maximum file size is 2.5 MB and 2560 x 1,024 px, and then we resize to 200 x 200.



## Manage notifications

Team administrators have the ability to add and edit alerts, allowing the team to receive email notifications as changes occur to work items, code reviews, source control files, and builds. Various alerts are predefined for each team. For more information, see [Manage team alerts](#).



**FabrikamFiber Team**  
The default project team.  
Relevant links: [Notifications](#) | [Dashboards](#) | [Iterations and Area Paths](#)

Members [Settings](#)

---

### Team Details

Team name

Description

[Save](#)

## Related articles

- [About projects and scaling your organization](#)
- [About teams and Agile tools](#)
- [Add teams](#)
- [Add a team administrator](#)
- [Automate work item state transitions](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

# Request a permission increase

Article • 02/07/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

To access certain tasks, you might need to request higher permissions or be assigned to a specific security role. This scenario typically occurs when you encounter an informational or error message indicating insufficient permissions, which specify the required permission levels.

## Common permissions to request

Most members of the **Contributors** group have the permissions they need to perform most tasks. However, the following tasks require membership in the **Project Administrators** group or a change in permissions.

- **Work tracking:**
  - **Add or change Area Paths or Iteration Paths:** Requires elevated permissions to an Area Path or Iteration Path node. For more information, see [Set work tracking permissions](#), [Create child nodes](#).
  - **Create shared queries or query folders:** Requires elevated permissions set for a shared query folder. For more information, see [Set work tracking permissions](#), [Set permissions on queries or query folders](#).
  - **Change team settings—such as board settings:** Requires addition as a team administrator. For more information, see [Add or remove a team administrator](#).
- **Source code, Git repositories:** The following tasks require elevated permissions for Git repositories or a specific repository. For more information, see [Set Git repository permissions](#).
  - Create, delete, or rename a Git repository
  - Manage repository permissions
  - Bypass policies

The following tasks require membership in the **Project Collection Administrators** group or a change in permissions at the collection-level or addition to a specific role.

- **Collection-level configurations:**
  - **Create projects:** Requires elevated permissions at the [collection level](#).
  - **Add, edit, or manage a process:** Requires elevated permissions at the collection level or [process-level permissions](#).

- **Install, uninstall, or disable extensions:** Requires addition to the [Manager role](#) for extensions.

For an overview of built-in security groups and default permission assignments, see [Default permissions and access](#).

## Prerequisites

[+] Expand table

Category	Requirements
Permissions	To view permissions and to look up a project administrator: Member of the <b>Project Valid Users</b> group. Project members are automatically part of this security group. For more information, see <a href="#">View permissions for yourself or others</a> .
Knowledge	Before you request a permission change, ensure you understand the basics by reviewing <a href="#">Get started with permissions, access, and security groups</a> .

### ! Note

Users added to the **Project-scoped users** group don't have access to **Organization settings** other than the **Overview** section if the **Limit user visibility and collaboration to specific projects** preview feature is enabled for the organization. For more information including important security-related call-outs, see [Manage your organization, Limit user visibility for projects and more](#).

## Review your permission assignments

Before you request a change to permission levels, review your permission assignments as described in [View permissions for yourself or others](#).

Verify that your permission assignments are preventing you from accomplishing a task you need to perform.

## Request a change to a permission level or role change

To request a change or increase in your permission levels, take the following actions:

1. Identify the permissions you need and at what level. Permissions are set at the object, project, and project-collection level. Also, permissions are granted through various roles. To identify the level and permission you need, review the [Permissions lookup guide](#).
2. Identify a person in your organization who can grant you the permissions you need. For example:
  - To get permissions to manage team settings, [identify the team administrator for your team](#) or a [member of the Project Administrators group](#).
  - To change an object-level permission, identify the owner of the object or a member of the **Project Administrators** group. To learn how, see [Set object-level permissions](#).
  - To change a project-level permission, identify a member of the **Project Administrators** group. See [Look up a project administrator](#).
  - To change a project collection-level permission, identify a member of the **Project Collection Administrators** group. See [Look up a project collection administrator](#).
3. Contact the person you identified in step 2 and make your request. Make sure you specify the permission you want changed.

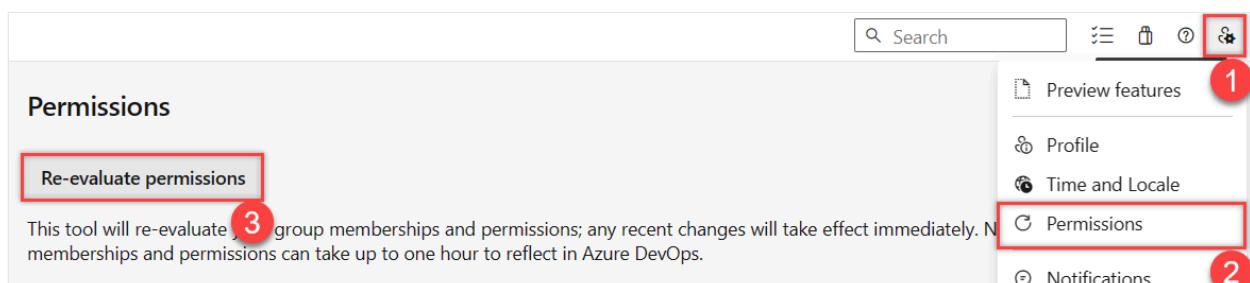
## Refresh or reevaluate your permissions

After your permission levels get changed, you might need to refresh your permissions for Azure DevOps to recognize the updates. This step is recommended when:

- **Permission or role changes:** Your permission level or role was modified.
- **Security group modifications:** You were added to a new or different security group in Azure DevOps, Microsoft Entra ID, or Active Directory.

Getting added to a new security group can alter your inherited permissions.

**Refresh your permissions**, which prompts Azure DevOps to reevaluate your permission assignments immediately. If you don't refresh, your permission assignments don't update until you sign out, close your browser, and sign back in.



## Related articles

- [Permissions lookup guide](#)
- [Default permissions and access](#)
- [Troubleshoot permissions](#)
- [Look up a project administrator](#)
- [Look up a project collection administrator](#)

 **Note:** The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Manage access to specific features

Article • 02/06/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Managing access to specific features in Azure DevOps can be crucial for maintaining the right balance of openness and security. Whether you're looking to grant or restrict access to certain functionalities for a group of users, understanding the flexibility beyond the standard permissions provided by built-in security groups is key.

If you're new to the permissions and groups landscape, see [Get started with permissions, access, and security groups](#). This article covers the essentials of permission states and how they inherit.

## 💡 Tip

The structure of your project in Azure DevOps plays a pivotal role in determining the granularity of permissions at an object level, such as repositories and area paths. This structure is the foundation that allows you to fine-tune access controls, enabling you to specifically delineate which areas are accessible or restricted. For more information, see [About projects and scaling your organization](#).

## Prerequisites

[+] Expand table

Category	Requirements
Permissions	Member of the <a href="#">Project Collection Administrators group</a> . Organization owners are automatically members of this group.

## Use security groups

For optimal maintenance, we recommend using the default security groups or establishing [custom security groups to manage permissions](#). The permission settings for the **Project Administrators** and **Project Collection Administrators** groups are fixed by design and can't be altered. However, you have the flexibility to modify permissions for all other groups.

Managing permissions for a few users individually might seem feasible, but custom security groups provide a more organized approach. They streamline the oversight of roles and their associated permissions, ensuring clarity and ease of management design and can't be altered. But, you have the flexibility to modify permissions for all other groups.

## Delegate tasks to specific roles

As an administrator or organization owner, delegating administrative tasks to team members who oversee specific areas is a strategic approach. The primary built-in roles equipped with predefined permissions and role assignments include:

- **Readers:** Have read-only access to the project.
- **Contributors:** Can contribute to the project by adding or modifying content.
- **Team Administrator:** Manage team-related settings and permissions.
- **Project Administrators:** Have administrative rights over the project.
- **Project Collection Administrators:** Oversee the entire project collection and have the highest level of permissions.

These roles facilitate the distribution of responsibilities and streamline the management of project areas.

For more information, see [Default permissions and access](#) and [Change project collection-level permissions](#).

To delegate tasks to other members within your organization, consider creating a custom security group and then granting permissions as indicated in the following table.

### Role

### Tasks to perform

#### Permissions to set to Allow

Development lead (Git)

Manage branch policies

Edit policies, Force push, and Manage permissions

See [Set branch permissions](#).

Development lead (Team Foundation Version Control (TFVC))

Manage repository and branches

Administer labels, Manage branch, and Manage permissions

See [Set TFVC repository permissions](#).

Software architect (Git)

Manage repositories

Create repositories, Force push, and Manage permissions

See [Set Git repository permissions](#)

Team administrators

Add area paths for their team

Add shared queries for their team

Create child nodes, Delete this node, Edit this node See [Create child nodes, modify work items under an area path](#)

Contribute, Delete, Manage permissions (for a query folder), See [Set query permissions](#).

Contributors

Add shared queries under a query folder, Contribute to dashboards

Contribute, Delete (for a query folder), See [Set query permissions](#)

View, Edit, and Manage dashboards, See [Set dashboard permissions](#).

Project or product manager

Add area paths, iteration paths, and shared queries

Delete and restore work items, Move work items out of this project, Permanently delete work items

Edit project-level information, See [Change project-level permissions](#).

Process template manager ([Inheritance process model](#))

Work tracking customization

Administer process permissions, Create new projects, Create process, Delete field from account, Delete process, Delete project, Edit process

See [Change project collection-level permissions](#).

Process template manager ([Hosted XML process model](#))

Work tracking customization

Edit collection-level information, See [Change project collection-level permissions](#).

Project management ([On-premises XML process model](#))

Work tracking customization

Edit project-level information, See [Change project-level permissions](#).

Permissions manager

Manage permissions for a project, account, or collection

For a project, Edit project-level information

For an account or collection, Edit instance-level (or collection-level) information

To understand the scope of these permissions, see [Permission lookup guide](#). To request a change in permissions, See [Request an increase in permission levels](#).

In addition to assigning permissions to individuals, you can manage permissions for various objects within Azure DevOps. These objects include:

- [Git repositories](#)
- [Git branches](#)
- [TFVC repositories](#)
- [Build and release pipelines](#)
- [Wikis](#).

These links provide detailed steps and guidelines for setting up and managing permissions effectively for the respective areas in Azure DevOps.

## Limit user visibility

### Warning

Consider the following limitations when using this preview feature:

- The limited visibility features described in this section apply only to interactions through the web portal. With the REST APIs or `azure devops` CLI commands, project members can access the restricted data.

- Users in the limited group can only select users who are explicitly added to Azure DevOps and not users who have access through Microsoft Entra group membership.
- Guest users who are members in the limited group with default access in Microsoft Entra ID, can't search for users with the people picker.

## Organizations and projects

By default, users added to an organization can view all organization and project information and settings. You can restrict specific users, such as Stakeholders, Microsoft Entra users, or member sof a particular security group, with the **Limit user visibility and collaboration to specific projects** preview feature for the organization. Once the feature [gets turned on](#), any user or group that [gets added to the Project-Scope Users group](#) is restricted in the following ways:

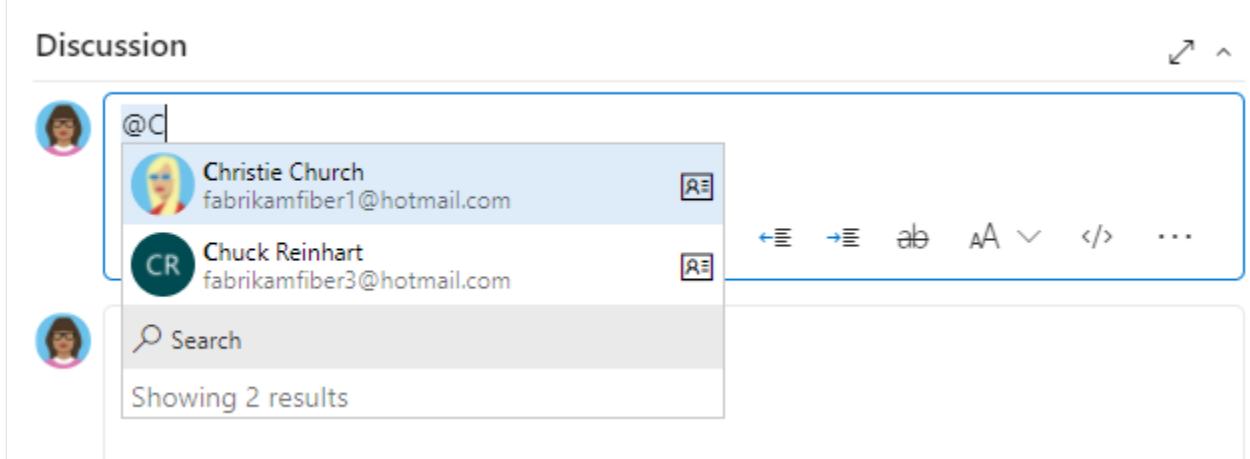
- Access is confined to only the projects to which they're explicitly added.
- Views displaying lists of users, projects, billing details, usage data, and more accessed through **Organization settings** are restricted.
- The set of people or groups that appear in people-picker search selections and the ability to **@mention** people is limited.

## Identity search and selection

With Microsoft Entra ID, you can use people pickers to search for any user or group in your organization, not just the ones in your current project. People pickers support the following Azure DevOps functions:

- Selection of a user identity from a work tracking identity field such as **Assigned To**
- Selection of a user or group using **@mention** in a work item discussion or rich-text field, a pull request discussion, commit comments, or changeset or shelveset comments
- Selection of a user or group using **@mention** from a wiki page

As shown in the following image, start entering a user or security group name into a people picker box until you find a match.



Users and groups who are added to the **Project-SScoped Users** group can only see and select users and groups in the project they're connected to from a people picker.

## Turn on the preview feature and add users to the security group

Do the following steps to turn on the preview feature and add users and group to the Project-SScoped Users group:

1. Turn on the **Limit user visibility and collaboration to specific projects** [preview feature](#) for the organization.
2. Add the users to your project as described in [Add users to a project or team](#). Users added to a team are automatically added to the project and team group.
3. Open [Organizations settings > Security > Permissions](#) and choose **Project-SScoped Users**. Select the **Members** tab.
4. Add all users and groups that you want to scope to the project they're added to. For more information, see [Set permissions at the project- or collection-level](#).

The **Project-SScoped Users** group only appears under the **Permissions > Groups** when the **Limit user visibility and collaboration to specific projects** preview feature is turned on.

All security groups in Azure DevOps are considered organization-level entities, even if they only have permissions for a specific project. This means that security groups get managed at the organization level.

From the web portal, the visibility of some security groups might be restricted based on the user's permissions. However, you can still discover the names of all security groups within an organization by using the `azure devops` CLI tool or the REST APIs. For more information, see [Add and manage security groups](#).

# Restrict access to view or modify objects

Azure DevOps is designed to allow all authorized users to view all defined objects within the system. However, you can tailor access to resources by setting the permission state to **Deny**. You can set permissions for members who belong to a custom security group or for individual users. For more information, see [Request an increase in permission levels](#).

## Area to restrict

### Permissions to set to Deny

View or contribute to a repository

View, Contribute

See [Set Git repository permissions](#) or [Set TFVC repository permissions](#).

View, create, or modify work items within an area path

Edit work items in this node, View work items in this node

See [Set permissions and access for work tracking](#), [Modify work items under an area path](#).

View or update select build and release pipelines

Edit build pipeline, View build pipeline

Edit release pipeline, View release pipeline

You set these permissions at the object level. See [Set build and release permissions](#).

Edit a dashboard

View dashboards

See [Set dashboard permissions](#).

# Restrict modification of work items or select fields

For examples that illustrate how to restrict modification of work items or select fields, see [Sample rule scenarios](#).

# Next steps

[Remove user accounts](#)

## Related articles

- [View default permissions and access](#)
- [Use the permission lookup guide](#)
- [Get started with permissions, access, and security groups](#)
- [Refer to permissions and groups](#)
- [Change project-level permissions](#)
- [Change project collection-level permissions](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Make your Azure DevOps secure

Article • 05/14/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

When you're handling information and data, especially in a cloud-based solution like Azure DevOps Services, security should be your top priority. While Microsoft ensures the security of the underlying cloud infrastructure, it's your responsibility to configure security within Azure DevOps. This article provides an overview of necessary security-related configurations to protect your Azure DevOps environment against threats and vulnerabilities.

## Protect your network and data

Securing your network is crucial when you're working with Azure DevOps to protect your data and resources from unauthorized access and potential threats. Implement network security and data protection measures to help ensure that only trusted sources can access your Azure DevOps environment. To secure your network when you're working with Azure DevOps, do the following actions:

- **[Set up IP allowlisting](#)**: Restrict access to specific IP addresses to allow traffic only from trusted sources, reducing the attack surface. If your organization is secured with a firewall or proxy server, add IPs and URLs to the allowlist.
- **[Use data encryption](#)**: Protect your data by using encryption, backup, and recovery strategies. Always encrypt data in transit and at rest. Secure communication channels using protocols like HTTPS. Learn more about [Azure Encryption](#).
- **[Validate certificates](#)**: Ensure certificates are valid and issued by trusted authorities when establishing connections.
- **[Implement Web Application Firewalls \(WAFs\)](#)**: Filter, monitor, and block malicious web-based traffic with WAFs for an extra layer of protection against common attacks.
- **[Network security groups \(NSGs\) overview](#)**: Use NSGs to control inbound and outbound traffic to Azure resources, ensuring only authorized traffic is allowed.
- **[Use Azure Firewall](#)**: Deploy Azure Firewall to provide a centralized network security policy across multiple Azure subscriptions and virtual networks.
- **[Monitor network traffic with Azure Network Watcher](#)**: Use Azure Network Watcher to monitor and diagnose network issues, ensuring the security and performance of your network.
- **[Implement DDoS protection with Azure DDoS Protection](#)**: Enable Azure DDoS Protection to safeguard your applications from distributed denial-of-service (DDoS) attacks.
- **[Protect your data]**: Protect your data by using encryption, backup, and recovery strategies.

For more information, see [Application management best practices](#).

## Implement Zero Trust

Adopt [Zero Trust](#) principles across your DevOps processes to make sure every access request is thoroughly verified, regardless of its origin. Zero Trust operates on the principle of "never trust, always verify," meaning that no entity, whether inside or outside the network, is trusted by default. By implementing Zero Trust, you can significantly reduce the risk of security breaches and ensure that only authorized users and devices can access your resources.

- Fortify your [DevOps platform](#),
- Safeguard your [development environment](#),
- Integrate Zero Trust seamlessly into your [developer workflows](#).

Zero Trust helps to protect against lateral movement within the network, ensuring that even if there's a compromised part of the network, the threat is contained and can't spread. For more information, see the [Zero Trust Assessment guide](#) ↗.

## Comply with industry standards

Ensure your Azure DevOps environment complies with industry standards and regulations that protect your environment and maintain trust with your users.

- **Ensure compliance with industry standards:** Azure DevOps complies with various industry standards and regulations, such as ISO/IEC 27001, SOC 1/2/3, and GDPR. Ensure your environment adheres to these standards.
- **Enforce compliance policies:** Implement [branch policies](#) and [compliance policies for your pipelines](#).
- **Onboard to Component Governance for CI/CDs**, which offers the following benefits:
  - Security vulnerability detection: Alerts you to known vulnerabilities in open-source components.
  - License compliance: Ensures components comply with your organization's licensing policies.
  - Policy enforcement: Ensures only approved versions are used.
  - Visibility with tracking: Provides visibility into components across repositories for easier management.

## Control and restrict access

Review through all the security policies available to administrators to restrict and control who has access to the organization. Maintain control of the organization by preventing unnecessary

project creation.

- **Disable “Allow public projects”:** Disable the option to [create public projects](#). Switch project visibility from public to private as needed. Users who never signed in have read-only access to public projects, while signed-in users can be granted access to private projects and make permitted changes.
- **Restrict unnecessary authentication mechanisms** and limit who has access to allowed authentication.
- **Limit access with Conditional Access Policies:** Protect your organization by [defining Conditional Access policies \(CAPs\)](#) on Microsoft Entra that react to sign-in events and request additional actions before a user is granted access.
  - Turn on the organization policy to [enable IP CAP validation on non-interactive flows](#).
  - Add an extra layer of security by [enabling Microsoft Entra multifactor authentication after sign-in](#).

## Manage external guests

External guest access can introduce potential security risks if not managed properly. Minimize these risks and ensure that external guests have the appropriate level of access without compromising the security of your environment.

- **Block external guest access:** Disable the “[Allow invitations to be sent to any domain](#)” [policy](#) to prevent external guest access if there's no business need for it.
  - [Disable “External guest access” organization policy](#) on Azure DevOps.
- **Use distinct emails or UPNs:** Use different email addresses or user principal names (UPNs) for personal and business accounts to eliminate ambiguity between personal and work-related accounts.
- **Group external guest users:** Place all external guest users in a single Microsoft Entra group and [manage permissions for this group appropriately](#). Remove direct assignments to ensure group rules apply to these users.
- **Reevaluate rules regularly:** Regularly review rules on the Group rules tab of the Users page. Consider any group membership changes in Microsoft Entra ID that might affect your organization. Microsoft Entra ID can take up to 24 hours to update dynamic group membership, and rules are automatically reevaluated every 24 hours and whenever a group rule changes.

For more information, see [B2B guests in the Microsoft Entra ID](#).

## Remove unnecessary users

Removing inactive or unauthorized users from your organization helps maintain a secure environment and reduces the risk of potential security breaches.

- **Directly remove inactive Microsoft account users (MSAs):** Directly remove inactive users from your organization if they're using MSAs. You can't create queries for work items assigned to removed MSA accounts.
- **Disable or delete Microsoft Entra user accounts:** If connected to Microsoft Entra ID, disable or delete the Microsoft Entra user account while keeping the Azure DevOps user account active. You may continue querying work item history using their Azure DevOps user ID.
- **Revoke user PATs for administrators:** Ensure secure management of these critical authentication tokens by regularly reviewing and revoking any existing user PATs.
- **Revoke special permissions granted to individual users:** Audit and revoke any special permissions granted to individual users to ensure alignment with the principle of least privilege.
- **Reassign work from removed users:** Before removing users, reassign their work items to current team members to distribute the load effectively.

## Scope permissions

Provide the minimum necessary [permissions](#) and [access levels](#) to ensure that only authorized individuals and services can access sensitive information and perform critical actions. This practice helps to minimize the risk of unauthorized access and potential data breaches.

Regularly review and update these settings to adapt to changes in your organization, such as role changes, new hires, or departures. Implementing a periodic [audit](#) of permissions and access levels can help identify and rectify any discrepancies, ensuring that your security posture remains robust and aligned with best practices.

Learn more about permissions:

- [Permissions and role lookup guide](#)
- [Set individual permissions](#)

To ensure secure and efficient management of permissions, properly scope [permissions](#) within your Azure DevOps environment. Scoping permissions involves defining and assigning the appropriate level of access to users and groups based on their roles and responsibilities. This practice helps to minimize the risk of unauthorized access and potential data breaches by ensuring that only authorized individuals have access to sensitive information and critical actions.

To scope permissions effectively, do the following actions:

- **Disable inheritance:** Avoid [permissions inheritance](#) and prevent unintended access. Inheritance can inadvertently grant permissions to users who shouldn't have them, due to its allow-by-default nature. Carefully manage and explicitly set permissions to ensure that only the intended users have access.
- **Segment environments:** Use separate Azure accounts for different environments, such as Development, Testing, and Production, to enhance security and prevent conflicts. This approach minimizes the risk of resource conflicts and data contamination between environments and allows for better management and isolation of resources. For more information, see [Azure Landing Zone](#).
- **Control access and ensure compliance:** Use [Azure Policy](#) to restrict access to unused Azure regions and services, ensuring compliance with organizational standards. This action helps enforce best practices and maintain a secure environment by preventing unauthorized access and usage.
- **Implement Azure role-based control (ABAC):** Use ABAC with properly tagged resources to limit unauthorized access. This action ensures that access permissions get granted based on specific attributes, enhancing security by preventing unauthorized resource creation and access.
- **Use security groups:** Use [security groups](#) to efficiently manage permissions for multiple users. This method simplifies granting and revoking access compared to assigning permissions individually and ensures consistency and easier management across your organization.
  - Use [Microsoft Entra ID](#), Active Directory, or Windows security groups when you're managing lots of users.
  - Reduce the risk of leaking sensitive information and deploying insecure code by [limiting access to projects and repositories](#) to built-in or custom security groups.
  - Take advantage of built-in roles and default to Contributor for developers. Admins get assigned to the Project Administrator security group for elevated permissions, allowing them to configure security permissions.
  - Keep groups as small as possible, restricting access.
  - Implement [just-in-time access](#) with a Microsoft Entra [Privileged Identity Management \(PIM\) group](#). Grant elevated permissions only when needed, reducing the risk associated with permanent access.

## Ditch service accounts

Historically, service accounts were used in conjunction with [personal access tokens \(PATs\)](#) to build tools that run automated processes and services. As a result, they often have elevated permissions. Before choosing to continue building with a service account, explore if it's still the right authentication approach for you.

- Give up your PATs for Microsoft Entra tokens: Microsoft Entra tokens are short-lived ([one-hour](#)) tokens that can be used in place of most PATs. PATs are popular due to their ease of use, but they are also a popular vector of attack due to the ease in which they are leaked.
- Read up on all the [authentication mechanisms available](#) before choosing one.
- Use service principals instead: Service principals represent a Microsoft Entra application's identity and have their own permissions that define what the application can do in a given tenant. Service principals are the recommended choice to manage the permissions needed by the app. Replace any service accounts' PATs with Microsoft Entra tokens acquired for the service principal.
  - Take it one step further by authenticating using a managed identity if you're building on top of Azure resources. Managed identities take care of all credential management for you.
- Use service connections: Service connections allow you to use service principals inside a pipeline. Use service connections whenever possible to securely connect to services without passing secret variables directly to builds. Restrict connections to specific use cases. for more information, see the [Scope service connections](#) section in this article.
  - Authenticate with Azure resources using [workload identity federation](#) with either an app registration or managed identity instead of using an app registration with a secret.

While a service account remains in use:

- Create single-purpose service accounts: Each service should have its dedicated account to minimize risk. Avoid using regular user accounts as [service accounts](#).
- Identify and disable unused service accounts: Regularly review and identify accounts no longer in use. Disable unused accounts before considering deletion.
- Restrict privileges: Limit service account privileges to the minimum necessary. Avoid interactive sign-in rights for service accounts.
- Use separate identities for report readers: If using domain accounts for service accounts, use a different identity for report readers to [isolate permissions and prevent unnecessary access](#).
- Use local accounts for workgroup installations: When installing components in a workgroup, use local accounts for user accounts. Avoid domain accounts in this scenario.
- Monitor service account activity: Implement auditing and create [audit streams](#) to monitor service account activity.

## Scope service connections

To ensure secure and efficient access to Azure resources, properly scope service connections. Service connections allow Azure DevOps to connect to external services and resources, and by

scoping these connections, you can limit access to only the necessary resources and reduce the risk of unauthorized access.

- **Limit access:** Limit access by scoping your [Azure Resource Manager](#) service connections to specific resources and groups. Don't grant broad contributor rights across the entire Azure subscription.
- **Use Azure Resource Manager:** Authenticate with Azure resources using workload identity federation with either an app registration or managed identity instead of using an app registration with a secret. For more information, see [Create an Azure Resource Manager service connection that uses workload identity federation](#).
- **Scope resource groups:** Ensure resource groups contain only the Virtual Machines (VMs) or resources needed for the build process.
- **Avoid classic service connections:** Opt for modern Azure Resource Manager service connections instead of classic ones, which lack scoping options.
- **Use purpose-specific team service accounts:** Authenticate service connections using purpose-specific team service accounts to maintain security and control.

For more information, see [Common service connection types](#).

## Review auditing events

Auditing can be used to track user actions, permissions changes, and usage patterns within your organization. Use these tools to identify and address potential security incidents promptly.

- **Enable auditing:** Track and view events related to user actions, permissions, changes, and security incidents.
- **Review audit logs and streams regularly:** Regularly review audit logs to monitor user activities and detect any suspicious behavior. Look for unexpected usage patterns, especially by administrators and other users. This action helps identify potential security breaches and takes corrective actions. Learn more about the [auditing events we track](#).
- **Configure security alerts:** Configure alerts to notify you of any security incidents or policy violations. This action ensures timely response to potential threats.

## Secure your services

To ensure the security and integrity of your services in Azure DevOps, implement security measures for each service. These measures include setting permissions, managing access, and using security features specific to each service.

- **Secure Azure Boards:** Protect your work tracking data by setting appropriate permissions and managing access levels.
  - [Set work tracking permissions](#)
  - [Set permissions for queries and query folders](#)
  - [Manage team administrators](#)
  - [Learn about default permissions and access levels for Azure Boards](#)
- **Secure Azure Repos:** Ensure the security of your code repositories by configuring Git settings, branch permissions, and policies.
  - [Learn about default Git settings and policies](#)
  - [Set permissions for a specific branch](#)
  - [Set branch policies](#)
  - [Configure GitHub Advanced Security for Azure DevOps](#)
  - [Learn about GitHub Advanced Security](#)
- **Secure Azure Pipelines:** Safeguard your CI/CD processes by setting permissions, using security templates, and securing agents and containers.
  - [Learn about Azure Pipelines security](#)
  - [Add users to Azure Pipelines](#)
  - [Use templates for security](#)
  - [Secure agents, projects, and containers](#)
  - [Secure access to Azure Repos from pipelines](#)
  - [Secure pipelines resources](#)
  - [Determine your approach for securing YAML pipelines](#)
  - [Protect secrets in Azure Pipelines](#)
- **Secure Azure Test Plans:** Ensure that your team has the appropriate access to efficiently manage and execute test plans.
  - [Learn default manual test and access permissions](#)
  - [Set permissions and access for testing](#)
- **Secure Azure Artifacts:** Manage access to your packages and control who can interact with them.
  - [Manage Azure Artifacts permissions](#)
  - [Set feed scopes](#)

## Automate security scanning

Monitor for code and secret vulnerabilities with the following automated security tools built by our partner teams:

- **Use code scanning and analysis:** Utilize tools like [Microsoft Defender](#) to scan your code for vulnerabilities, secrets, and misconfigurations. This action helps identify and remediate security issues early in the development process.

- **Use Azure DevOps Credential Scanner (CredScan) for GitHub:** When using a managed identity isn't an option, ensure that credentials get stored in secure locations such as Azure Key Vault, instead of embedding them into the code and configuration files. Implement Azure DevOps Credential Scanner to identify credentials within the code. For more information, see [Getting started with CredScan](#).
- **Use native secret scanning for GitHub:** When using a managed identity isn't an option, ensure that secrets get stored in secure locations such as Azure Key Vault, instead of embedding them into the code and configuration files. Use the native secret scanning feature to identify secrets within the code. For more information, see [About secret scanning](#).

For more information, see the [GitHub advanced security overview](#).

## Related articles

- [Data locations for Azure DevOps](#)
- [Microsoft Security Development Lifecycle](#)
- [Azure Trust Center](#)

# Plan your organizational structure

Article • 02/05/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Use your business structure as a guide for the number of organizations, projects, and teams that you create in Azure DevOps. This article helps you plan for different structures and scenarios for Azure DevOps.

Consider the following structures for your business and collaborative work in Azure DevOps:

- [Number of organizations](#)
- [Number of projects under an organization](#)

Also, plan for the following scenarios:

- [Map your organizations and projects](#) in Azure DevOps to your enterprise, business unit, and team structure
- [Structure your repositories \(repos\)](#)
- [Structure your teams](#)- it can either help or hinder teams to be Agile and autonomous
- [Manage access to data](#) - who needs to have access and who doesn't?
- [Reporting needs](#)
- Promote common practices - [use foundational elements to create an agile mindset and culture](#)

Have at least one organization, which might represent your company, your larger collection of code projects, or even multiple related business units.

## What's an organization?

An organization in Azure DevOps is a mechanism for organizing and connecting groups of related projects. Examples include business divisions, regional divisions, or other enterprise structures. You can choose one organization for your entire company, one organization for yourself, or separate organizations for specific business units.

Each organization gets its own *free tier* of services (up to five users for each service type) as follows. You can use all the services, or choose only what you need to complement your existing workflows.

- [Azure Pipelines](#): One hosted job with 1,800 minutes per month for CI/CD and one self-hosted job
- [Azure Boards](#): Work item tracking and boards
- [Azure Repos](#): Unlimited private Git repos

- [Azure Artifacts](#) : Package management
- Unlimited Stakeholders
  - First five users free (Basic license)
- **Azure Pipelines:**
  - One [Microsoft-hosted CI/CD](#) (one concurrent job, up to 30 hours per month)
  - One self-hosted CI/CD concurrent job
- **Azure Boards:** Work item tracking and boards
- **Azure Repos:** Unlimited private Git repos
- **Azure Artifacts:** Two GiB free per organization

 **Note**

The Azure DevOps cloud-based load testing service is deprecated, but [Azure Load Testing](#) remains available. This fully managed load testing service allows you to generate high-scale load using your existing Apache JMeter scripts. For more information, see [What is Azure Load Testing?](#) and [Changes to load test functionality in Visual Studio and cloud load testing in Azure DevOps](#).

## How many organizations do you need?

Start with one organization in Azure DevOps. Then, you can add more organizations—which may require different security models—later. A single code repo or project only needs one organization. If you have separate teams that need to work on code or other projects in isolation, consider creating separate organizations for those teams. They'll have different URLs. Add projects, teams, and repos, as necessary, before you add another organization.

Take some time to review your work structure and the different business groups and participants to be managed. For more information, see [Map your projects to business units](#) and [Structure considerations](#).

 **Tip**

For company-owned Microsoft Entra organizations, consider restricting users from creating new organizations as a way to protect your IP. For more information, see [Restrict organization creation via Microsoft Entra tenant policy](#). Users can create organizations using their MSA or GitHub accounts with no restrictions.

## What's a team?

A team is a unit that supports many [team-configurable tools](#). These tools help you plan and manage work, and make collaboration easier.

## Create a team for each distinct product or feature team

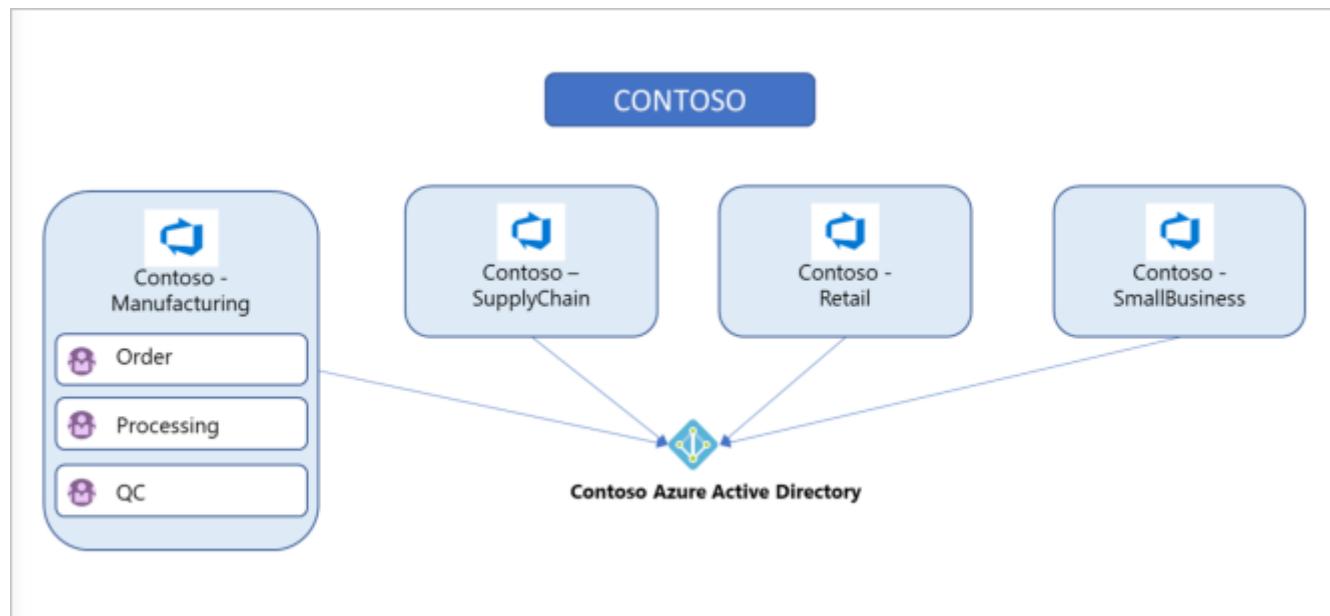
Each team owns their own backlog. To create a new backlog, you create a new team. [Configure teams and backlogs into a hierarchical structure](#), so program owners can more easily track progress across teams, manage portfolios, and generate rollup data. A team group gets created when you create a team. You can use this group in queries or to set permissions for your team.

## What's a project?

A project in Azure DevOps contains the following set of features:

- Boards and backlogs for agile planning
  - Pipelines for continuous integration and deployment
  - Repos for version control and management of source code and artifacts
  - Continuous test integration throughout the project life cycle
- Each organization contains one or more projects

In the following image, the fictitious Contoso company has four projects within their Contoso-Manufacturing organization.



## How many projects do you need?

Have at least one project to start using an Azure DevOps service, such as Azure Boards, Azure Repos, or Azure Pipelines. When you create your organization, a default project gets created

for you. In your default project, there's a code repo to start working in, backlog to track work, and at least one pipeline to begin automating build and release.

Within an organization, you can do either of the following approaches:

- Create a single project that contains many repos and teams
- Create many projects, each with its own set of teams, repos, builds, work items, and other elements

Even if you have many teams working on hundreds of different applications and software projects, you can manage them within a single project in Azure DevOps. However, if you want to manage more granular security between your software projects and their teams, consider using many projects. At the highest level of isolation is an organization, where each organization is connected to a single Microsoft Entra tenant. A single Microsoft Entra tenant, however, can be connected to many Azure DevOps organizations.

#### Note

If the **Limit user visibility and collaboration to specific projects** preview feature is enabled for the organization, users added to the **Project-SScoped Users** group won't be able to access projects that they haven't been added to. For more information and important security-related call-outs, see [Manage your organization, Limit user visibility for projects and more](#).

## Single project

A single project puts all of the work at the same "portfolio" level for the entire organization. Your work has the same set of repos and iteration paths. With a single project, teams share source repos, build definitions, release definitions, reports, and package feeds. You might have a large product or service that's managed by many teams. Those teams have tight inter-dependencies across the product life cycle. You create a project and divide the work using teams and area paths. This setup gives your teams visibility into each other's work, so the organization stays aligned. Your teams use the same taxonomy for work item tracking, making it easier to communicate and stay consistent.

#### Tip

When multiple teams work on the same product, having all teams on the same iteration schedule helps keep your teams aligned and delivering value on the same cadence. For example, our organization in Azure DevOps has over 40 feature teams and 500 users

within a single project - this works well because we're all working on a common product set with common goals and a common release schedule.

A high volume of queries and boards can make it hard to find what you're looking for. Depending on the architecture of your product, this difficulty can bleed into other areas such as builds, releases, and repos. Make sure to use good naming conventions and a simple folder structure. When you add a repo to your project, consider your strategy and determine whether that repo could be placed into its own project.

## Many projects

You can best determine project structure by how you ship the product. Having several projects shifts the administration burden and gives your teams more autonomy to manage the project as the team decides. It also provides greater control of security and access to assets across the different projects. Having team independence with many projects creates some alignment challenges, however. If each project is using a different process or iteration schedule, it can make communication and collaboration difficult if the taxonomies aren't the same.

### Tip

If you use the same process and iteration schedules across all your projects, your ability to roll-up data and report across teams improves.

Azure DevOps provides cross-project experiences for managing work.

You may want to add another project due to the following scenarios:

- To prohibit or manage access to the information within a project
- To support custom work tracking processes for specific business units within your organization
- To support entirely separate business units that have their own administrative policies and administrators
- To support testing customization activities or adding extensions before rolling out changes to the working project

When you're considering many projects, keep in mind that Git repo portability makes it easy to migrate repos (including full history) between projects. Other history can't be migrated between projects. Examples are push and pull request history.

When you map projects to business units, your company gets a single organization and sets up many projects with one or more projects representing a business unit. All Azure DevOps assets

of the company are contained within this organization and located within a given region (for example, Western Europe). Consider the following guidance for mapping your projects to business units:

[+] [Expand table](#)

	One project, many teams	One organization, many projects, and teams	Many organizations
<b>General guidance</b>	Best for smaller organizations or larger organizations with highly aligned teams.	Good when different efforts require different processes.	Useful as part of TFS legacy migrations and for hard security boundaries between organizations. Used with multiple projects and teams within each organization.
<b>Scale</b>	Supports tens of thousands of users and hundreds of teams, but best at this scale if all teams are working on related efforts.	Same as with one project, but many projects may be easier.	
<b>Process</b>	Aligned processes across teams; team flexibility to customize boards, dashboards, and so on.	Independent processes for each project. For example, different work item types, custom fields, and so on.	Same as many projects.
<b>Collaboration</b>	Highest default visibility and reuse between work and assets of different teams.	Good visibility and reuse are possible, but it's easier to hide assets between projects whether intentional.	Poor visibility, collaboration, and reuse between organizations.
<b>Roll-up reporting and portfolio management</b>	Best ability to roll up across teams and coordinate between teams.	Good reporting possible across projects. More difficult for cross-project roll-up and team coordination.	No roll-up or coordination between organizations.

	One project, many teams	One organization, many projects, and teams	Many organizations
Security/isolation	Can lock down assets at a team level, but default is open visibility and collaboration.	Better ability to lock down between projects. By default, provides good visibility within projects and good isolation across projects.	Hard boundaries across organizations; excellent isolation and minimal ability to share across organizations.
Context switching	Easiest for teams to work together and for users to switch between efforts.	Relatively easy for users to work together and switch contexts between efforts.	More difficult for users having to work across different organizations.
Information overload	By default, all assets are visible to users who make use of "favorites" and similar mechanisms to avoid "information overload."	Reduced risk of information overload; most project assets hidden across project boundaries.	Assets across organizations are isolated, reducing risk of information overload.
Administrative overhead	Much administration is delegated down to individual teams. Easiest for user licensing and org-level administration. More work may be needed if alignment is required between efforts.	More administration at the project level. More overhead, but can be useful when projects have different administrative needs.	As with more projects, there's more administrative overhead, which enables more flexibility between orgs.

## Structure repos and version control within a project

Consider the specific strategic work scoped to one of the organizations you created previously and who needs access. Use this information to name and [create a project](#). This project has a URL defined under the organization you created it in and can be accessed at <https://dev.azure.com/{organization-name}/{project-name}>.

Configure your project in [Project settings](#).

The screenshot shows the Azure DevOps Project Overview page for the 'FabrikamFiber' project. The left sidebar contains navigation links: 'Overview', 'Summary', 'Dashboards', 'Wiki', 'Boards', 'Repos', 'Pipelines', 'Test Plans', 'Artifacts', and 'Project settings'. The 'Project settings' link is highlighted with a red box. The main content area features a large 'Welcome to the project!' message with a cartoon illustration of a person working at a desk with a dog. Below the welcome message are several service links: 'Boards', 'Repos', 'Pipelines', 'Test Plans', and 'Artifacts'. A link to 'or manage your services' is also present. At the top right, there are 'Private' and 'Invite' buttons.

For more information about managing projects, see [Manage projects in Azure DevOps](#). You can move a project to a different organization by migrating the data. For more information about migrating your project, see the [Migration overview](#).

## Manage version control

In projects where the Azure Repos service is enabled, version control repos can store and revise code. Consider the following options when you're configuring repos.

### Git vs. Team Foundation Version Control (TFVC)

Azure Repos offers the following version control systems for teams to choose from:

- Git and TFVC. Projects can have repos of each type. By default, new projects have an empty Git repo. Git enables a great amount of flexibility in developer workflows and integrates with nearly every relevant tool in the developer ecosystem. Any project can use Git repos. There's no limit on the amount of Git repos that can be added to a project.

TFVC is a centralized version control system that is also available. Unlike Git, only one TFVC repository is allowed for a project. But, within that repo, folders, and branches are used to organize code for multiple products and services, if wanted. Projects can use both TFVC and Git, if appropriate.

## Monorepo vs. one repo per service

Deploying various independent services from a monorepo can be effective for small teams aiming to build early momentum. However, this strategy can become problematic as the team grows due to several factors:

- The knowledge required for new members increases with the overall complexity of the system.
- Code sharing within a single repository can result in unintended coupling between services.
- Changes in shared code can impact the behavior of various services, making it challenging to track these changes.

For larger teams, managing a monorepo necessitates strong engineering discipline and robust tooling. Alternatively, you can opt for individual repositories for each service, along with a separate repo for shared resources. Although this approach involves more initial setup, it scales more effectively as the team grows. It also makes onboarding easier for new members, who can concentrate solely on their specific service repo.

If you're starting with a small team, a monorepo can be a good choice. As your team expands and complexity rises, you can transition to separate repositories.

## One vs. many repos within a project

Do you need to set up multiple repos within a single project or have a repo set up per project? The following guidance relates to the planning and administration functions across those repos.

One project containing multiple repos works well if the products/services are working on a coordinated release schedule. If developers are frequently working with multiple repos, keep them in a single project to ensure the processes remain shared and consistent. It's easier to manage repo access within a single project, as access controls and options like case

enforcement and max file size get set at the project level. You can manage the access controls and settings individually, even if your repos are in a single project.

If the products stored in multiple repos work on independent schedules or processes, you can split them into multiple projects. Git repo portability makes it easy to move a repo between projects and still keep full-fidelity commit history. Other history, such as pull requests or build history, aren't easily migrated.

Base your decision for one vs. many repos on the following factors and tips:

- Code dependencies and architecture
- Put each independently deployable product or service in its own repo
- Don't separate a codebase into many repos if you expect to make coordinated code changes across those repos, as no tools can help coordinate those changes
- If your codebase is already a monolith, keep it in one repo. For more information about monolithic repos, see [How Microsoft develops modern software with DevOps](#) articles
- If you have many disconnected services, one repo per service is a good strategy

### Tip

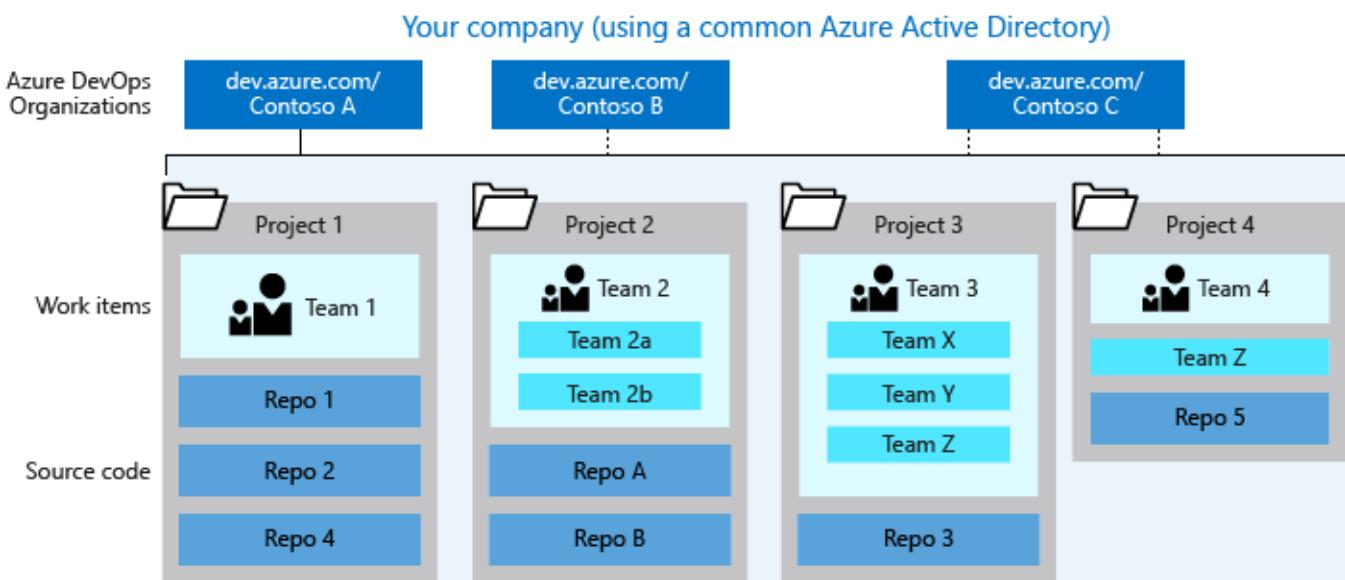
Consider [managing your permissions](#), so not everyone in your organization can [create a repo](#). If you have too many repos, it's hard to keep track of who owns which code or other content stored in those repos.

## Shared repo vs. forked repos

We recommend using a shared repo within a trusted organization. Developers use branches to maintain isolation of their changes from one another. With a good branching and release strategy, a single repo can scale to support concurrent development for more than a thousand developers. For more information about branching and release strategy, see [Adopt a Git branching strategy and Release Flow: Our Branching Strategy](#).

Forks can be useful when you're working with vendor teams that shouldn't have direct access to update the main repository. Forks can also be useful in scenarios where many developers contribute infrequently, such as in an open-source project. When you're working with forks, you may want to maintain a separate project to isolate the forked repos from the main repo. There may be added administrative overhead, but it keeps the main project cleaner. For more information, see the [Forks article](#).

The following image displays a sample of how "your company" could structure its organizations, projects, work items, teams, and repos.



## Managing temporary and shared resources

Consider how to manage temporary and shared resources effectively by employing the following best practices:

- **Temporary environments:** Temporary environments are short-lived and used for tasks such as testing, development, or staging. To manage these environments efficiently:
  - **Separate repositories and pipelines:** Each temporary environment and its associated resources, for example, Azure Functions, should have its own repository and pipeline. This separation allows you to deploy and roll back the environment and its resources simultaneously, making it easier to spin up and discard them as needed.
  - **Example:** Create a repository and pipeline specifically for your development environment, including all necessary resources such as Azure Functions, storage accounts, and other services.
- **Shared resources:** Shared resources are typically long-lived and used across multiple environments. These resources often have longer spin-up times and higher costs. To manage shared resources effectively:
  - **Separate repositories and pipelines:** Shared resources, such as Azure SQL Database, should have their own repository and pipeline. This separation ensures that temporary environments can use these shared resources, making their deployments faster and more cost-effective.
  - **Example:** Create a repository and pipeline for your Azure SQL Database, which can be used by multiple temporary environments.
- **Shared infrastructure resources:** Shared infrastructure resources, such as Virtual Private Clouds (VPCs) and subnets, also known as landing zones, should also have their own repositories and pipelines. This approach ensures that your infrastructure is managed consistently and can be reused across different environments.

- **Example:** Create a repository and pipeline for your VPC and subnet configuration, which can be referenced by other repositories and pipelines.

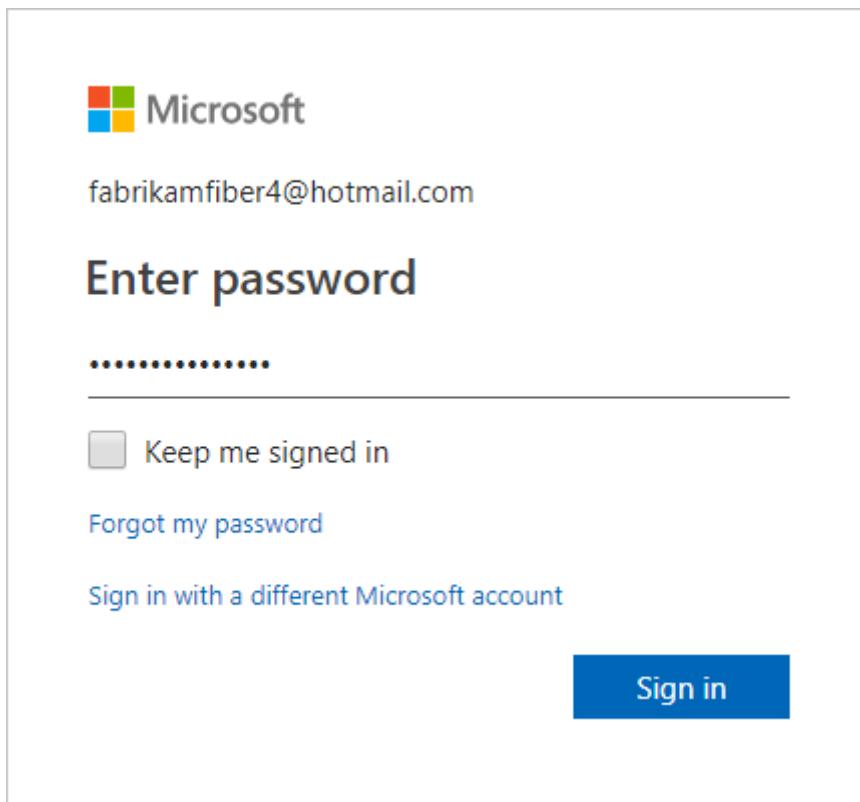
## More about organizational structure

### Choose your organization administrator account type

When you create an organization, the credentials that you sign in with define which identity provider your organization uses. Create your organization with a Microsoft account or Microsoft Entra instance. Use those credentials to sign in as an administrator to your new organization at <https://dev.azure.com/{YourOrganization}>.

### Use your Microsoft account

Use your Microsoft account if you don't need to authenticate users for an organization with Microsoft Entra ID. All users must sign in to your organization with a Microsoft account. If you don't have one, [create a Microsoft account](#).



If you don't have a Microsoft Entra instance, create one for free from the [Azure portal](#) or use your Microsoft account to create an organization. Then, you can [connect your organization to Microsoft Entra ID](#).

### Use your Microsoft Entra account

You might have a Microsoft Entra account already if you use Azure or Microsoft 365. If you work for a company that uses Microsoft Entra ID to manage user permissions, you probably have a Microsoft Entra account.

If you don't have a Microsoft Entra account, [sign up for Microsoft Entra ID](#) to automatically connect your organization to your Microsoft Entra ID. All users must be members in that directory to access your organization. To add users from other organizations, use [Microsoft Entra B2B collaboration](#).

Azure DevOps authenticates users through your Microsoft Entra ID, so that only users who are members in that directory have access to your organization. When you remove users from that directory, they can no longer access your organization. Only specific [Microsoft Entra administrators](#) manage users in your directory, so administrators control who accesses your organization.

For more information on managing users, see [Manage users](#).

## Map organizations to business units

Each business unit within your company gets its own organization in Azure DevOps, along with its own Microsoft Entra tenant. You can [set up projects](#) within those individual organizations, as required, based on teams or ongoing work.

For a larger company, you can create multiple organizations using different user accounts (most likely Microsoft Entra accounts). Consider what groups and users share strategies and work, and group them into specific organizations.

For example, the fictional Fabrikam company created the following three organizations:

- Fabrikam-Marketing
- Fabrikam-Engineering
- Fabrikam-Sales

Each organization has a separate URL, such as:

- <https://dev.azure.com/Fabrikam-Marketing>
- <https://dev.azure.com/Fabrikam-Engineering>
- <https://dev.azure.com/Fabrikam-Sales>

The organizations are for the same company, but are mostly isolated from each other. You don't need to separate anything this way. Only create boundaries when it makes sense to your business.



Tip

You can more easily partition an existing organization with projects, than combine different organizations.

## Related articles

- [Create an organization](#)
- [Create a project](#)
- [Connect your organization to Microsoft Entra ID](#)
- [Set up billing](#)
- [Set user preferences](#)

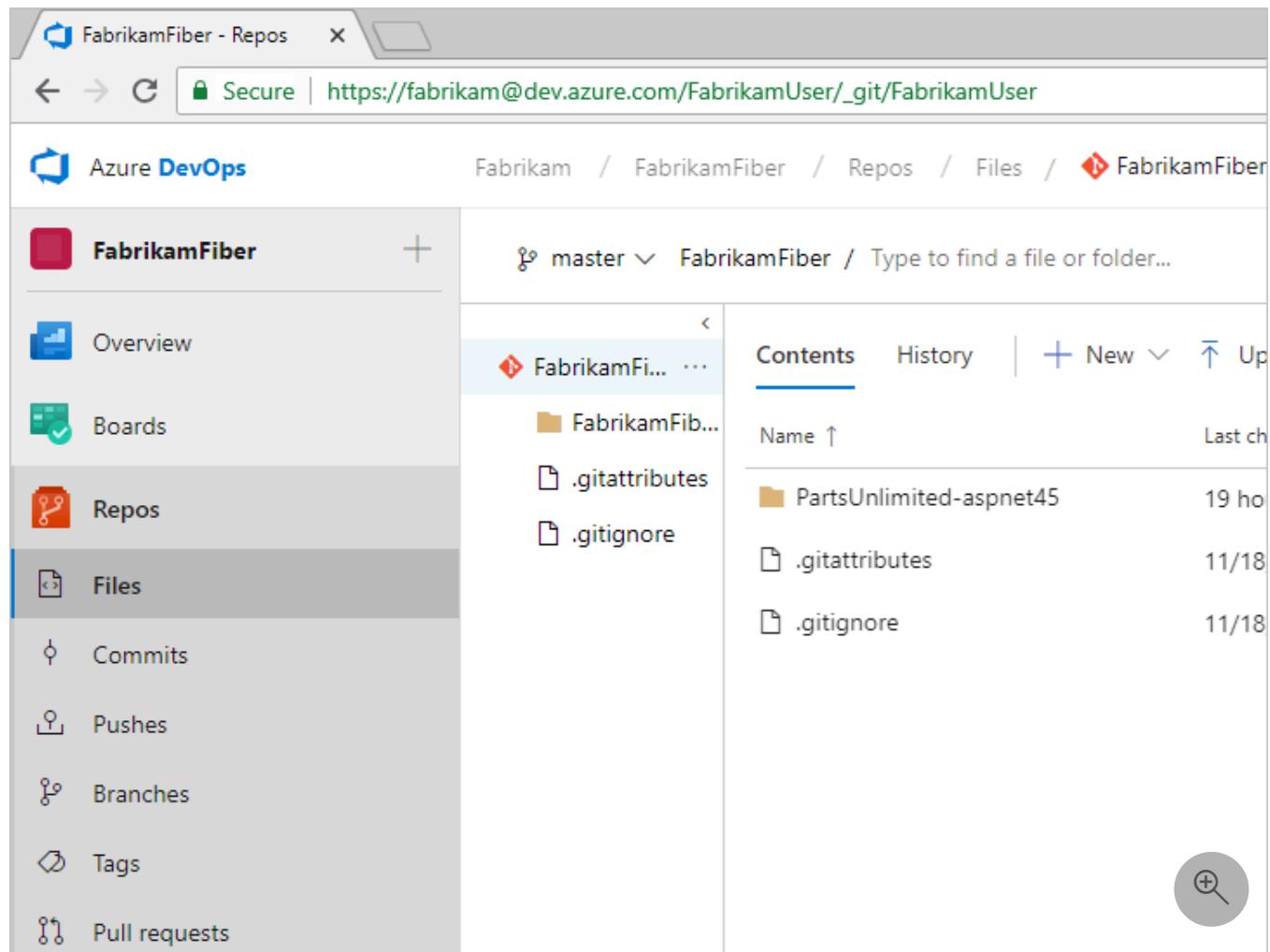
# What is source control?

Article • 04/23/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

A source control system (also called a *version control system*) allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.

Azure DevOps supports two types of source control: Git (distributed) and Team Foundation Version Control (TFVC). TFVC is a centralized, client-server system. In both Git and TFVC, you can check in files and organize files in folders, branches, and repositories. You can manage your repositories, branches, and other code development operations from **Azure Repos**.



The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' repository. The left sidebar has a navigation menu with items: Overview, Boards, **Repos**, Files, Commits, Pushes, Branches, Tags, and Pull requests. The 'Repos' item is currently selected. The main content area shows the 'master' branch of the 'FabrikamFiber' repository. It displays files: '.gitattributes' and '.gitignore'. There is also a folder named 'PartsUnlimited-aspnet45'. At the top of the main area, there is a search bar with the placeholder 'Type to find a file or folder...'. Below the search bar, there are tabs for 'Contents' (which is selected), 'History', and buttons for '+ New' and 'Up'.

## Compare Git and TFVC

With Git, each developer has a copy of the source repository on their development machine. The source repo includes all branch and history information. Each developer works directly with their local repo and changes are shared between repos as a separate step.

Developers can commit each set of changes and perform version control operations, such as history and compare without a network connection. Branches are lightweight. When

developers need to switch contexts, they create a private local branch. Developers can quickly switch from one branch to another to pivot among different variations of the code base. Later, developers can merge, publish, or dispose of the branch.

With TFVC, developers have only one version of each file on their dev machines. Historical data is maintained only on the server. Branches are path-based and are created on the server.

## Get started with Git for source control

Start sharing your code or get your code by using [source control with Git](#).

 **Note**

Git in Visual Studio and Azure DevOps is standard Git. You can use Visual Studio with third-party Git services. You can also use third-party Git clients with Azure DevOps Server.

## Related content

- [Azure Repos documentation](#)
- [Git repositories documentation](#)

# Software development roles supported by Azure DevOps

Article • 07/24/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

If you're a sole developer or work in a small setting, you track issues, plan features, code, test, build, and deploy.

If you work in a large setting, you might be more focused on a specific set of tasks that aligns with specific roles. These specific roles could be software development, product and scrum management, or DevOps.

The following article describes the features and tasks available to you, based on your role.

## Contributor roles

Team members are contributors who have access to the following areas and more:

- code base
- work item tracking
- Agile tools
- build pipelines
- test tools

If you need to lock down specific areas to a select set of contributors, see [permission management](#).

## Software developers

Developers use Visual Studio or other [tools](#) to develop their applications. They then check in their changes to a Git or Team Foundation Version Control (TFVC) repository hosted in Azure DevOps. From the web portal or a supported IDE, they can view repositories, check history, and more.

To get started with using Git, see one of the following resources:

- [Share your code with Git and Visual Studio](#)
- [Share your code in Git by using Eclipse](#)
- [Share your code in Git by using Xcode](#)

- [Share your code in Git by using IntelliJ](#)
- [Get started with using Git and Azure DevOps Services](#)

To get started with using TFVC, see one of the following resources:

- [Develop and share your code in TFVC by using Visual Studio](#)
- [Share your code in TFVC by using Eclipse](#)
- [Share your code in TFVC by using Xcode](#)

## Product owners

Product owners typically plan the feature set to deliver, set priorities, and track the status of work, code defects, and customer issues. The suite of web-based Agile tools in Azure DevOps provides product owners with the views and features that they need to do these tasks. All work gets captured within a work item. Each work item represents a specific type such as a user story, task, or bug.

- Use the product backlog to quickly define and prioritize user stories, features, and other work items
- Use the sprint backlog and task board to implement Scrum practices
- Use your board to work with Kanban methods
- Use queries to list and update work items, create status and trend charts, and post charts to dashboards
- Use dashboards to share information, status, and trends with your team or organization

For more information about getting started, see [About Azure Boards and Agile tools](#).

You can integrate Microsoft Excel with Azure DevOps to plan and track your work. For more information, see [Bulk modify by using Excel](#).

## Scrum masters

Scrum masters help to facilitate scrum to the larger team by ensuring the scrum framework gets followed. They're committed to the practices, but stay flexible and open to opportunities for the team to improve their workflow. Scrum masters utilize the same features as [product owners](#).

## DevOps: builders, testers, and release managers

An advantage of working with Azure DevOps is the suite of tools and integrated functionality that support build, testing, and deploying software applications. See the

following general DevOps-associated tasks that Azure DevOps supports.

- Define builds
- Unit test your code
- Run tests with your builds
- Perform exploratory tests
- Define, manage, track, and approve releases
- Deploy applications to Azure, a virtual machine, Docker containers, and more

To get started, see the overviews in [Azure Pipelines](#) and [Azure Test Plans](#).

## Stakeholders

With Stakeholder access, anyone in your organization can check project status and provide feedback. Stakeholders can track project priorities and provide direction, feature ideas, and business alignment to a team. Stakeholders also contribute to plans by adding and modifying work items. They can't, however, contribute to the code base or exercise test tools.

Stakeholder access essentially provides free access to a limited set of feature to project sponsors and supporters. For more information, see [Work as a Stakeholder](#).

## Administrator roles

A distinct advantage to working in Azure DevOps Services is the reduced overhead of server maintenance. But there are several administrative tasks required to support a collaborative, integrated software development environment.

The main tasks are grouped as follows by membership in a security group or role.

### Team administrators

Responsible for configuring team settings, which include:

- Backlog and board settings
- Team areas and iterations (sprints)
- Team members
- Team dashboards
- Team work item templates
- Team alerts

To get started, see [Manage teams and configure team tools](#).

# Project administrators

Responsible for configuring project-level resources, including:

- Area paths and iteration paths
- Project permissions and repository security
- Build agents, pools, and service connections
- Test and release retention policies

## Organization owners and Project Collection Administrators

Organization owners are automatically members of the Project Collection Administrators group. Responsible for configuring organization-level resources, including the following tasks:

- Manage billing
- Add and manage projects
- Manage collection-level permissions
- Customize work tracking processes
- Install and manage extensions

To get started, see [Manage organizations](#) and [Settings](#).

## Related articles

- [A tour of services](#)
- [Plan your organizational structure in Azure DevOps](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Troubleshoot connecting to a project

Article • 02/05/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

If you're experiencing issues connecting to a project in Azure DevOps, follow these troubleshooting steps to resolve common connectivity problems.

## Prerequisites

 Expand table

Category	Requirements
Project access	Project member.

## Troubleshoot connectivity

To resolve connectivity issues, complete the following steps:

1. Sign out of your browser. To do so, select the [Visual Studio sign out](#) link.
2. Delete the cookies in your browser. To delete cookies in most browsers, select **Ctrl+Shift+Delete**.
3. Open Microsoft Edge and delete the browser cookies. The Visual Studio IDE uses Microsoft Edge cookies.
4. Close all browsers and close the Visual Studio IDE.
5. Use a private browser session to retry the connection. If the issue is with the Visual Studio IDE, remove the connection and then readd it in Team Explorer.

For more troubleshooting options, see [Switch organizations](#), further in this article.

## Troubleshoot sign in

Two types of identities can sign in: Microsoft accounts and Microsoft Entra accounts. Depending on your account, you might experience the following error.

### 401 - Not Authorized

# 401

## NOT AUTHORIZED

Sorry, but Jamal Hartnett <jamal@fabrikam.com> (Microsoft account) is not authorized to access this page

[Sign out and connect with another login](#)

Service Status and Support @AzureDevOps

The most common error page is the *401 Not Authorized* error, which occurs when your identity doesn't have permissions to enter an organization. See the following common reasons for the error:

- Your identity isn't a member of the organization.
- Your identity has an invalid or missing license assignment.
- Your identity doesn't have enough memberships to access the resource. For example, membership to the Reader/Contributors group.
- Your identity is a B2B guest in the tenant, and the invitation isn't accepted.

If you think you're a member of the organization, but get this error page, [contact Support](#).

## Scenario 1

Your work or school Microsoft Entra account doesn't have access, but your personal Microsoft account does.

401 - Work or school, or Personal account

# 401

## NOT AUTHORIZED

jamal@fabrikam.com has multiple accounts associated with it.

Your work or school account does not have access to dev.azure.com/Fabrikam, but **your personal account does have access**.

[Sign in with your personal account](#)

[Sign out and connect with another login](#)

Service Status and Support @AzureDevOps

A highly specific 401 error case. In this case, both a personal Microsoft account and a work or school account (Microsoft Entra ID) that have the same sign-in address exist. You signed in with your work or school account, but your personal account is the identity with access to the organization.

## Mitigation

In some cases, you might not know you have two identities with the same sign-in address. It's possible that an administrator created the work or school Microsoft Entra account when you were added to Office 365 or Microsoft Entra ID.

To sign out of your current work or school Microsoft Entra account, select **Sign in with your personal MSA account**, and then sign in by using your personal Microsoft account. After authentication, you should have access to the organization.

- If you can't access to the organization, make sure that your Microsoft Entra ID still exists and that your work or school account is in the Microsoft Entra tenant.

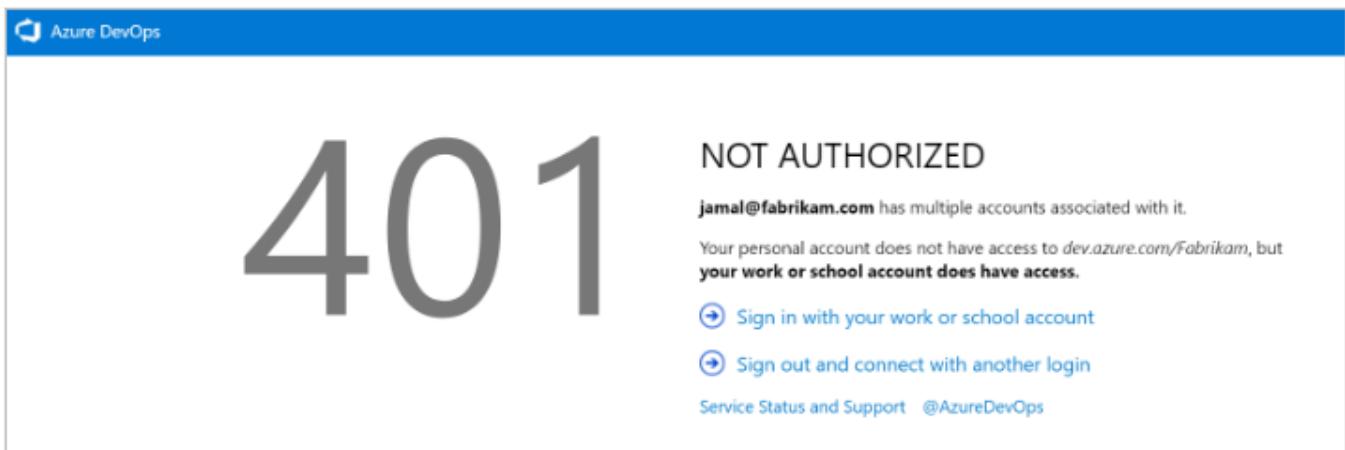
### 💡 Tip

To avoid seeing this prompt, you can rename your Microsoft account. Then, only one identity, your work or school account, or Microsoft Entra account, uses your sign-in address.

## Scenario 2

Your personal Microsoft account doesn't have access, but your Microsoft Entra account does. This scenario is an opposite version of the 401 error page. In this case, the personal account (Microsoft account identity) doesn't have access to the organization and the work or school account (Microsoft Entra identity) does. The same guidance from Scenario 1 applies, but in reverse.

### 401 - Work or school, or Personal account



## Mitigation

When you get redirected back to the original sign-in page, we recommend that you clear all cookies, and then reattempt to sign in. If that doesn't fix the issue, [contact Support](#).

## Unable to connect to Azure DevOps Services

 [Expand table](#)

Problem	Resolution
You don't have an active account or license.	Check with your administrator that you're a member of the account and have an active, valid license. For more information, see <a href="#">Assign licenses to users</a> .
Your Azure DevOps Services organization is connected to the Microsoft Entra ID.	When your Azure DevOps Services organization is connected to a directory that is associated with a Microsoft 365 or Microsoft Azure subscription, only members in the directory can access the account.  Check with your directory administrator to have them <a href="#">create an organizational account for you or add your account to the directory as external member</a> .
You can't switch between different organizational accounts.	If you work with several organizations that connect to different directories, such as accounts created from the Microsoft Azure portal, the sign out function might not work as expected. For example, you can't switch between different organizational accounts to connect to multiple accounts that are linked to directory tenants.  When this problem occurs, there's a flashing blank sign in dialog box. Then, you receive either TF31002 or TF31003 error after you connect to or add a new connection in the dialog box.  To resolve this problem, apply the most recent <a href="#">Visual Studio update</a> .  For more information, see <a href="#">You can't switch between different organizational accounts in Visual Studio Codespace</a> .
You want to sign in to Azure DevOps Services from Visual Studio using different credentials.	See <a href="#">Connect to projects, Sign in with different credentials</a> .

## Switch organizations

When you use two or more organizations that are linked to Microsoft Entra ID, the sign out function might not work as expected. For example, you can't switch between different organizations to connect to multiple organizations that are linked to directory tenants.

When this problem occurs, a blank screen flashes several times. Then, one of the following error messages appears after you connect to or add a new connection in the **Connect to Azure DevOps Server** dialog box:

TF31003: Either you have not entered the necessary credentials, or your user account does not have permission to connect to the Azure DevOps Server

TF31002: Unable to connect to this Azure DevOps Server

To resolve this issue, apply Visual Studio 2013.2 or install a later version from the [Visual Studio download website](#).

Another solution is to delete your browser cookies. For more information, see the support article [You can't switch between different organizations in Visual Studio Codespaces](#).

# Capture a browser trace for troubleshooting

Article • 02/05/2025

If you're troubleshooting an issue with Azure DevOps and need to contact [Microsoft Support](#), capture additional information such as a browser trace, step recording, and console output. This data provides important details about what is happening in Azure DevOps when the issue occurs.

A HAR (HTTP Archive) file tracks information between a web browser and a website. It contains detailed performance data about web pages, including resources loaded, time taken for each resource, and any errors encountered. Sharing a HAR file with Microsoft Support can help diagnose and resolve issues more effectively.

## Warning

Browser traces often contain sensitive information and might include authentication tokens linked to your identity. Remove any passwords before sharing traces with others. Handle these HAR files with care to ensure the security and privacy of the contained information. Microsoft support uses these traces for troubleshooting purposes only.

## Prerequisites

 [Expand table](#)

Category	Requirements
Project access	<a href="#">Project member</a> .

## Generate HAR file and record browser activity

You can capture this information from Microsoft Edge or Google Chrome. Steps for each browser are shown as follows.

Microsoft Edge

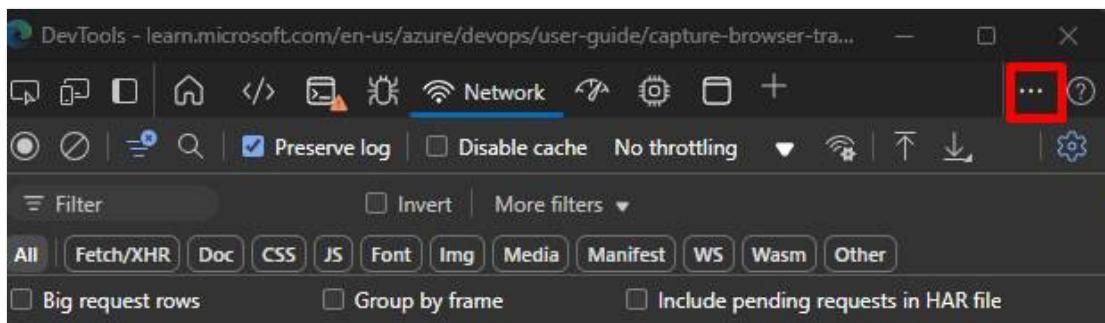
The following steps show how to use the developer tools in Microsoft Edge. For more information, see [Microsoft Edge DevTools](#).

### ! Note

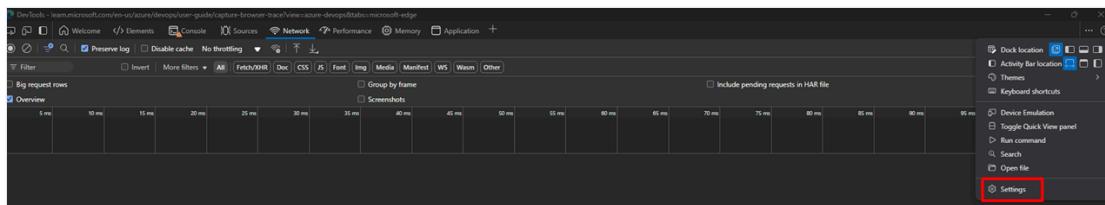
The screenshots in this article show the DevTools in Focus Mode with a vertical **Activity Bar**. Depending on your settings, your configuration might look different. For more information, see [Simplify DevTools using Focus Mode](#).

1. In your browser, select **F12 > Open DevTools**.

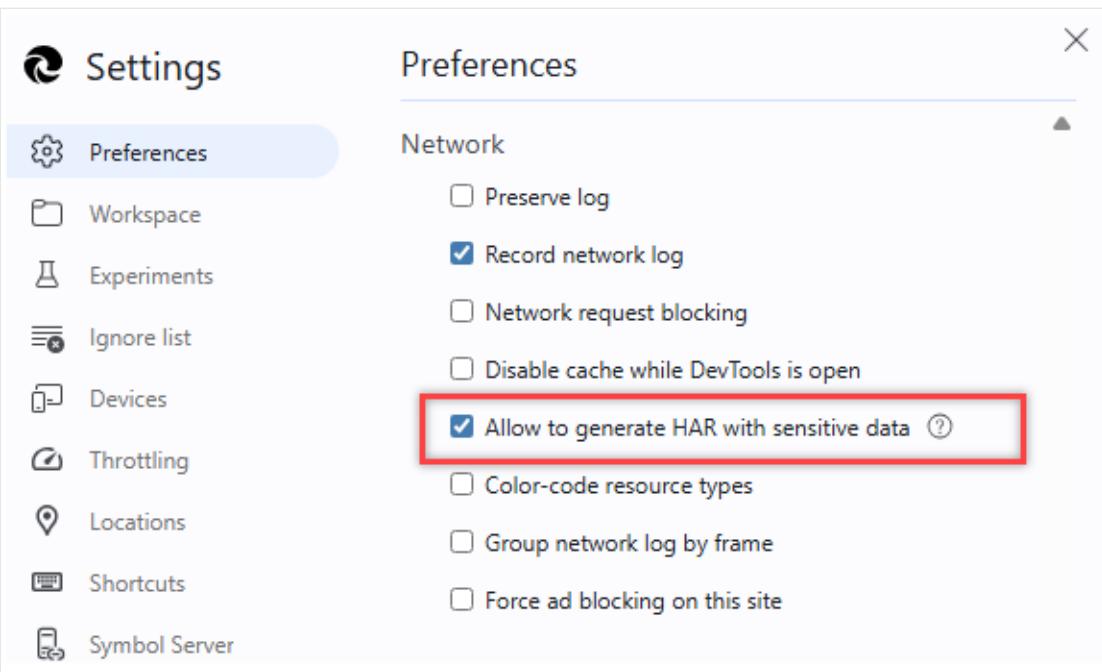
2. Select **... more actions**.



3. Select **Settings**.

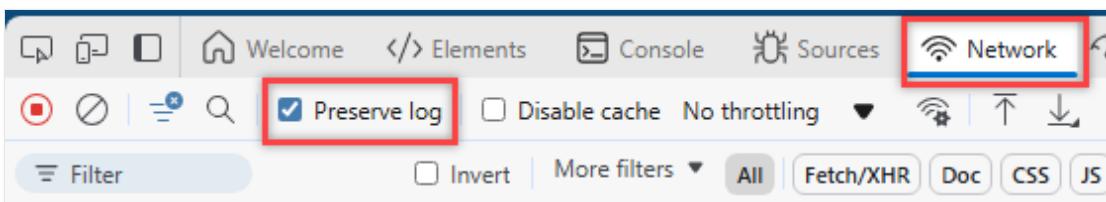


4. Under **Preferences**, scroll to the **Network** section and enter a check in the box next to **Allow to generate HAR with sensitive data**.



5. Close the settings menu.

6. Ensure the Network tab is set to Preserve log and is capturing traffic.

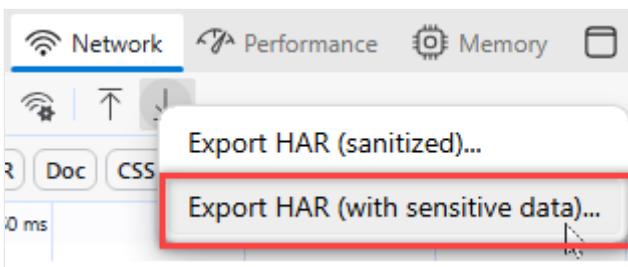


7. Go to the step before where the issue occurs.

8. Record the steps you take in Azure DevOps using [Steps Recorder](#). Steps Recorder doesn't automatically start recording HAR traces in DevTools, so make sure to start the recording in DevTools, too.

9. When you're done recording, stop recording in Step Recorder. In DevTools, stop recording and long press Export so that it shows a menu. If you only do a short press, a sanitized version of the HAR gets exported, which is missing information needed for troubleshooting.

10. Select Export HAR (with sensitive data).



11. (Optional) Uncheck the "Allow to generate HAR with sensitive data" box when you're done.

You have a complete HAR file with the necessary data for troubleshooting.

## Related articles

- [Access Azure DevOps troubleshooting documentation](#)
- [Get support and provide feedback](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Troubleshoot connecting to a project

Article • 02/05/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

If you're experiencing issues connecting to a project in Azure DevOps, follow these troubleshooting steps to resolve common connectivity problems.

## Prerequisites

 Expand table

Category	Requirements
Project access	Project member.

## Troubleshoot connectivity

To resolve connectivity issues, complete the following steps:

1. Sign out of your browser. To do so, select the [Visual Studio sign out](#) link.
2. Delete the cookies in your browser. To delete cookies in most browsers, select **Ctrl+Shift+Delete**.
3. Open Microsoft Edge and delete the browser cookies. The Visual Studio IDE uses Microsoft Edge cookies.
4. Close all browsers and close the Visual Studio IDE.
5. Use a private browser session to retry the connection. If the issue is with the Visual Studio IDE, remove the connection and then readd it in Team Explorer.

For more troubleshooting options, see [Switch organizations](#), further in this article.

## Troubleshoot sign in

Two types of identities can sign in: Microsoft accounts and Microsoft Entra accounts. Depending on your account, you might experience the following error.

### 401 - Not Authorized

# 401

## NOT AUTHORIZED

Sorry, but Jamal Hartnett <jamal@fabrikam.com> (Microsoft account) is not authorized to access this page

[Sign out and connect with another login](#)

Service Status and Support @AzureDevOps

The most common error page is the *401 Not Authorized* error, which occurs when your identity doesn't have permissions to enter an organization. See the following common reasons for the error:

- Your identity isn't a member of the organization.
- Your identity has an invalid or missing license assignment.
- Your identity doesn't have enough memberships to access the resource. For example, membership to the Reader/Contributors group.
- Your identity is a B2B guest in the tenant, and the invitation isn't accepted.

If you think you're a member of the organization, but get this error page, [contact Support](#).

## Scenario 1

Your work or school Microsoft Entra account doesn't have access, but your personal Microsoft account does.

401 - Work or school, or Personal account

# 401

## NOT AUTHORIZED

jamal@fabrikam.com has multiple accounts associated with it.

Your work or school account does not have access to dev.azure.com/Fabrikam, but **your personal account does have access**.

[Sign in with your personal account](#)

[Sign out and connect with another login](#)

Service Status and Support @AzureDevOps

A highly specific 401 error case. In this case, both a personal Microsoft account and a work or school account (Microsoft Entra ID) that have the same sign-in address exist. You signed in with your work or school account, but your personal account is the identity with access to the organization.

## Mitigation

In some cases, you might not know you have two identities with the same sign-in address. It's possible that an administrator created the work or school Microsoft Entra account when you were added to Office 365 or Microsoft Entra ID.

To sign out of your current work or school Microsoft Entra account, select **Sign in with your personal MSA account**, and then sign in by using your personal Microsoft account. After authentication, you should have access to the organization.

- If you can't access to the organization, make sure that your Microsoft Entra ID still exists and that your work or school account is in the Microsoft Entra tenant.

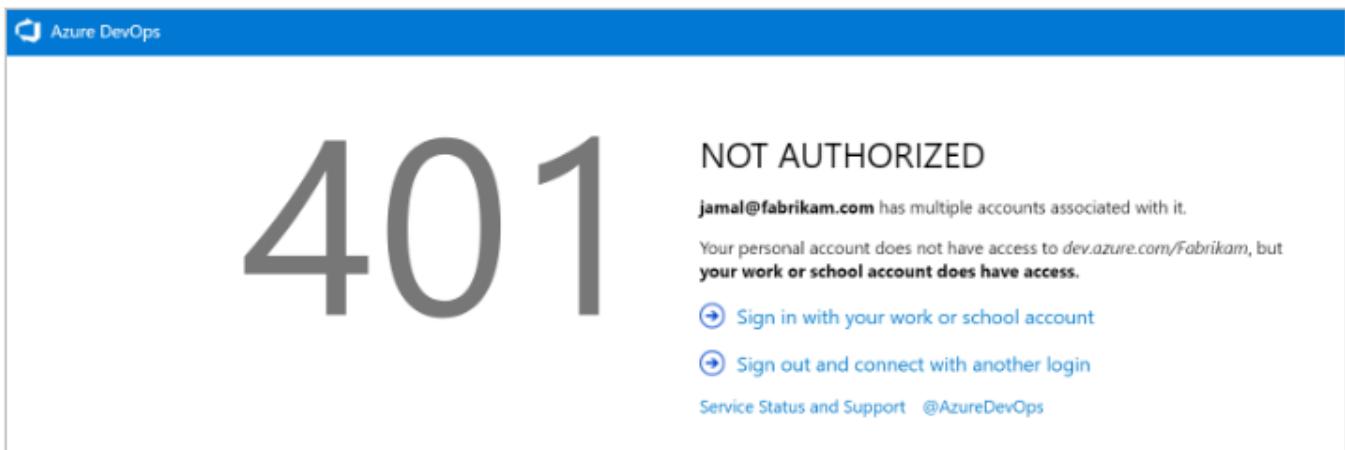
### Tip

To avoid seeing this prompt, you can rename your Microsoft account. Then, only one identity, your work or school account, or Microsoft Entra account, uses your sign-in address.

## Scenario 2

Your personal Microsoft account doesn't have access, but your Microsoft Entra account does. This scenario is an opposite version of the 401 error page. In this case, the personal account (Microsoft account identity) doesn't have access to the organization and the work or school account (Microsoft Entra identity) does. The same guidance from Scenario 1 applies, but in reverse.

### 401 - Work or school, or Personal account



## Mitigation

When you get redirected back to the original sign-in page, we recommend that you clear all cookies, and then reattempt to sign in. If that doesn't fix the issue, [contact Support](#).

## Unable to connect to Azure DevOps Services

 Expand table

Problem	Resolution
You don't have an active account or license.	Check with your administrator that you're a member of the account and have an active, valid license. For more information, see <a href="#">Assign licenses to users</a> .
Your Azure DevOps Services organization is connected to the Microsoft Entra ID.	When your Azure DevOps Services organization is connected to a directory that is associated with a Microsoft 365 or Microsoft Azure subscription, only members in the directory can access the account.  Check with your directory administrator to have them <a href="#">create an organizational account for you or add your account to the directory as external member</a> .
You can't switch between different organizational accounts.	If you work with several organizations that connect to different directories, such as accounts created from the Microsoft Azure portal, the sign out function might not work as expected. For example, you can't switch between different organizational accounts to connect to multiple accounts that are linked to directory tenants.  When this problem occurs, there's a flashing blank sign in dialog box. Then, you receive either TF31002 or TF31003 error after you connect to or add a new connection in the dialog box.  To resolve this problem, apply the most recent <a href="#">Visual Studio update</a> .  For more information, see <a href="#">You can't switch between different organizational accounts in Visual Studio Codespace</a> .
You want to sign in to Azure DevOps Services from Visual Studio using different credentials.	See <a href="#">Connect to projects, Sign in with different credentials</a> .

## Switch organizations

When you use two or more organizations that are linked to Microsoft Entra ID, the sign out function might not work as expected. For example, you can't switch between different organizations to connect to multiple organizations that are linked to directory tenants.

When this problem occurs, a blank screen flashes several times. Then, one of the following error messages appears after you connect to or add a new connection in the **Connect to Azure DevOps Server** dialog box:

TF31003: Either you have not entered the necessary credentials, or your user account does not have permission to connect to the Azure DevOps Server

TF31002: Unable to connect to this Azure DevOps Server

To resolve this issue, apply Visual Studio 2013.2 or install a later version from the [Visual Studio download website](#).

Another solution is to delete your browser cookies. For more information, see the support article [You can't switch between different organizations in Visual Studio Codespaces](#).

# Troubleshoot access and permission issues

Article • 02/10/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Due to the extensive security and permission structure of Azure DevOps, you might need to investigate why a user lacks access to a project, service, or feature they expect. Find step-by-step guidance to understand and address issues a user might encounter when connecting to a project or accessing an Azure DevOps service or feature.

## Prerequisites

[+] Expand table

Category	Requirements
Permissions	To manage permissions or groups at the organization or collection level: Member of the <a href="#">Project Collection Administrators security group</a> . If you created the organization or collection, you're automatically a member of this group.
Recommendation	Before using this guide, we recommend getting familiar with the following content: <ul style="list-style-type: none"><li>- <a href="#">Get started with permissions, access, and security groups</a></li><li>- <a href="#">Default permissions and access quick reference</a>.</li></ul>

### 💡 Tip

When you create an Azure DevOps security group, label it clearly to indicate whether it's intended to limit access.

You can set permissions at the following levels:

- Object level
- Project level
- Organization or project collection level
- Security role
- Team administrator role

# Common access and permission issues

See the most common reasons a project member can't access a project, service, or feature:

[+] [Expand table](#)

Issue	Troubleshooting action
Their access level doesn't support access to the service or feature.	To determine whether it's the cause, <a href="#">determine the user's access level and subscription status</a> .
Their membership within a security group doesn't support access to a feature or they were explicitly denied permission to a feature.	To determine whether it's the cause, <a href="#">trace a permission</a> .
The user was recently granted permission but their client needs a refresh to recognize the changes.	Have the user <a href="#">refresh or reevaluate their permissions</a> .
The user's trying to exercise a feature granted only to a team administrator for a specific team, however they aren't granted that role.	To add them to the role, see <a href="#">Add, remove team administrator</a> .
The user didn't enable a preview feature.	Have the user open the Preview features and determine the on/off status for the specific feature. For more information, see <a href="#">Manage preview features</a> .
Project member was added to a limited scope security group, such as the Project-Scope Users group.	To determine whether it's the cause, <a href="#">look up the user's security group memberships</a> .

## Less common access and permission issues

Less common reasons for limited access are when one of the following events occurred:

[+] [Expand table](#)

Issue	Troubleshooting action
A project administrator disabled a service. In this case, no one has access to the disabled service.	To determine whether a service is disabled, see <a href="#">Turn an Azure DevOps service on or off</a> .

Issue	Troubleshooting action
A Project Collection Administrator disabled a preview feature, which disables it for all project members in the organization.	See <a href="#">Manage preview features</a> .
Group rules governing the user's access level or project membership are restricting access.	See <a href="#">Determine a user's access level and subscription status</a> .
Custom rules were defined to a work item type's workflow.	see <a href="#">Rules applied to a work item type that restrict select operation</a> .

## Determine a user's access level and subscription status

You can assign users or groups of users to one of the following access levels:

- Stakeholder
- Basic
- Basic + Test Plans
- Visual Studio subscription
- GitHub Enterprise

For more information about restricting access levels in Azure DevOps, see [Supported access levels](#).

To use Azure DevOps features, users must be added to a security group with the appropriate permissions and have access to the web portal. Feature limitations are based on the user's access level and security group.

Users can lose access for the following reasons:

[+] [Expand table](#)

Reason for loss of access	Troubleshooting action
The user's Visual Studio subscription expired.	This user can <a href="#">work as a Stakeholder</a> , or you can give the user Basic access until the user renews their subscription. After the user signs in, Azure DevOps restores access automatically.
The Azure subscription used for billing is no longer active.	All purchases made with this subscription are affected, including Visual Studio subscriptions. To fix this issue, visit the <a href="#">Azure account portal</a> .
The Azure subscription used for billing was removed from	Learn more about <a href="#">linking your organization</a>

Reason for loss of access	Troubleshooting action
your organization.	

Otherwise, users who didn't sign in to your organization for the longest time lose access first. If your organization has users who don't need access anymore, [remove them from your organization](#).

For more information about permissions, see [Permissions and groups](#) and the [Permissions lookup guide](#).

## Trace a permission

Use permission tracing to determine why a user's permissions aren't allowing them access to a specific feature or function. Learn how a user or an administrator can investigate the inheritance of permissions. To trace a permission from the web portal, open the permission or security page for the corresponding level. For more information, see [Request an increase in permission levels](#).

If a user is having permissions issues, and you use default security groups or custom groups for permissions, use tracing to investigate where those permissions are coming from. Permissions issues could be because of delayed changes. It can take up to 1 hour for Microsoft Entra group memberships or permissions changes to propagate throughout Azure DevOps. If a user's having issues that don't resolve immediately, wait a day to see if they resolve. For more information about user and access management, see [Manage users and access in Azure DevOps](#).

Users can receive their effective permissions either directly or via groups.

Complete the following steps so administrators can understand where exactly those permissions are coming from and adjust them, as needed.

1. Select **Project settings > Permissions > Users**, and then select the user.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. The left sidebar has 'Project settings' highlighted with a red box and a red number '1'. The main content area shows 'Project Settings' for 'FabrikamFiber' with a red box around the 'Permissions' link under 'General' and a red number '2'. On the right, the 'Permissions' section is displayed with a red box around the 'Users' tab and a red number '3'. The 'Users' table lists six entries:

Name	
Customer service Build Service (fabrikamfibero)	CS
Jamal Hartnett fabrikamfiber4@hotmail.com	JH
Project Collection Build Service (fabrikamfiberc)	PS
Management team Build Service (fabrikamfiber)	MS
Fabrikam Test Build Service (fabrikamfiberorg)	FS
FabrikamFiber Build Service (fabrikamfiberorg)	FS

You should now have a user-specific view that shows what permissions they have.

2. To trace why a user does or doesn't have any of the listed permissions, select the information icon next to the permission in question.

The screenshot shows the 'Permissions' section of the Azure DevOps user profile for 'Jamal Hartnett'. The 'General' section includes permissions like 'Delete team project', 'Edit project-level information', and 'Manage project properties', all set to 'Allow (inherited)'. A tooltip for the 'Edit project-level information' permission states: 'The permission value is being inherited through your direct or indirect membership in these groups: [FabrikamFiber]\Project Administrators'. Other sections like 'Boards' and 'Analytics' also show 'Allow (inherited)' for most items.

The resulting trace lets you know how they're inheriting the listed permission. You can then adjust the user's permissions by adjusting the permissions that are provided to the groups that they're in.

For more information, see [Manage access to specific features and functions](#) or [Request an increase in permission levels](#).

## Refresh or reevaluate permissions

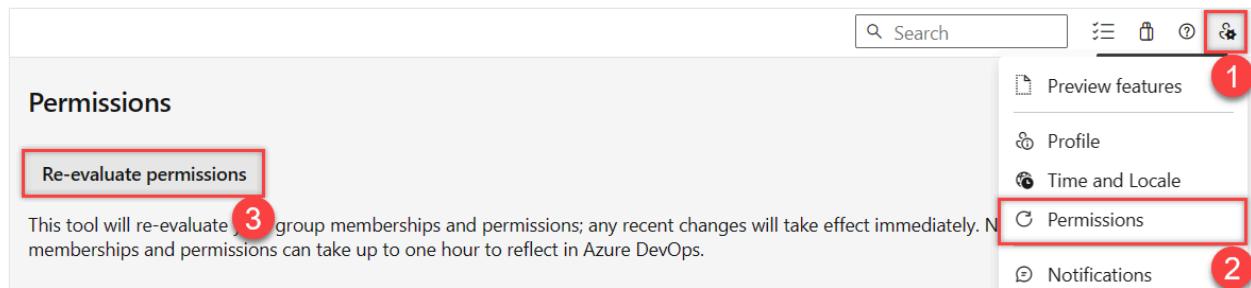
See the following scenario where refreshing or reevaluating permissions might be necessary.

### Problem

Users get added to an Azure DevOps or Microsoft Entra group. This action grants inherited access to an organization or project. But, they don't get access immediately. Users must either wait or sign out, close their browser, and then sign back in to get their permissions refreshed.

## Solution

Go to  **User settings > Permissions > Re-evaluate permissions**. This function reevaluates your group memberships and permissions, and then any recent changes take effect immediately.



## Rules applied to a work item type that restrict select operations

Before you customize a process, we recommend that you review [Configure and customize Azure Boards](#), which provides guidance on how to customize Azure Boards to meet your business needs.

For more information about work item type rules that apply toward restricting operations, see:

- [Apply rules to workflow states \(Inheritance process\)](#)
- [Sample rule scenarios](#)
- [Define area paths and assign to a team](#)

## Hide organization settings from users

If a user is limited to seeing only their projects or can't access organization settings, the following information might explain why. To restrict users from accessing organization settings, enable the **Limit user visibility and collaboration to specific projects** preview feature. For more information, including important security-related call-outs, see [Manage your organization, Limit user visibility for projects and more](#).

Examples of restricted users include Stakeholders, Microsoft Entra guest users, or members of a security group. Once enabled, any user or group added to the Project-Scope Users group is restricted from accessing the **Organization settings** pages, except for **Overview** and **Projects**. They can only access the projects to which they get added.

For more information, see [Manage your organization, Limit user visibility for projects and more.](#)

## View, add, and manage permissions with CLI

You can view, add, and manage permissions at a granular level with the `az devops security permission` commands. For more information, see [Manage permissions with command line tool](#).

## Group rules with lesser permissions

Group rule types are ranked in the following order: Subscriber > Basic + Test Plans > Basic > Stakeholder. Users always receive the highest access level available to them across all group rules, including any Visual Studio (VS) subscriptions.

### Note

- Changes made to **project readers** through group rules don't persist. To adjust project readers, consider alternative methods such as [direct assignment](#) or [custom security groups](#).
- Regularly review the rules listed on the "Group rules" tab of the "Users" page. Changes to Microsoft Entra ID group membership will appear in the next re-evaluation of the group rules, which can be done on-demand, when a group rule is modified, or automatically every 24 hours. Azure DevOps updates Microsoft Entra group membership every hour, but it may take up to 24 hours for Microsoft Entra ID to update [dynamic group membership](#).

See the following examples, showing how subscriber detection factors into group rules.

### Example 1: Group rule gives me more access

If I have a VS Pro subscription and I'm in a group rule that gives me Basic + Test Plans – what happens?

Expected: I get Basic + Test Plans because what the group rule gives me is greater than my subscription. Group rule assignment always provides the greater access, rather than limiting access.

## Example 2: Group rule gives me the same access

I have a Visual Studio Test Pro subscription and I'm in a group rule that gives me Basic + Test Plans – what happens?

Expected: I get detected as a Visual Studio Test Pro subscriber, because the access is the same as the group rule. I'm already paying for the Visual Studio Test Pro, so I don't want to pay again.

## Work with GitHub

See the following troubleshooting information for deploying code in Azure DevOps with GitHub.

### Problem

You can't bring the rest of your team into the organization and project, despite adding them as members. They receive emails, but when signing in, they get a 401 error.

### Solution

You might be signed into Azure DevOps with an incorrect identity. Do the following steps:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to the following URL: <https://aka.ms/vssignout>.

A message displays, "Sign out in progress." After you sign out, you get redirected to `dev.azure.microsoft.com`.

4. Sign in to [Azure DevOps](#) again and choose a different identity.

## Other areas where permissions might be applied

- [Area path permissions](#)
- [Work item tags](#)
- [Moved work items out of a project](#)

- Deleted work items
- Quick guide to default permissions and access for Azure Boards
- Custom rules
- Sample custom rule scenarios
- Custom backlogs and boards
- Custom controls

## Related articles

- Manage permissions with the command line tool
  - Change individual or group permissions
  - Security overview
  - Add users to an administrator role
- 

## Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

# Allowed IP addresses and domain URLs

Article • 04/03/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

If your organization is secured with a firewall or proxy server, you must add certain internet protocol (IP) addresses and domain uniform resource locators (URLs) to the **allowlist**. Adding these IPs and URLs to the allowlist helps to ensure that you have the best experience with Azure DevOps. You know that you need to update your allowlist if you can't access Azure DevOps on your network. See the following sections in this article:

- [Allowed domain URLs](#)
- [IP addresses and range restrictions](#)

## Tip

So that Visual Studio and Azure Services work well with no network issues, open select ports and protocols. For more information, see [Install and use Visual Studio behind a firewall or proxy server](#), [Use Visual Studio and Azure Services](#).

## IP addresses and range restrictions

### Outbound connections

*Outbound connections* target other dependent sites. Examples of such connections include:

- Browsers connecting to Azure DevOps website as users go to and use features of Azure DevOps
- Azure Pipelines agents installed on your organization's network connecting to Azure DevOps to poll for pending jobs
- CI events sent from a source code repository hosted within your organization's network to Azure DevOps

Ensure the following IP addresses are allowed for outbound connections, so your organization works with any existing firewall or IP restrictions. The endpoint data in the following chart lists requirements for connectivity from a machine in your organization to Azure DevOps Services.

IP V4 ranges
IP
13.107.6.0/24
13.107.9.0/24
13.107.42.0/24
13.107.43.0/24
150.171.22.0/24
150.171.23.0/24
150.171.73.0/24
150.171.74.0/24
150.171.75.0/24
150.171.76.0/24

If you're currently allowing the `13.107.6.183` and `13.107.9.183` IP addresses, leave them in place, as you don't need to remove them.

 **Note**

Azure Service Tags aren't supported for *outbound* connections.

## Inbound connections

*Inbound connections* originate from Azure DevOps and target resources within your organization's network. Examples of such connections include:

- Azure DevOps Services connecting to endpoints for [Service Hooks](#)
- Azure DevOps Services connecting to customer-controlled SQL Azure VMs for [Data Import](#)
- Azure Pipelines connecting to on-premises source code repositories such as [GitHub Enterprise](#) or [Bitbucket Server](#)
- Azure DevOps Services [Audit Streaming](#) connecting to on-premises or cloud-based Splunk

Ensure the following IP addresses are allowed for inbound connections, so your organization works with any existing firewall or IP restrictions. The endpoint data in the following chart lists requirements for connectivity from Azure DevOps Services to your on-premises or other cloud services.

 Expand table

<b>Geography</b>	<b>Region</b>	<b>IP V4 ranges</b>
Australia	Australia East	20.37.194.0/24
	Australia South East	20.42.226.0/24
Brazil	Brazil South	191.235.226.0/24
Canada	Central Canada	52.228.82.0/24
Asia Pacific	Southeast Asia (Singapore)	20.195.68.0/24
India	South India	20.41.194.0/24
	Central India	20.204.197.192/26
United States	Central United States	20.37.158.0/23
	West Central United States	52.150.138.0/24
	East United States	20.42.5.0/24
	East 2 United States	20.41.6.0/23
	North United States	40.80.187.0/24
	South United States	40.119.10.0/24
	West United States	40.82.252.0/24
	West 2 United States	20.42.134.0/23
	West 3 United States	20.125.155.0/24
Europe	Western Europe	40.74.28.0/23
	North Europe	20.166.41.0/24
United Kingdom	United Kingdom South	51.104.26.0/24

Azure Service Tags are supported only for *inbound* connections. Instead of allowing the previously listed IP ranges, you may use the **AzureDevOps** service tag for Azure Firewall and Network Security Group (NSG) or on-premises firewall via a JSON file download.

#### ⓘ Note

The Service Tag or previously mentioned inbound IP addresses don't apply to Microsoft Hosted agents. Customers are still required to allow the [entire geography for the Microsoft Hosted agents](#). If allowing the entire geography is a concern, we recommend using the [Microsoft Managed DevOps Pools](#).

Alternatively, you can also use [Azure Virtual Machine Scale Set agents](#). Managed DevOps Pools and Scale Set agents are a form of self-hosted agents that can be auto-scaled to meet your demands.

Hosted macOS agents are hosted in GitHub's macOS cloud. IP ranges can be retrieved using the [GitHub metadata API](#) using the instructions provided [here](#).

## Other IP addresses

Most of the following IP addresses pertain to Microsoft 365 Common and Office Online.

### Microsoft365Common&Office IPs

40.82.190.38  
52.108.0.0/14  
52.237.19.6  
52.238.106.116/32  
52.244.37.168/32  
52.244.203.72/32  
52.244.207.172/32  
52.244.223.198/32  
52.247.150.191/32

For more information, see [Worldwide endpoints](#) and [Adding IP address rules](#).

## Azure DevOps ExpressRoute connections

If your organization uses ExpressRoute, ensure the following IP addresses are allowed for both outbound and inbound connections.

### IP V4 ranges

IP  
13.107.6.175/32  
13.107.6.176/32  
13.107.6.183/32  
13.107.9.175/32  
13.107.9.176/32  
13.107.9.183/32  
13.107.42.18/32  
13.107.42.19/32  
13.107.42.20/32  
13.107.43.18/32  
13.107.43.19/32  
13.107.43.20/32

```
150.171.73.14/32
150.171.73.15/32
150.171.73.16/32
150.171.74.14/32
150.171.74.15/32
150.171.74.16/32
150.171.75.14/32
150.171.75.15/32
150.171.75.16/32
150.171.76.14/32
150.171.76.15/32
150.171.76.16/32
150.171.22.17/32
150.171.22.18/32
150.171.22.19/32
150.171.23.17/32
150.171.23.18/32
150.171.23.19/32
```

For more information about Azure DevOps and ExpressRoute, see [ExpressRoute for Azure DevOps](#).

## Allowed Domain URLs

Network connection issues could occur because of your security appliances, which may be blocking connections - Visual Studio uses TLS 1.2 and above. When you're using [NuGet](#) or connecting from Visual Studio 2015 and later, update the security appliances to support TLS 1.2 and above for the following connections.

To ensure your organization works with any existing firewall or IP restrictions, ensure that `dev.azure.com` and `*.dev.azure.com` are open.

The following section includes the most common domain URLs to support sign in and licensing connections.

### CommonDomainURLs

```
https://dev.azure.com
https://*.dev.azure.com
https://aex.dev.azure.com
https://aexprodea1.vsaex.visualstudio.com
https://*vstmrblob.vsassets.io
https://amp.azure.net
https://app.vssps.dev.azure.com
https://app.vssps.visualstudio.com
https://*.vsblob.visualstudio.com
https://*.vssps.visualstudio.com
```

```
https://*.vstmr.visualstudio.com  
https://azure.microsoft.com  
https://go.microsoft.com  
https://graph.microsoft.com  
https://login.microsoftonline.com  
https://management.azure.com  
https://management.core.windows.net  
https://microsoft.com  
https://microsoftonline.com  
https://static2.sharepointonline.com  
https://visualstudio.com  
https://vsrm.dev.azure.com  
https://*.windows.net  
https://{{organization_name}}.visualstudio.com  
https://{{organization_name}}.vsrm.visualstudio.com  
https://{{organization_name}}.vstmr.visualstudio.com  
https://{{organization_name}}.pkgs.visualstudio.com  
https://{{organization_name}}.vssps.visualstudio.com
```

Azure DevOps uses the following URLs to provide the agent software for download for self-hosted agents.

```
https://vstsagentpackage.azureedge.net  
https://download.agent.dev.azure.com
```

Azure DevOps uses content delivery network (CDN) to serve static content.

The following URLs are part of that.

```
https://cdn.vsassets.io  
https://*.vsassets.io  
https://*gallerycdn.vsassets.io  
https://aadcdn.msauth.net  
https://aadcdn.msftauth.net  
https://amcdn.msftauth.net  
https://azurecomcdn.azureedge.net
```

The following endpoints are used to authenticate Azure DevOps organizations using a Microsoft Account (MSA). These endpoints are only needed for Azure DevOps organizations backed by Microsoft Accounts (MSA). Azure DevOps organizations backed a Microsoft Entra tenant doesn't need the following URLs.

```
https://live.com  
https://login.live.com
```

The following URL is required if you're migrating from Azure DevOps server to the cloud service using our data migration tool.

<https://dataimport.dev.azure.com>

### ⓘ Note

Azure DevOps uses Content Delivery Networks (CDNs) to serve static content. Users in **China** should also add the following domain URLs to an allowlist:

#### NuGetDomainURLs

[https://\\*.vsassetscdn.azure.cn](https://*.vsassetscdn.azure.cn)  
[https://\\*.gallerycdn.azure.cn](https://*.gallerycdn.azure.cn)

We recommend you open port 443 to all traffic on the following IP addresses and domains. We also recommend you open port 22 to a smaller subset of targeted IP addresses.

[+] Expand table

More domain URLs	Descriptions
<a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Authentication and sign-in related
<a href="https://*.vssps.visualstudio.com">https://*.vssps.visualstudio.com</a>	Authentication and sign-in related
<a href="https://*gallerycdn.vsassets.io">https://*gallerycdn.vsassets.io</a>	Hosts Azure DevOps extensions
<a href="https://*vstmrblob.vsassets.io">https://*vstmrblob.vsassets.io</a>	Hosts Azure DevOps TCM log data
<a href="https://cdn.vsassets.io">https://cdn.vsassets.io</a>	Hosts Azure DevOps Content Delivery Networks (CDNs) content
<a href="https://static2.sharepointonline.com">https://static2.sharepointonline.com</a>	Hosts some resources that Azure DevOps uses in "office fabric" UI kit for fonts, and so on
<a href="https://vsrm.dev.azure.com">https://vsrm.dev.azure.com</a>	Hosts releases
<a href="https://vstsagentpackage.azureedge.net">https://vstsagentpackage.azureedge.net</a> <a href="https://download.agent.dev.azure.com">https://download.agent.dev.azure.com</a>	Required to set up self-hosted agent in machines within your network
<a href="https://amp.azure.net">https://amp.azure.net</a>	Needed for deploying to Azure app service
<a href="https://go.microsoft.com">https://go.microsoft.com</a>	Accesses go links

## Azure Artifacts

Ensure the following domain URLs are allowed for Azure Artifacts:

#### AzureArtifactsDomainURLs

```
https://*.blob.core.windows.net  
https://*.visualstudio.com  
https://*.dedup.microsoft.com
```

Also allow all IP addresses in the "name": "Storage.{region}" section of the following file (updated weekly): [Azure IP ranges and Service Tags - Public Cloud](#). {region} is the same Azure Geography as your organization.

## NuGet connections

Ensure the following domain URLs are allowed for NuGet connections:

#### NuGetDomainURLs

```
https://*azurewebsites.net  
https://*.nuget.org
```

#### ⚠ Note

Privately owned NuGet server URLs might not be included in the previous list. You can check the NuGet servers you're using by opening

```
%APPData%\Nuget\NuGet.Config.
```

## SSH connections

If you need to connect to Git repositories on Azure DevOps with SSH, allow requests to port 22 for the following hosts:

#### SSHDomainHosts

```
ssh.dev.azure.com  
vs-ssh.visualstudio.com
```

Also allow IP addresses in the "name": "AzureDevOps" section of [this downloadable file](#) (updated weekly) named: [Azure IP ranges and Service Tags - Public Cloud](#)

## Azure Pipelines Microsoft-hosted agents

If you use Microsoft-hosted agent to run your jobs and you need the information about what IP addresses are used, see [Microsoft-hosted agents IP ranges](#). See all [Microsoft Managed DevOps Pools](#) and [Azure Virtual Machine Scale Set agents](#).

For more information about hosted Windows, Linux, and macOS agents, see [Microsoft-hosted agent IP ranges](#).

## Azure Pipelines self-hosted agents

If you're running a firewall and your code is in Azure Repos, see [Self-hosted Linux agents FAQs](#), [Self-hosted macOS agents FAQs](#) or [Self-hosted Windows agents FAQs](#). This article has information about which domain URLs and IP addresses your private agent needs to communicate with.

### Important

[Edgio CDN for Azure DevOps is being retired](#), which requires a new domain URL to be allow-listed in firewall rules for agent software download. The new domain to allow-list for agent download is `https://*.dev.azure.com`. If your firewall rules don't allow wildcards, use `https://download.agent.dev.azure.com`.

The Azure DevOps team recommends to make this change by the following date:

- May 1, 2025 for Azure DevOps Services
- May 15, 2025 for Azure DevOps Server

For more information, see [CDN Domain URL change for Agents in Pipelines](#).

## Azure DevOps import service

During the import process, we highly recommend that you restrict access to your virtual machine (VM) to only IP addresses from Azure DevOps. To restrict access, allow only connections from the set of Azure DevOps IP addresses, which were involved in the collection database import process. For information about identifying the correct IP addresses, see [\(Optional\) Restrict access to Azure DevOps Services IPs only](#).

### Note

Azure DevOps doesn't natively support allowlisting directly within its settings. However, you can manage allowlisting at the network level using your organization's firewall or proxy settings.

## Related articles

- [Available service tags](#)
- [Microsoft-hosted agents IP address ranges](#)
- [Self-hosted Windows agents FAQs](#)
- [Configure Azure Storage firewalls and virtual networks](#)
- [Install and use Visual Studio behind a firewall or proxy server](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Get support and provide feedback

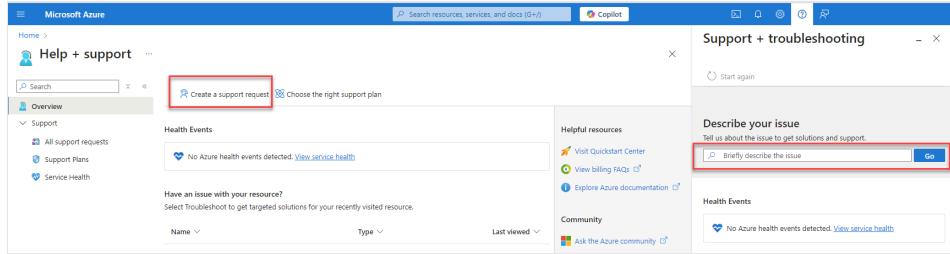
Article • 02/23/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

This article helps you access support resources and provide feedback for Azure DevOps. Learn how to [contact Support](#), report issues, suggest features, and give feedback on both the product and documentation.

## Get support and give feedback

[Expand table](#)

Action	More info
<a href="#">Contact Support</a>	In the Microsoft Azure portal, create a support request, briefly describe the issue to get to solutions and support, and then follow the prompts for additional details. 
<a href="#">Get Virtual Agent support</a>	Chat with our Virtual Agent to get help with common issues, including user management, organization-level configuration and management, sign-in issues, region moves, and more.
<a href="#">Troubleshoot access issues</a>	<ul style="list-style-type: none"><li>- <a href="#">Collect an HTTP Archive (HAR) trace</a> sign-in issues via Microsoft Edge or Google Chrome.</li><li>- <a href="#">Troubleshoot access and permissions issues</a>.</li><li>- View <a href="#">user and permissions management FAQs</a>.</li><li>- View <a href="#">Microsoft Entra access FAQs</a>.</li></ul>
<a href="#">Report a bug or problem</a>	Report a problem via the Developer Community, which is an open channel to Microsoft engineering teams: <ul style="list-style-type: none"><li>- <a href="#">Azure DevOps Services</a></li><li>- <a href="#">Azure DevOps Server</a></li></ul>
<a href="#">Suggest a feature</a>	Submit your suggestion via the Developer Community, which is an open channel to Microsoft engineering teams: <ul style="list-style-type: none"><li>- <a href="#">Azure DevOps Services</a></li><li>- <a href="#">Azure DevOps Server</a></li></ul>

Action	More info
Contact your project administrator	Contact your project administrator for assistance with access issues, permission changes, project configuration, resource allocation, or troubleshooting.
Get advice	Get advice from developers via StackOverflow: - <a href="#">Azure DevOps Services ↗</a> - <a href="#">Azure DevOps Server ↗</a>
Report security flaws ↗	Report potential security issues to ensure the safety and integrity of the system.
<a href="#">View Release Notes</a>	Check out what's new in Azure DevOps Release Notes, which get updated every three weeks.

## Tips for effective feedback

If you want to vent about the product or the documentation, that's okay. It helps us know when you're happy or unhappy with an experience. Provide the following details so we can better understand what we're doing right or wrong:

- **Provide context.** What problem were you trying to solve? At what point did it go wrong?
- **Include your role.** Are you a developer, manager, or business owner? Understanding our audience helps us create better solutions.
- **Include your product version.** What other products were you using with it?

## Give product feedback

Enter clear, precise, detailed feedback when you [create a support request ↗](#).

**Example:** "I'm a project manager for a small start-up using Azure DevOps. I'm trying to create work item templates through the UI, but my changes don't persist. It's not clear what I'm doing wrong."

## Give documentation feedback

All articles on Microsoft Learn have a ratings tool. Select **Feedback** beneath the title of the article, and in the "Was this page helpful?" pane, select **Yes** or **No** based on your experience.

Enter clear, precise, detailed feedback in the **Tell us more** section. Avoid including sensitive or personal information. Although we can't reply, we regularly review this

feedback and use it in our content planning.

**Example:** "I'm a developer in a large organization working on Java apps. I tried to use Maven with your build system in Azure DevOps Server 2017 Update 1 (15.112.26307.0), but I couldn't get the configuration shown in the documentation to work."

For more information, see the following section of related articles.

## Related articles

- [View the Azure DevOps Roadmap](#)
  - [View Azure Boards FAQs](#)
  - [Troubleshoot Azure Pipelines](#)
  - [Troubleshoot migration errors](#)
  - [Troubleshoot common errors with Azure DevOps CLI](#)
  - [Report a problem with Visual Studio](#)
- 

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Look up your Azure DevOps platform and version

Article • 04/24/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

The **About** page for Azure DevOps Services or Azure DevOps Server shows the platform and version in use. You can access the **About** page from the UI or by using a URL to look up your platform and version.

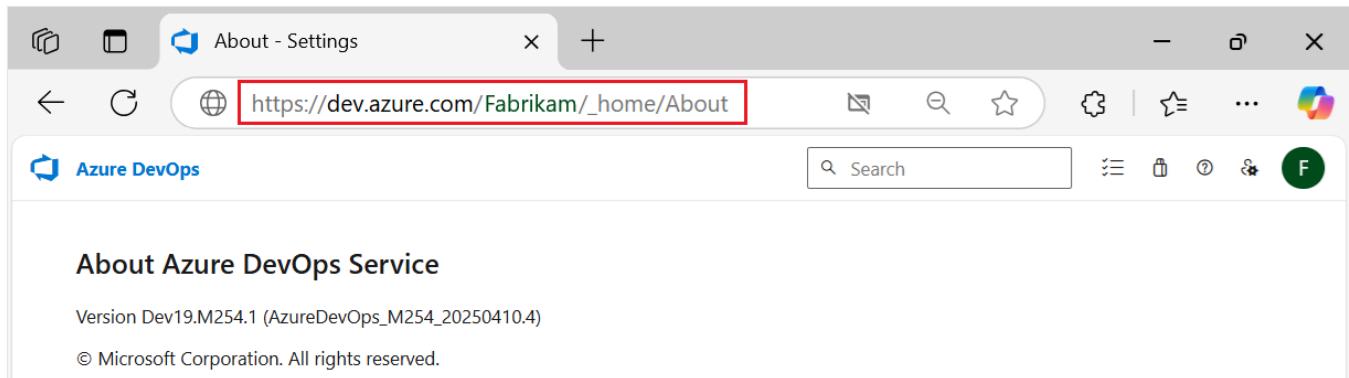
## Azure DevOps Services

Look up the version number for Azure DevOps Services by following these steps:

1. Open a browser window.
2. Enter the following URL. Replace the `\<organization>` placeholder with the name of your organization:

```
https://dev.azure.com/<Organization>/_home/About
```

A page similar to the following example opens showing the platform in use and the version number:



## Azure DevOps Server

Look up the version number for Azure DevOps Server by following these steps in the UI:

1. In Azure DevOps, go to the **Overview** page for your organization.
2. Open the **Profile** menu by selecting your user picture, and then select **Help > About**.

A page similar to the following example opens showing the platform in use and the version number:

A screenshot of the Azure DevOps web interface. At the top, there are two tabs: 'devops-2022 - Microsoft Azure' and 'Projects - Home'. The address bar shows 'Not secure | devops-2022/DefaultCollection'. On the left, a sidebar lists 'DefaultCollection' (selected) and 'CustomCollection'. The main area is titled 'DefaultCollection' with tabs for 'Projects', 'My work items', and 'My pull requests'. A project card for 'FabrikamFiber' is visible. On the right, a user profile menu is open for 'Jamal Hartnett fabrikam@fabrikam.com'. The menu includes links for 'My profile', 'Security', 'Notification settings', 'Theme', 'Help' (with a red arrow pointing to it), 'Sign in as...', and 'Sign out'. A magnifying glass icon is at the bottom right of the menu.

You can also find the version number by using a URL in the browser:

1. Open a browser window.
2. Enter the following URL. Replace the `\<Server>` placeholder with the name of your server, and the `\<Collection>` placeholder with the name of your collection:

`https://<Server>/<Collection>/_home/About`

A page similar to the following example opens showing the platform in use and the version number:

A screenshot of the 'About Azure DevOps Server' page. It features the Azure DevOps logo and title. Below that, it says 'About Azure DevOps Server'. It displays the version 'Version Azure DevOps Server 2022 RC1 (AzureDevOpsServer\_20220720.1)' and the copyright notice '© Microsoft Corporation. All rights reserved.'

## Access server release notes

The following table provides links to the Release to Web (RTW) Release Notes for the most recent versions of Azure DevOps Server. You can also access notes for specific Release Updates and SHA hash values to verify download integrity.

[ ] Expand table

Version	RTW notes	Update notes	SHA values
Azure DevOps Server 2022	Release	Update 2 Update 1	SHA
Azure DevOps Server 2020	Release	Update 1	SHA
Azure DevOps Server 2019	Release	Update 1	SHA

## Related content

- [Azure DevOps features timeline](#)
- [Report a problem with Visual Studio](#)

# Rate and usage limits

Article • 03/21/2025

## Azure DevOps Services

Azure DevOps Services uses multi-tenancy to reduce costs and improve performance. This design leaves users vulnerable to performance issues and even outages when other users of their shared resources have spikes in their consumption. So, Azure DevOps limits the resources individuals can consume, and the amount of requests they can make to certain commands. When these limits are exceeded, future requests might be either delayed or blocked.

For more information, see [Git limits](#) and [Best practices to avoid hitting rate limits](#).

## Global consumption limit

Azure DevOps currently has a global consumption limit, which delays requests from individual users beyond a threshold when shared resources are in danger of being overwhelmed. This limit is focused exclusively on avoiding outages when shared resources are close to being overwhelmed. Individual users typically only get delayed requests when one of the following incidents occurs:

- One of their shared resources is at risk of being overwhelmed
- Their personal usage exceeds 200 times the consumption of a typical user within a (sliding) five-minute window

The amount of the delay depends on the user's sustained level of consumption. Delays range from a few milliseconds per request up to 30 seconds. Once consumption goes to zero or the resource is no longer overwhelmed, the delays stop within five minutes. If consumption remains high, delays might continue indefinitely to protect the resource.

When a user request gets delayed by a significant amount, that user receives an email and a warning banner in the web. For the build service account and others without an email address, members of the Project Collection Administrators group get the email. For more information, see [Usage monitoring](#).

When an individual user's requests get blocked, responses with HTTP code 429 (too many requests) are received, with a message similar to the following message:

```
TF400733: The request has been canceled: Request was blocked due to exceeding usage  
of resource <resource name> in namespace <namespace ID>.
```

# Azure DevOps throughput units

Azure DevOps users consume many shared resources, and consumption depends on the following factors:

- Uploading a large number of files to version control creates a large amount of load on databases and storage accounts
- Complex work item tracking queries create database load based on the number of work items they search through
- Builds drive load by downloading files from version control, producing log output
- All operations consume CPU and memory on various parts of the service

To accommodate, Azure DevOps resource consumption is expressed in abstract units called Azure DevOps throughput units (TSTUs). TSTUs eventually incorporate a blend of the following items:

- [Azure SQL Database DTUs](#) as a measure of database consumption
- Application tier and job agent CPU, memory, and I/O as a measure of compute consumption
- Azure Storage bandwidth as a measure of storage consumption

For now, TSTUs are primarily focused on Azure SQL Database DTUs, since Azure SQL Databases are the shared resources most commonly overwhelmed by excessive consumption. A single TSTU is the average load we expect a typical user of Azure DevOps to generate per five minutes. Typical users also generate spikes in load. These spikes are typically 10 or fewer TSTUs per five minutes. Less frequently, spikes go as high as 100 TSTUs.

The global consumption limit is 200 TSTUs within a sliding five-minute window.

We recommend that you at least respond to the `Retry-After` header. If you detect a `Retry-After` header in any response, wait until some time passes before you send another request. Doing so helps your client application experience fewer enforced delays. Keep in mind that the response is 200, so you don't need to apply retry logic to the request.

If possible, we further recommend that you monitor `X-RateLimit-Remaining` and `X-RateLimit-Limit` headers. Doing so allows you to approximate how quickly you're approaching the delay threshold. Your client can intelligently react and spread out its requests over time.

## ⓘ Note

Identities used by tools and applications to integrate with Azure DevOps might occasionally need higher rate and usage limits beyond the allowed consumption limit. You can increase these limits by assigning the [Basic + Test Plans](#) access level to the desired identities used by your application. Once the need for higher rate limits is fulfilled, you can revert to the previous access level. You get charged for the [Basic + Test Plans](#) access level only for the duration assigned to the identity.

Identities already assigned a Visual Studio Enterprise subscription can't get assigned the [Basic + Test Plans](#) access level until they get removed.

## Pipelines

Rate limiting is similar for Azure Pipelines. Each pipeline gets treated as an individual entity with its own resource consumption tracked. Even if build agents are self-hosted, they generate load in the form of cloning and sending logs.

We apply a 200 TSTU limit for an individual pipeline in a sliding 5-minute window. This limit is the same as the global consumption limit for users. If a pipeline gets delayed or blocked by rate limiting, a message appears in the attached logs.

## API client experience

When requests get delayed or blocked, Azure DevOps returns response headers to help API clients react. While not fully standardized, these headers are [broadly in line with other popular services](#).

The following table lists the headers available and what they mean. Except for `x-RateLimit-Delay`, all of these headers get sent before requests start getting delayed. This design gives clients the opportunity to proactively slow down their rate of requests.

### Header name

### Description

#### Retry-After

The [RFC 6585](#)-specified header sent to tell you how long to wait before you send your next request to fall under the detection threshold. Units: seconds.

#### X-RateLimit-Resource

A custom header indicating the service and type of threshold that was reached. Threshold types and service names might vary over time and without warning. We recommend displaying this string to a human, but not relying on it for computation.

---

#### X-RateLimit-Delay

How long the request was delayed. Units: seconds with up to three decimal places (milliseconds).

---

#### X-RateLimit-Limit

Total number of TSTUs allowed before delays are imposed.

---

#### X-RateLimit-Remaining

Number of TSTUs remaining before being delayed. If requests are already being delayed or blocked, it's 0.

---

#### X-RateLimit-Reset

Time at which, if all resource consumption stopped immediately, tracked usage would return to 0 TSTUs. Expressed in Unix epoch time.

---

## Work tracking, process, & project limits

Azure DevOps imposes limits for the number of projects you can have in an organization and the number of teams you can have within each project. Also be aware of limits for work items, queries, backlogs, boards, dashboards, and more. For more information, see [Work tracking, process, and project limits](#).

In addition to the usual [repository limits](#), wikis defined for a project are limited to 25 MB per single file.

## Service connections

There are no per-project limits placed on creating service connections. However, there might be limits, which are imposed through Microsoft Entra ID. For additional information, review the following articles:

- [Microsoft Entra service limits and restrictions](#)
- [Azure subscription and service limits, quotas, and constraints](#)

## Related articles

- [Track work, manage processes, and set project limits](#)
- [Configure and customize Azure Boards](#)
- [Monitor usage](#)
- [Understand Git limits](#)
- [Follow best practices for avoiding hitting rate limits](#)

---

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Get started with Azure DevOps CLI

Article • 09/04/2024

## Azure DevOps Services

With the Azure DevOps extension for Azure Command Line Interface (CLI), you can manage many Azure DevOps Services from the command line. CLI commands enable you to streamline your tasks with faster and flexible interactive canvas, bypassing user interface workflows.

### ⓘ Note

The Azure DevOps Command Line Interface (CLI) is only available for use with Azure DevOps Services. The Azure DevOps extension for the Azure CLI does not support any version of Azure DevOps Server.

To start using the Azure DevOps extension for Azure CLI, perform the following steps:

1. Install Azure CLI: Follow the instructions provided in [Install the Azure CLI](#) to set up your Azure CLI environment. At a minimum, your Azure CLI version must be 2.10.1. You can use `az --version` to validate.
2. Add the Azure DevOps extension:

```
az extension add --name azure-devops
```

You can use `az extension list` or `az extension show --name azure-devops` to confirm the installation.

3. Sign in: Run `az login` to sign in. Note that we support only interactive or log in using user name and password with `az login`. To sign in using a Personal Access Token (PAT), see [Sign in via Azure DevOps Personal Access Token \(PAT\)](#).

### ⓘ Note

The Azure DevOps extension does not currently support authenticating with [Managed Identities](#).

4. Configure defaults: We recommend you set the default configuration for your organization and project. Otherwise, you can set these within the individual commands themselves.

```
az devops configure --defaults organization=https://dev.azure.com/contoso  
project=ContosoWebApp
```

## Command usage

Adding the Azure DevOps Extension adds `devops`, `pipelines`, `artifacts`, `boards`, and `repos` groups. For usage and help content for any command, enter the `-h` parameter, for example:

Azure CLI

```
az devops -h
```

Output

Group

```
az devops : Manage Azure DevOps organization level operations.  
  Related Groups  
    az pipelines: Manage Azure Pipelines  
    az boards: Manage Azure Boards  
    az repos: Manage Azure Repos  
    az artifacts: Manage Azure Artifacts.
```

Subgroups:

```
  admin          : Manage administration operations.  
  extension     : Manage extensions.  
  project       : Manage team projects.  
  security      : Manage security related operations.  
  service-endpoint : Manage service endpoints/service connections.  
  team          : Manage teams.  
  user          : Manage users.  
  wiki          : Manage wikis.
```

Commands:

```
  configure      : Configure the Azure DevOps CLI or view your configuration.  
  feedback       : Displays information on how to provide feedback to the  
Azure DevOps CLI team.  
  invoke         : This command will invoke request for any DevOps area and  
resource. Please use  
                  only json output as the response of this command is not  
fixed. Helpful docs -  
                  https://learn.microsoft.com/rest/api/azure/devops/.  
  login          : Set the credential (PAT) to use for a particular  
organization.  
  logout         : Clear the credential for all or a particular organization.
```

# Open items in browser

You can use `--open` switch to open any artifact in Azure DevOps portal in your default browser.

For example :

Azure CLI

```
az pipelines build show --id 1 --open
```

This command shows the details of build with `id 1` on the command-line and also opens it in the default browser.

## Related articles

- [Sign in via Azure DevOps Personal Access Token \(PAT\)](#)
- [Output formats](#)
- [Index to az devops examples](#)
- [Azure DevOps CLI Extension GitHub Repo ↗](#)

# Azure DevOps integration of services overview

Article • 03/05/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

With Azure DevOps, you can connect to and collaborate across its core services. You can use various features to link and track your devops tasks across Azure Boards, Azure Repos, Azure Pipelines, and Azure Test Plans. This article shows you options for how to use the cross-service integration of Azure DevOps to improve your workflow and productivity.

Links to more information:

- [Power Automate, Azure DevOps ↗](#)
- [Power Automate templates for Azure DevOps ↗](#)

## Collaboration across Azure DevOps

The following table summarizes some of the features that help you work with your team and other teams.

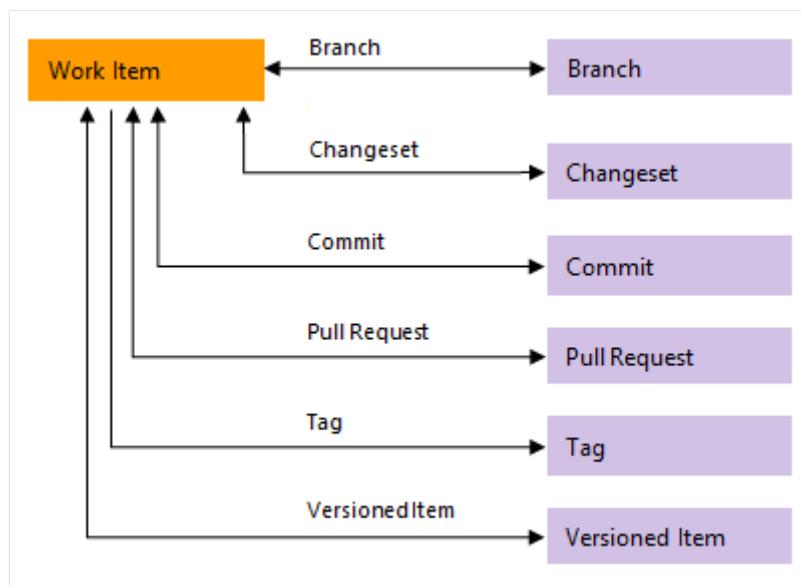
[ ] [Expand table](#)

Feature	Description
@mentions (add to discussions and comments)	You can <a href="#">@mention a team member or an entire team</a> within a work item form discussion or the comment section of a commit, pull request, or changeset.
#ID (link to a work item)	To support end-to-end traceability, you can <a href="#">link to work items from commits, pull requests, and changesets</a> .
Teams	<a href="#">Each team gets access to a suite of Agile tools</a> and team assets. These tools let teams work autonomously and collaborate with other teams across the enterprise. Each team can configure and customize each tool to support how they work. For quick navigation, they can favorite repositories, pipelines, and test plans.
Alerts	Configure or opt out of personal, team, project, or organization-level alerts. <a href="#">Subscribe to email alerts</a> when changes occur to work items, code reviews, pull requests, source control files, builds, and more.

Feature	Description
Summaries by email	- Email a list of work items - Email query items - Send release summaries by email
Wiki	Embed Azure Boards query results in Wiki.

## Azure Boards and Azure Repos integration

You can link code changes to user stories and features with different link types. For Git, use *Branch*, *Commit*, *Pull Request*, or *Tag*. For TFVC, use *Changeset* or *Versioned Item*.



The following table summarizes the integration points between Azure Boards and Azure Repos.

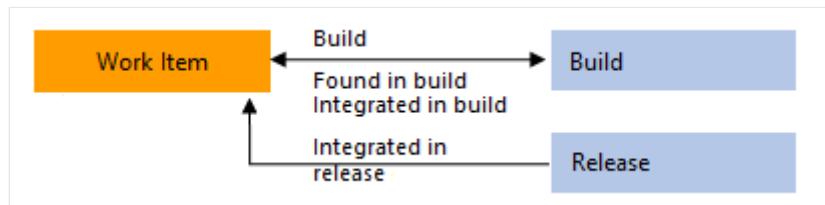
[Expand table](#)

Feature	Description
Drive Git development from work items	You can initiate a Git branch or link to Git commits or pull requests and <a href="#">drive your Git development cycle for a work item</a> from within the work item form.
Automatically link and transition work items with Git commits	For a Git repository, you can turn on or off the following options: <ul style="list-style-type: none"> <li>- Close work items with mentions in commit comments.</li> <li>- Remember user choices for completing work items with pull requests.</li> <li>- Link work items from commit comments. You can also automate linking from commits or pull requests in repo settings.</li> <li>- Commit mention linking: Turn on to link commits to work items with #WorkItemID in commit messages. Turn off when you push a repo from a different account or service. Azure DevOps automatically turns off this</li> </ul>

Feature	Description
	feature when you import a repo. - Commit mention work item resolution: Turn on to close work items with Fixes #WorkItemID in commits. - Work item transition preferences: On by default, it remembers each user's option to complete linked work items with pull requests. You can turn this feature off to discourage users from completing work items with pull requests. When it's off, users have to choose to complete work items for each pull request.
Check for linked work items in a Git branch	Encourage traceability by checking for linked work items on pull requests.
Auto complete work items with pull requests	When you link a work item to a pull request (PR), you can <a href="#">automatically complete</a> those work items when you successfully complete the PR. The system defaults to your selection for future PRs.
View list of code objects a single work item is linked to	You can link work items to code changes, builds, and releases—providing an audit trail of the feature development.
Query for external links	You can <a href="#">query for work items that contain links</a> to branches, commits, pull requests, or tags.
Configure branch policies to support work tracking	To ensure that changes to a branch have links to work items, you configure the branch policy for a Git repository in repo settings. Turn on the <b>Check for linked work items</b> option. Choose <b>Required</b> to mandate all pull requests have at least one linked work item in order to be completed. Choose <b>Optional</b> to allow pull requests without linked work items, but warn about it.

## Azure Boards and Azure Pipelines integration

The following table summarizes the integration points between Azure Boards and Azure Pipelines. Several features provide support for end-to-end traceability as user stories and features move through the development cycle. As with Azure Repos, you can link work items to pipeline objects with the following link types: *Build*, *Integrated in build*, and *Integrated in release*.



### Feature

## Description

---

Manually link work items to builds.

Link work items to builds in the same or other project within the organization or collection.

Set integration option to automatically create *Integrated in build* links to work items linked to a branch, commit, or pull request associated with a pipeline.

Required to populate the **Development** control with *Integrated in build* links. The work items or commits that are part of a release are computed from the versions of artifacts. For example, each build in Azure Pipelines is associated with a set of work items and commits. For more information, see [Configure pipelines to support integration](#).

---

To link work items to builds and releases, choose an option and a branch for a Classic or YAML pipeline. This action creates *Integrated in build* and *Integrated in release stage* links for work items that are linked to a branch, commit, or pull request.

Required to populate the work item form **Development** control with *Integrated in build* links and the **Deployment** control with *Integrated in release stage* links when running a Classic or YAML pipeline. For more information, see [Configure pipelines to support integration](#).

---

Set integration option to automatically create *Integrated in release stage* links to work items linked to a branch, commit, or pull request associated with a release.

Required to populate **Deployment** control in work item form with **Integrated in release stage** links. For more information, see [Release pipelines, How do I integrate and report release status?](#).

---

View and open list of work items linked to a Classic or YAML pipeline.

Lists all work items linked to a release since the previous selected release. Can sort the list by each column.

---

View list of build or release objects a single work item is linked to

You can [link work items to builds and releases](#)—providing an audit trail of the feature development and deployment.

---

Query for external links.

You can [query for work items that contain external links](#).

---

View and quickly navigate to release stages a work item is linked to.

The **Deployment** control on the work item form shows the stages that the work item is linked to. You can see the status of some runs and open each stage or run by expanding a stage. For more information, see [Link and view work items to deployments](#).

---

Create a work item on failure (Classic or YAML), optionally set values for a work item field (Classic)

Automatically create a work item and set fields when a build fails. For more information, see [Build options](#) for Classic pipelines, and [Customize pipelines, Create work item on failure](#).

---

Query Work Items task. Ensure the number of matching work items returned from a query is within a threshold.

Use this task to ensure the number of matching items returned by a work item query is within the configured thresholds. For more information, see [Query Work Items task](#), [Control deployments with gates and approvals](#).

---

## Azure Repos and Azure Pipelines integration

Azure Pipelines provides support for building code stored in Azure Repos, either a Git or Team Foundation Version Control (TFVC) repository. Other repositories that Azure Pipelines supports are listed in [Supported source repositories](#).

The following table summarizes the integration features between Azure Repos and Azure Pipelines.

[+] Expand table

Feature	Description
Report deployment status	Indicates the status of a deployment on the <a href="#">Files</a> , <a href="#">Commits</a> , and <a href="#">Branches</a> pages for Git repositories. This feature improves the traceability from code commit to deployment. You can <a href="#">configure the release environments to report deployment status</a> .
Release status badge	<a href="#">Post the status of your most recent pipeline build in your repository</a> .
Code coverage	<a href="#">Publish</a> and <a href="#">review</a> code coverage results that indicate the proportion of your project's code that is actually being tested.

## Azure Boards, Azure Repos, and Azure Test Plans integration

Several collaboration scenarios are supported through Azure Boards work item types. You can use [managed queries](#) and the [Azure DevOps search function](#) to find and list work items.

### ⓘ Note

You should create some work item types—such as Feedback Request, Code Review Request, Shared Steps, and Shared Parameters—through specific tools or forms. These types get added to the Hidden Types category and don't appear in the menus used to add work items.

For the Inherited process model, you can only customize the following work item types: Test Plan, Test Suite, and Test Case.

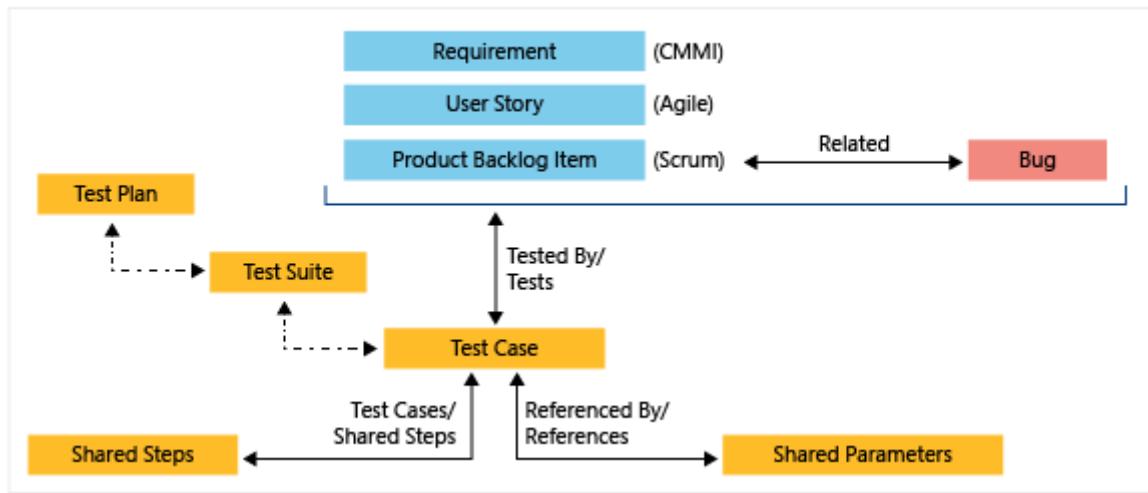
[+] Expand table

Scenario	Work item type	Description
Request code review	Code Review Request	Tracks information entered into the TFVC New Code Review form. For more information, see <a href="#">Get your code reviewed with Visual Studio</a> .

Scenario	Work item type	Description
Provide code review	Code Review Response	Tracks review comments provided by code reviewers in <a href="#">response to a code review request</a> .
Request feedback	Feedback Request	Tracks information entered into a request feedback form. Use the following forms to initiate a feedback request. <ul style="list-style-type: none"> <li>- <a href="#">Request stakeholder feedback</a></li> <li>- <a href="#">Get feedback</a>.</li> </ul>
Provide feedback	Feedback Review	Lets stakeholders <a href="#">provide feedback</a> based on requests for feedback or by <a href="#">volunteering feedback</a> using the <a href="#">Microsoft Test &amp; Feedback</a> Marketplace extension.
Manual testing	Test Plan	Groups one or more test suites and individual test cases together. Test plans include static test suites, requirement-based suites, and query-based suites. To get started, see <a href="#">Create test plans and test suites</a> .
Manual testing	Test Suite	Groups one or more test cases into separate testing scenarios within a single test plan. Grouping test cases makes it easier to see which scenarios are complete.
Manual testing	Test Case	Defines steps used to validate individual parts of your code to ensure your code works correctly, has no errors, and meets business and customer requirements. You can <a href="#">add individual test cases</a> to a test plan without creating a test suite. More than one test suite or test plan can refer to a test case. You can effectively reuse test cases without having to copy or clone them for each suite or plan.
Manual testing	Shared Steps	Enables <a href="#">sharing steps across several test cases</a> .
Manual testing	Shared Parameters	Enables <a href="#">repeating the same test cases with different data</a> .

## Test work item types

Work item types that support the test experience are linked together using the link types shown in the following image. These types include *Tested By/Tests*, *Test Cases/Shared Steps*, and *Reference By/References*.



You can use the web portal to see the test cases that are defined for a test suite, and the test suites that are defined for a test plan. But, there's no specific link type that connects these objects to each other.

## Track bugs

The Bug work item type supports the following integrations that you should be aware of when you're tracking bugs.

  Expand table

Scenario	Description
Create a bug from a testing tool	You can add a bug from Test Runner or the Test & Feedback extension. For more information, see <a href="#">Define, capture, triage, and manage bugs</a> .
Create inline tests linked to bugs or user stories	When your team tracks bugs as requirements, you can use the board to <a href="#">add tests</a> to verify bug fixes or user stories.
Track build information with bugs	The Bug work item form contains System Info, Found in Build, and Integrated in Build, which support tracking code defects found and resolved within pipeline builds. For more information, see <a href="#">Query based on build and test integration fields</a> .

## Azure Pipelines and Azure Test Plans integration

Azure Test Plans is fully integrated with Azure Pipelines to support testing within continuous integration/continuous deployment (CI/CD). You can associate test plans and test cases with build or release pipelines. Add pipeline tasks to pipeline definitions to capture and publish test results. Review test results via built-in progress reports and

pipeline test reports. The following table summarizes the integration points between Azure Pipelines and Azure Test Plans.

[+] Expand table

Feature	Description
Test plans setting	With test plan settings, you can <a href="#">configure the Test Run settings</a> to associate build or release pipelines and Test Outcome settings.
Pipeline test-enable tasks	Specify test-enable tasks within a pipeline definition. Azure Pipelines provides several tasks, including the following tasks, that support a comprehensive test reporting and analytics experience. <ul style="list-style-type: none"><li>- <a href="#">Publish Test Results task</a>: Use to publish test results to Azure Pipelines.</li><li>- <a href="#">Visual Studio Test task</a>: Use to run unit and functional tests (Selenium, Appium, Coded UI test, and more) using the Visual Studio Test Runner.</li><li>- <a href="#">.NET Core CLI task</a>: Use to build, test, package, or publish a dotnet application.</li></ul> For other tasks, see <a href="#">Publish Test Results task</a>
Run automated tests in build pipelines	<a href="#">Associate test plans with a build pipeline</a> so that they run with each build.
Associate automated tests with test cases	<a href="#">Associate automated tests with test cases</a> .
Set retention policy for automated test results associated with builds	You can <a href="#">set the test retention policy</a> for automated builds from the <a href="#">Pipelines &gt; Retention</a> page.
Requirements traceability	The Requirements quality widget supports tracking quality continuously from a build or release pipeline. The widget shows the mapping between a requirement and latest test results executed against that requirement. It provides insights into <a href="#">requirements traceability</a> .
Test results trend	The Test results trend configurable widget displays the trend of test results for the selected build or release pipeline. The widget helps you visualize the test trends over a period of time, surfacing patterns about test failures, test duration, and so on. For more information, see <a href="#">Configure the Test Results Trend (Advanced) widget</a>
Deployment status	The Deployment status configurable widget shows a combined view of the deployment status and test pass rate across multiple environments for a recent set of builds. You configure the widget by specifying a build pipeline, branch, and linked release pipelines. To view the test summary across multiple environments in a release, the widget provides a matrix view of each environment and corresponding test pass rate. See <a href="#">Associate automated tests with test cases</a>

Feature	Description
View test results in builds and releases	Both build and release summaries provide details of test execution. <a href="#">Review these summaries</a> to assess pipeline quality, review traceability, and troubleshoot failures. Choose <b>Test summary</b> to view the details in the <b>Tests</b> tab.
Test analytics for builds	Each build summary includes an <b>Analytics</b> tab that hosts the <a href="#">Test analytics</a> report.

## Dashboards, reporting, and Analytics

[Dashboards](#) provide an easy way to monitor progress and status. Teams can add configurable widgets to support their goals. The [Analytics service](#) is the reporting platform for Azure DevOps, and replaces the previous platform based on SQL Server Reporting Services. Analytics is optimized for fast read-access and server-based aggregations and provides the following benefits:

- Analytics widgets that you can add to your dashboards
- In-context Analytics reports available from select Azure DevOps pages
- Rollup bars and counts for Azure Boards backlogs
- Custom reports you can create using Power BI
- Custom reports you can create using OData queries
- Support to develop and add your custom Analytics widgets you can add to dashboards

You can add the following built-in widgets to your dashboard. They're organized under the service they support. You might find more widgets from the [Azure DevOps Marketplace](#).

## Data available from Analytics

Analytics provides the reporting platform for Azure DevOps. For information, see [Data available from Analytics](#).

## Automation and connectors

Microsoft products support automation or integration with several other applications and services. For more information, see the following articles.

- [Power Automate, Azure DevOps](#)
- [Power Automate templates for Azure DevOps](#)

## Related articles

- End-to-end traceability
- Data model for Analytics
- GitHub integration

ⓘ Note: The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# About GitHub integration

Article • 03/05/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Azure Boards and Azure Pipelines offer multiple integration points with GitHub and GitHub Enterprise. These integrations enable seamless collaboration between development and project management, enhancing traceability, workflow efficiency, and overall productivity. By connecting your GitHub repositories with Azure DevOps, you can streamline your development processes and gain better insights into your projects.

## Authenticate and collaborate with GitHub

[⋮] [Expand table](#)

Feature	Description
<b>Sign into Azure DevOps using your GitHub credentials</b>	Allows users to sign in using their GitHub credentials and link their GitHub account to a Microsoft account. For more information, see <a href="#">Signing into Azure DevOps using your GitHub credentials (Release Notes)</a> .
<b>Invite GitHub collaborators into Azure DevOps</b>	Provides support for inviting GitHub account users to collaborate within an Azure DevOps project. For more information, see <a href="#">Invite GitHub collaborators into Azure DevOps (Release Notes)</a> .
<b>Connect to a GitHub repository from Visual Studio</b>	Provides a user interface to support cloning GitHub repositories, pushing and pulling commits, and more. For more information, see <a href="#">Side-by-side comparison of Git and Team Explorer</a> .

## Integrate Azure Boards with GitHub

By integrating Azure Boards with GitHub repositories, you can link GitHub commits, pull requests, branches, and issues to work items. This integration allows you to use GitHub for software development while using Azure Boards to plan and track your work. To get started, see [Azure Boards-GitHub integration](#).

## Benefits of integration

- **Enhanced traceability:** Link work items to GitHub commits, pull requests, branches, and issues for better traceability.

- **Streamlined workflow:** Use GitHub for development and Azure Boards for planning and tracking, ensuring a seamless workflow.
- **Improved collaboration:** Collaborate more effectively by connecting development activities in GitHub with project management in Azure Boards.

## Features of Azure Boards and GitHub integration

[+] [Expand table](#)

Feature	Description
Link work items	Easily link work items to GitHub commits, pull requests, branches, and issues.
View linked objects	Quickly view and open linked objects from the board.
Add status badges	Add status badges of Azure Boards to a GitHub repository README file.
View release summary	Review work items linked to GitHub commits in the Release summary page.
Sync GitHub issues	Sync GitHub Issues to Azure Boards Work Items using the <a href="#">GitHub Action</a> .

## Integrate Azure Pipelines with GitHub

You can use Azure Pipelines to automatically build, test, package, release, and deploy your GitHub repository code. To get started, see [Build GitHub repositories](#).

Additionally, you can map your GitHub repositories to one or more projects in Azure DevOps, enabling seamless integration and management across your development lifecycle.

## Benefits of integration

- **Automated workflows:** Automatically build, test, package, release, and deploy your GitHub repository code using Azure Pipelines.
- **Continuous integration and continuous deployment (CI/CD):** Implement CI/CD practices to ensure that your code changes are automatically tested and deployed.
- **Seamless integration:** Map your GitHub repositories to one or more projects in Azure DevOps for seamless integration and management across your development lifecycle.

- **Enhanced collaboration:** Collaborate more effectively by linking work items to GitHub commits, pull requests, branches, and issues.
- **Improved traceability:** Achieve better traceability by reviewing work items linked to GitHub commits in the release summary page.
- **Status badges:** Add status badges of Azure Boards to a GitHub repository README file and display the build status.
- **Issue synchronization:** Sync GitHub Issues to Azure Boards work items using the GitHub Action for better issue tracking and management.

## Features of Azure Pipelines and GitHub integration

[+] Expand table

Feature	Description
Create GitHub repository and pull request builds	<ul style="list-style-type: none"> <li>- Automatically build your GitHub pull requests. After the build is done, status is reported back with a comment in your GitHub pull request.</li> <li>- Manually run a pipeline or test suite triggered by a GitHub pull request comment.</li> <li>- Configure draft PR validation for GitHub repository. Supports adding <code>drafts</code> to the <code>pr</code> trigger YAML syntax for GitHub draft pull requests. You can choose if you want your draft PRs to queue a build. The default option is true (a build is queued) like it currently is for GitHub PRs.</li> <li>- Rebuild GitHub pull request builds upon failure. Provides support for queueing a failed build.</li> <li>- Configure draft PR validation for GitHub repositories.</li> <li>- Automatically build pull requests from repository forks to ensure changes successfully build and tests pass before they get merged. For more information, see <a href="#">Build GitHub repositories</a>.</li> </ul>
Create GitHub Enterprise builds	<ul style="list-style-type: none"> <li>- Supports continuous integration (CI) builds for GitHub Enterprise repositories.</li> <li>- Create a pipeline to build code contained within a GitHub Enterprise repository using the build pipeline wizard. For more information, see <a href="#">Build GitHub repositories, CI triggers</a>.</li> </ul>
Use GitHub service connections	The pipeline wizard automatically creates and reuses a service connection for the repository you choose. If you wish to manually choose a connection other than the one that is automatically selected, follow the <a href="#">Choose connection</a> hyperlink. For more information, see <a href="#">Build GitHub repositories</a> .
Manage GitHub releases	<ul style="list-style-type: none"> <li>- Inline GitHub connection as a release artifact source.</li> <li>- Automate GitHub releases using the <a href="#">GitHub Release</a> task.</li> <li>- Link your GitHub releases as an artifact source in release pipelines. This function lets you consume the GitHub release as part of your</li> </ul>

Feature	Description
	deployments. For more information, see <a href="#">CI triggers</a> , <a href="#">Download GitHub Release task</a> , and <a href="#">GitHub Release task</a> .
<b>Use build tags to trace GitHub sources or trigger GitHub releases</b>	<ul style="list-style-type: none"> <li>- Use build tags to trace GitHub sources to builds. While choosing a GitHub repository in a build definition, you can select the types of builds you want to tag, along with the tag format.</li> <li>- Specify a tag pattern to determine when to trigger a GitHub release. By specifying a tag regular expression, you can control when a GitHub release is created based on the triggering commit. For more information, see <a href="#">Build GitHub repositories</a>, <a href="#">Label sources</a>.</li> </ul>
<b>Support GitHub packages in YAML pipelines</b>	In your YAML pipeline, specify a package type (NuGet or npm) that you want to consume from GitHub. For more information, see <a href="#">Resources: packages</a> .
<b>Get status checks, tracking, and traceability</b>	<ul style="list-style-type: none"> <li>- <b>GitHub Checks:</b> <ul style="list-style-type: none"> <li>- Display status for each pipeline job: Run a pipeline or test suite to validate a GitHub pull request from the comments section of the GitHub pull request.</li> <li>- Send detailed information about the pipeline status, test, code coverage, and errors. Status is posted to GitHub Checks for each job in the pipeline.</li> </ul> </li> <li>- <b>Status badges:</b> Add Markdown syntax to a GitHub repo README.md file and display the pipeline status.</li> <li>- <b>GitHub artifacts:</b> Show associated commits deployed in a release. To enhance traceability, you can see all the commits that were deployed to an environment for GitHub repositories, as a part of a specific release.</li> <li>- Track GitHub commits and associated issues in releases. List commits made in GitHub repos and the associated GitHub issues that are being deployed with a release. For more information, see <a href="#">Track GitHub commits and associated issues in releases (Release Notes)</a>. For more information, see: <ul style="list-style-type: none"> <li>- <a href="#">Create your first pipeline</a>, <a href="#">Add a status badge to your repository</a></li> <li>- <a href="#">GitHub Checks API ↗</a></li> <li>- <a href="#">Display status for each pipeline job in GitHub Checks (Release Notes)</a></li> </ul> </li> </ul>

## Related articles

- [Azure Boards-GitHub integration](#)
- [Build GitHub repositories](#)
- [Git experience in Visual Studio](#)

ⓘ **Note:** The author created this article with assistance from AI. [Learn more](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Deploy to Azure services

Article • 07/15/2024

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Azure Pipelines combines continuous integration (CI) and continuous delivery (CD) to test and build your code and ship it to any target. While you don't have to use Azure services with Azure Pipelines, you can use Azure Pipelines to integrate your CI/CD process with most Azure services. Azure Pipelines CI/CD helps you take the best advantage of your Azure services.

The following articles describe how different Azure services support CI and CD with Azure Pipelines.

### Azure App Configuration

- [Push settings to App Configuration with Azure Pipelines](#)
- [Pull settings from App Configuration with Azure Pipelines](#)

### Azure App Service

- [Deploy to App Service using Azure Pipelines](#)
- [Deploy a custom container to Azure App Service with Azure Pipelines](#)
- [Use Azure Pipelines to build and deploy a Python web app to Azure App Service](#)

### Azure Container Registry

- [Build and push Docker images to Azure Container Registry](#)

### Azure Cosmos DB

- [Set up a CI/CD pipeline with the Azure Cosmos DB Emulator build task in Azure DevOps](#)

### Azure Data Factory

- [Configure Azure Databricks and Azure Data Factory](#)

### Azure Government

- [Deploy an app in Azure Government with Azure Pipelines](#)

### Azure IoT Edge

- [Continuous integration and continuous deployment to Azure IoT Edge devices](#)

## Azure Kubernetes Service

- Build and deploy to Azure Kubernetes Service with Azure Pipelines

## Azure Monitor

- Query Azure Monitor Alerts

## Azure Database for MySQL - Flexible Server

- Azure Pipelines for Azure Database for MySQL - Flexible Server

## Azure Service Fabric

- Tutorial: Set up CI/CD for a Service Fabric application by using Azure Pipelines

## Azure Static Web Apps

- Quickstart: Build your first static web app

## Azure SQL Database

- Deploy to Azure SQL Database

## Azure Virtual Machines

- Quickstart: Use an ARM template to deploy a Linux web app to Azure
- Deploy to Azure VMs using deployment groups in Azure Pipelines
- Tutorial: Deploy a Java app to a virtual machine scale set

For a complete list of Azure Pipelines tasks, see [Build and release tasks](#) and the [Azure Pipelines task reference](#).

---

## Feedback

Was this page helpful?



Provide product feedback

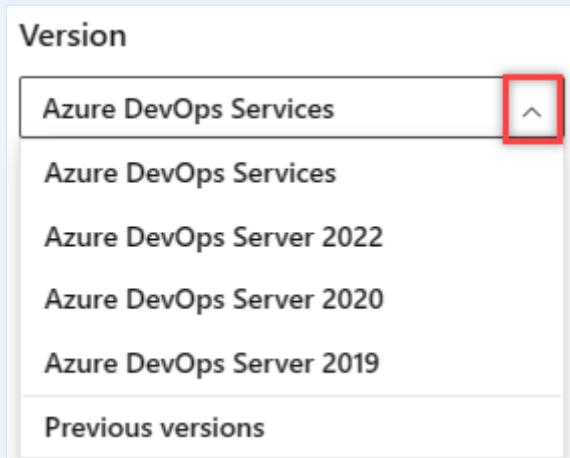
# Navigate the Azure DevOps web portal

Article • 03/25/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

The Azure DevOps web portal is organized into various services, administrative pages, and task-specific features like the search box. Service labels vary depending on whether you're using Azure DevOps Services or an on-premises version.

## Important



Select the version of this article that corresponds to your platform and version. The version selector is above the table of contents. [Look up your Azure DevOps platform and version.](#)

Each service offers multiple pages with numerous features and functional tasks. Within each page, you can choose options to select or add specific artifacts.

## Key features and navigation

Here's what you need to know to start using the web portal effectively.

- **Open a service, page, or settings:** Use to switch to a different [service or functional area](#)
- **Add an artifact or team:** Use to quickly add a work item, Git repo, build or release pipelines, or a new team
- **Open another project or repo:** Use to switch to a different project or access work items and pull requests defined in different projects, or your favorite items
- **Open team artifacts, use breadcrumbs, selectors and directories:** Use to navigate within a service, open other artifacts, or return to a root function
- **Work with favorites:** Mark your favorite artifacts for quick navigation

- **Search box:** Use to find code, work items, or wiki content
- **Your profile menu:** Use to set personal preferences, notifications, and enable preview features
- **Settings:** Use to add teams, manage security, and configure other project and organization level resources.

**! Note**

Only enabled services are visible in the user interface. For example, if **Boards** is disabled, then **Boards** or **Work** and all pages associated with that service don't appear. To enable or disable a service, see [Turn an Azure DevOps service on or off](#).

Select services—such as **Boards**, **Repos**, and **Pipelines**—from the sidebar and pages within those services.

ID	Title	State	Title
375	Check service status	New	New
492	Develop form	In Progress	Build Settings Experience
543	Auto-save	To Do	Develop form
372	Standardize	To Do	To Do
539		In Progress	Auto-save

Now that you understand the user interface structure, it's time to start using it. You can find a wide range of features and functionalities to explore.

If all you need is a code repository and bug tracking solution, then start with [Get started with Git](#) and [Manage bugs](#).

To start planning and tracking work, see [About Agile tools](#).

# Connect to the web portal, user accounts, and licensing

You connect to the web portal through a supported web browser—such as the latest versions of Microsoft Edge, Chrome, Safari, or Firefox. Only users [added to a project](#) can connect, which is typically done by the organization owner.

Five account users are free as are Visual Studio subscribers and stakeholders. After that, you need to [pay for more users](#). Find out more about licensing from [Azure DevOps pricing](#).

Limited access is available to an unlimited number of stakeholders for free. For details, see [Work as a Stakeholder](#).

## Refresh the web portal

If data doesn't appear as expected, the first thing to try is to refresh your web browser.

Refreshing your client updates the local cache with changes that were made in another client or the server. To refresh the page or object you're currently viewing, refresh the page or choose the  Refresh icon if available.

To avoid potential errors, you should refresh your client application in the following scenarios:

- Process change applied
- Work item type definition added, removed, renamed, or updated
- Area or iteration path added, removed, renamed, or updated
- User added or removed in security groups, or user permissions updated
- New shared query added or existing shared query updated
- Build definition added or deleted
- Team or project added or deleted

## Differences between the web portal and Visual Studio

Although you can access source code, work items, and builds from both clients, some task specific tools are only supported in the web browser or an IDE but not in both. Supported tasks differ depending on whether you connect to a Git or TFVC repository from Team Explorer.

- Product backlog, Portfolio backlogs, Sprint backlogs, Taskboards, Capacity planning
- Boards
- Dashboards, Widgets, Charts
- Request feedback
- Web-based Test Management
- Administration pages to administer accounts, team projects, and teams
- Git: Changes, Branches, Pull Requests, Sync, Work Items, Builds
- TFVC: My Work, Pending Changes | Source Control Explorer, Work Items | Builds
- Greater integration with work items and Office integration clients. You can open a work item or query result in an office supported client.

---

 Note

Visual Studio 2019 version 16.8 and later provide a Git menu for managing the Git workflow with less context switching than Team Explorer. Procedures in this article under the Visual Studio tab describe how to use the Git experience and also Team Explorer. For more information, see [Side-by-side comparison of Git and Team Explorer](#).

## Related articles

- [Manage projects](#)
- [Manage settings for projects and organizations](#)

# Open a service, page, or settings

Article • 01/28/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

The web portal for Azure DevOps provides support for software development teams to collaborate through the planning, development, and release cycles. You can manage source code, plan and track work, define builds, run tests, and manage releases.

This article shows you how to navigate to functional and administrative tasks available from the web portal. There are three levels of administrative tasks: team, project, and organization.

## Prerequisites

**Permissions:** Member of the [Project Collection Administrators group](#). Organization owners are automatically members of this group.

## Open a service or functional task page

Services support getting work done—managing code, planning and tracking work, defining and managing pipelines, creating and running tests, and so on.

### Note

Only those services that are enabled appear in the user interface. For example, if **Boards** is disabled, then **Boards** or **Work** and all pages associated with that service don't appear. To enable or disable a service, see [Turn an Azure DevOps service on or off](#).

You open a service by choosing the service from the sidebar and then selecting from the available pages.

For example, here we select **Boards** > **Backlogs**.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar includes links for 'Overview', 'Boards', 'Backlogs' (which is selected), 'Sprints', 'Queries', 'Repos', and 'Pipelines'. The main area displays a backlog board titled 'Web' with 8 items. The columns are 'Order', 'Work item Type', and 'Title'. The items are:

Order	Work item Type	Title
1	Product Backlog Item	Hello World Web Site
2	Bug	Slow response on information form
3	Product Backlog Item	Change initial view
4	Product Backlog Item	Interim save on long form
5	Bug	Canadian addresses don't display correctly
6	Product Backlog Item	Hello World Web Site
7	Product Backlog Item	GSP locator interface
8	Product Backlog Item	Request support

Within the page you might select a specific view or artifact, such as a team backlog or choose another page.

## Open team settings

Select configurations are made to teams through the team settings pages. For an overview of all team settings, see [About user, team, project, and organization-level settings](#).

1. Choose **Project settings**.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. The left sidebar contains a navigation menu with items like 'Overview', 'Summary' (which is selected and highlighted in grey), 'Dashboards', 'Wiki', 'Boards', 'Repos', 'Pipelines', 'Test Plans', 'Artifacts', and 'Project settings'. The 'Project settings' item is highlighted with a red box. The main content area features a large 'FabrikamFiber' logo, a 'Private' status indicator, and an 'Invite' button. Below this is a cartoon illustration of a person sitting at a desk with a laptop, accompanied by a dog. The text 'Welcome to the project!' is displayed prominently. A section titled 'What service would you like to start with?' offers links to 'Boards', 'Repos', 'Pipelines', 'Test Plans', and 'Artifacts'. At the bottom right, there is a link to 'or manage your services'.

2. Expand Boards and choose Team configuration.

Project Settings > Team configuration > Fabrikam Team

General

- Overview
- Services
- Teams
- Security
- Notifications
- Service hooks
- Dashboards

Boards

This project is currently using the MyScrum process. To customize your work item types, go to the process customization page.

General Iterations Areas Templates

Backlogs

See only the backlogs your team manages.

Backlog navigation levels

- Epics
- Features
- Backlog items

Working days

Capacity and burndown are based on the days your team works.

Select days

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

- Choose one of the pages **General**, **Iterations**, **Areas**, or **Templates** to configure settings for the team. For more information, see [Manage teams](#).
- If you need to switch to a different team, use the team selector within the breadcrumbs.

/ Settings / Teams / **Fabrikam Fiber Team**

Team Profile



Name  
Fabrikam Fiber Team

Description  
The default project team.

Customer Service (Fabrikam Fiber) ★

Fabrikam Fiber Team (Fabrikam F...)

+ Add... |

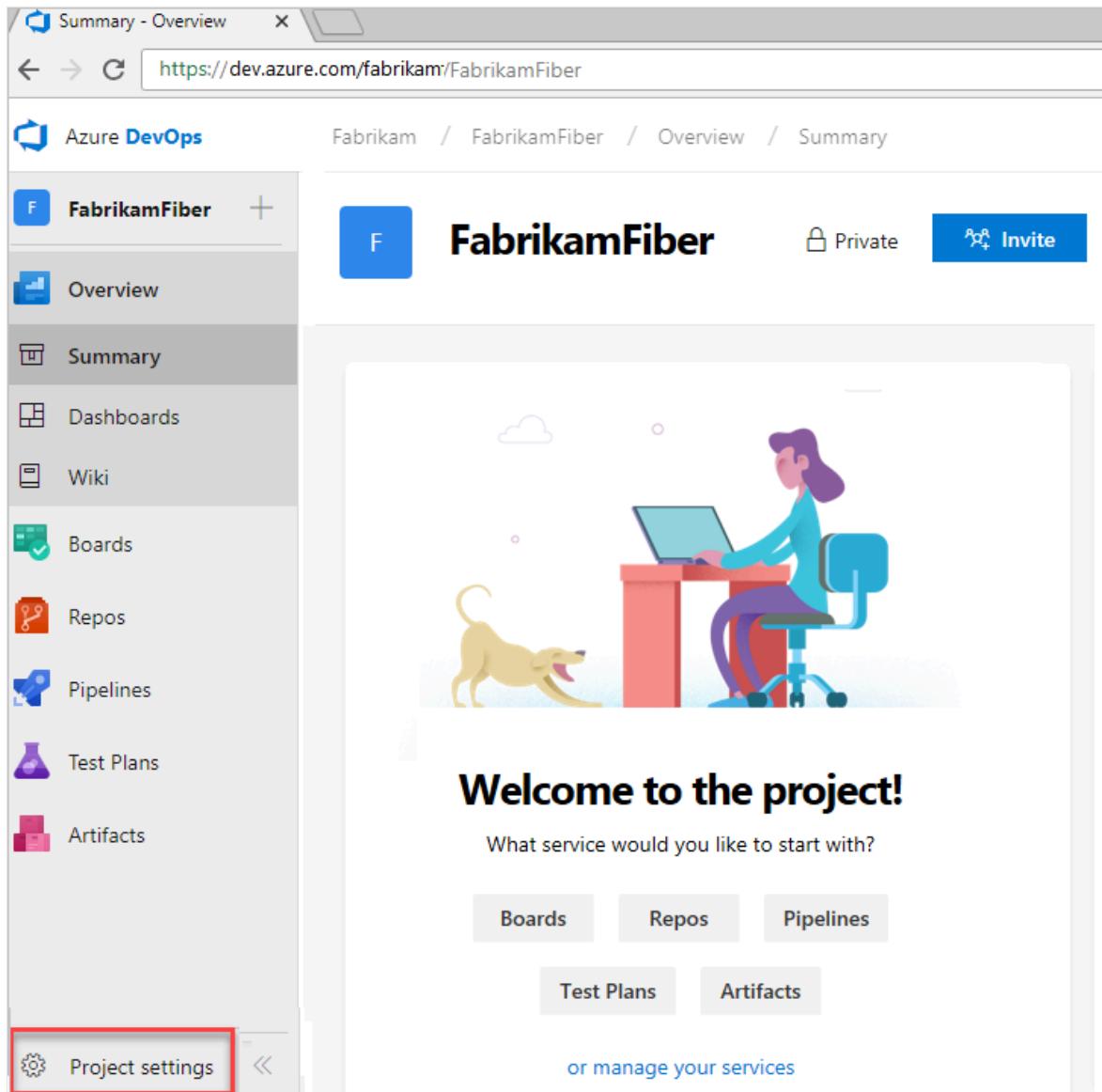
Display Name	Username Or Scope
Jamal Hartnett	fabrikamfiber4@hotmail.com

- To add a team administrator, add team members, or change the team profile, choose **Teams** from the vertical sidebar, and then choose the name of the team you want to configure.

# Open project settings

Administrators configure resources for a project and manage project-level permissions from the **Project settings** pages. Tasks performed in this context can impact the project and team functions. For an overview of all project settings, see [Project administrator role and managing projects](#).

1. Choose **Project Settings**.



2. From there, you can choose a page from the list. Settings are organized based on the service they support, such as **Boards**, **Pipelines**, **Repos**, and **Test**.

# Open Organization settings

Organization owners and members of the Project Collection Administrators group configure resources for all projects or the entire organization, including adding users, from the Organization settings pages. This includes managing permissions at the

organization-level. For an overview of all organization settings, see [Project collection administrator role and managing collections of projects](#).

From there, you can choose a page from the list of settings. Settings are organized based on the service they support, such as **Boards**, **Repos**, **Pipelines**, and **Artifacts**.

## Related articles

- [Manage projects](#)
  - [About team, project, and admin settings](#)
- 

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Add an artifact or team artifacts

Article • 01/28/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Select the service of interest to get started adding new artifacts or objects. For example, to add work items, choose **Boards** or **Work**. Some artifacts—such as a product backlog, board, portfolio backlogs—are added when you add a team.

Prior to adding an artifact, make sure that you've [selected the project and repository](#) that you want to work in.

## Prerequisites

[ ] [Expand table](#)

Category	Requirements
Project access	<a href="#">Project member</a> .
Permissions	<ul style="list-style-type: none"><li>- Member of the <b>Contributors</b> or <b>Project Administrators</b> security group.</li><li>- To view or modify work items: <a href="#">View work items in this node</a> and <a href="#">Edit work items in this node</a> permissions set to <b>Allow</b>. By default, the <b>Contributors</b> group has this permission set to <b>Allow</b>. For more information, see <a href="#">Set work tracking permissions</a>.</li></ul>
Access levels	To add or modify work items: At least <b>Basic access</b> . Users with <b>Stakeholder</b> access for public projects have full access to backlog and board features, like users with <b>Basic</b> access. For more information, see <a href="#">Stakeholder access quick reference</a> .
Defined iterations	To use the <b>Planning</b> pane: Ensure your team administrator <a href="#">defined iteration (sprint) paths and configure team iterations</a> .

There might be other prerequisites for managing specific items. For more information, see [Security groups, service accounts, and permissions reference](#).

## Add work items, queries, or other work tracking artifacts

You can quickly add a query or work item when working from a **Boards** or **Work** page.

Choose a **Boards** page—such as **Work Items**, **Boards**, or **Backlogs**. Then choose the **+** plus icon and select from the menu of options.

ID	Title	State
368	Change background color	Approved
390	Cancel order form	Committed
492	Build Settings Experience	New

To add other work tracking artifacts, see one of the following articles:

- To add a board, backlog, or sprint backlog, first [add a team](#) which will be associated with those artifacts
- [Add a delivery plan](#)
- [Add a managed work item query](#)
- [Add work items](#).

## Add a pull request or Git repository

You can quickly add a pull request, Git repository, or work item using the **Add** menu when working from **Code**.

Expand the **Repos** service and choose **Files**, **Commits**, or **Pull Requests** (Git repos) or **Files**, **Changesets**, or **Shelvesets** (TFVC). Then, choose the **+** plus icon and select from the menu of options.

Azure DevOps interface showing the 'fabrikam / Fabrikam Fiber / Code / Files' path. The 'Fabrikam Fiber' project is selected. A red box highlights the '+' icon in the top navigation bar. A red arrow points from the project name to this icon. A red box also highlights the 'New repository' option in the dropdown menu that appears when the '+' icon is clicked.

For details on adding a Git repository, see [Git repository](#).

Note that you can only add one TFVC repository per project, but an unlimited number of Git repositories. To learn more about Git artifacts, see one of the following articles:

- [Git repository](#)
- [Git branch](#)
- [Git pull request](#)
- [Add work items](#)

## Add build and release pipelines

Expand **Pipelines** and choose **Builds** or **Releases**. Then choose the **+** plus icon and select from the menu of options.

Azure DevOps interface showing the 'fabrikam / Fabrikam Fiber / Build and release / Builds' path. The 'Fabrikam Fiber' project is selected. A red box highlights the '+' icon in the top navigation bar. A red arrow points from the project name to this icon. A red box also highlights the 'New build pipeline' option in the dropdown menu that appears when the '+' icon is clicked.

For more information about adding other pipeline related artifacts, see the following articles:

- Deployment groups
- Task groups
- Variable groups
- Secure files

## Add a team

Agile tools and dashboards are typically associated with teams. You add teams to a project. To learn more about teams, see [About teams and Agile tools](#). To add a team, see [Add a team and team members](#).

## View teams already defined

To view the set of defined teams, open **Project settings**, and choose **Overview**.

The screenshot shows the Azure DevOps interface for a project named 'Fabrikam Fiber'. The left sidebar has links for Overview, Boards, Repos, Pipelines, Test Plans, Artifacts, and Project settings. The 'Project settings' link is highlighted with a red box. The main content area shows 'Project Settings > Teams'. A secondary navigation menu on the left lists General, Overview, Services, Teams (which is also highlighted with a red box), Security, Notifications, Service hooks, and Dashboards. The main pane displays a table of teams with columns for Team Name, Members, and Description. The teams listed are Customer Service (7 members), Fabrikam Fiber Team (7 members), Management team (1 member), Phone (1 member), Voice (1 member), and Web (2 members).

Team Name	Members	Description
Customer Service	7	
Fabrikam Fiber Team	7	
Management team	1	
Phone	1	
Voice	1	
Web	2	

## Add a dashboard

Dashboards are associated with a team or a project. Each team can create and configure a number of dashboards. And, any team member can create one or more project dashboards. To learn how, see [Add a dashboard](#).

## Add a wiki

If you don't have a wiki yet, you can add one. Once added, you can add and update pages to that wiki.

- [Create a wiki](#)
- [Add and edit wiki pages](#)
- [Publish a Git repository to a wiki](#)

## Related articles

- [Azure Artifacts](#)
- [Exploratory & Manual Testing](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Switch project, repository, team

Article • 01/28/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Several features depend on the project, repository, or team that you have selected. For example, dashboards, backlogs, and board views will change depending on the project and team you select.

Also, when you add a work item, the system references the default area and iteration paths defined for the team context. Work items you add from the team dashboard (new work item widget) and queries page are assigned the team default iteration. Work items you add from a team backlog or board, are assigned the team default backlog iteration. For more information, see [About teams and Agile tools](#).

## Prerequisites

 Expand table

Category	Requirements
Permissions	At least <a href="#">Contributor role</a> .

### Note

If the **Limit user visibility and collaboration to specific projects** preview feature is enabled for the organization, users added to the **Project-SScoped Users** group won't be able to access projects that they haven't been added to. For more information including important security-related call-outs, see [Manage your organization, Limit user visibility for projects and more](#).

## View and open a project

From the **Projects** page you can quickly navigate to a project that you have permissions to view.

1. Choose the  Azure DevOps logo to open **Projects**.

The screenshot shows the Azure DevOps interface. At the top, there's a navigation bar with a back arrow, forward arrow, refresh icon, a star icon, and three dots. The URL in the address bar is <https://dev.azure.com/fabrikamfiber/Fabrikam%20Fiber>. Below the address bar, the Azure DevOps logo is highlighted with a red box. The page title is "Summary - Summary". The breadcrumb navigation shows "fabrikam / Fabrikam Fiber / Overview / Summary". On the left, a sidebar lists "Fabrikam Fiber" (selected), "Overview", "Boards", "Repos", "Pipelines", and "Test Plans". The main content area features a large teal square with the letters "FF". To its right, the text "Fabrikam Fiber" is displayed with a yellow star icon. Below that, it says "Web, voice, and phone apps". There's a "Add tags" button. A list of items follows: "Fabrikam Fiber / README.md" (with a file icon), "minor modification to test development section in mobile form", "Update this README.md file.", and a note about README.md files being intended to quickly orient readers to what your project is about.

The projects you most recently viewed are displayed, followed by a list of all projects in alphabetic order.

2. Hover over the dots and you can open the service of interest for that project.

# Projects

Filter projects

+ Create project

FF

Fabrikam Fiber

Web, voice, and phone apps

M

MyFirstProject

All projects

A1

Agile 11

New agile project

D1

Demo 11

Agile team project



FF

Fabrikam Fiber

Web, voice, and phone apps



M

MyFirstProject



3. You can filter the project and team list using the *Filter projects* search box. Simply type a keyword contained within the name of a project or team. Here we type **Fabrikam** to find all projects or teams with *Fabrikam* in their name.

## Projects

Fabrikam

+ Create project

FF

**Fabrikam Fiber**

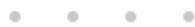
Web, voice, and phone apps



FT

**Fabrikam Test**

Project used to verify MyAgile process customizations



F

**FabrikamFiber**

Customer-focused apps under development based on Agile process.



4. Choose **Create Project** to add a project. Be an account administrator or a member of the Project Collection Administrators group to [add a project](#).

The screenshot shows the 'Projects' page within a project collection. On the left, there's a sidebar titled 'My accounts' listing three accounts: 'fabrikamfib' (selected), 'FabrikamFiber', and 'fabrikam-fiber'. The main area is titled 'Projects' and contains two project cards. The first card is for 'Fabrikam Fiber' (Web, voice, and phone apps) and the second is for 'MyFirstProject'. A search bar labeled 'Filter projects' and a blue 'Create project' button are also visible. The 'Create project' button is highlighted with a red box.

## View and open a repository

1. Choose **Repos>Files**.

A screenshot of the Azure DevOps interface showing a repository named 'MyGreatLibrary2'. The left sidebar has a 'Files' tab highlighted with a red box. The main area shows the contents of the 'MyGreatLibrary2' folder, including subfolders 'MyGreatLibrary.Tests' and 'Properties', and files '.gitattributes', '.gitignore', 'Class1.cs', 'MyGreatLibrary.csproj', and 'MyGreatLibrary.sln'. A red box highlights the repository selector at the top right.

2. Select the repository of interest from the repository selector.

A screenshot of the Azure DevOps interface showing the repository selector expanded. A red box highlights the repository selector at the top right. A red arrow points from the repository selector to the expanded list of repositories below. The list includes 'breadth-of-trees', 'Compose', 'GVFS', 'MyGreatLibrary', 'MyGreatLibrary2' (which is highlighted with a red box), 'RedBot', 'Specs', 'VSCode', '+ New repository', '↑ Import repository', and 'Manage repositories'. The 'MyGreatLibrary2' entry has a yellow star icon next to it.

## Switch to a different team

From a user page, one under—**Boards, Repos, Pipelines, or Test Plans**—you can't switch to a different team, you can [only select team artifacts](#).

From a **Project Settings>Work>Team configuration** page, you select a team from the team selector breadcrumb.

Project Settings > Team configuration > **Fabrikam Fiber Team**

General Work Backlogs

See only the backlog

Backlog navigation

Epics     Features     Backlogs

**Fabrikam Fiber Team (Fabrikam Fib...)**

Management team (Fabrikam Fiber)

Email (Fabrikam Fiber)

Working days

Capacity and burndown are based on the days your team works.

Select days

Monday     Tuesday

## Related articles

- [Work across projects](#)
- [Add teams](#)

# Switch project, repository, team

Article • 01/28/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Several features depend on the project, repository, or team that you have selected. For example, dashboards, backlogs, and board views will change depending on the project and team you select.

Also, when you add a work item, the system references the default area and iteration paths defined for the team context. Work items you add from the team dashboard (new work item widget) and queries page are assigned the team default iteration. Work items you add from a team backlog or board, are assigned the team default backlog iteration. For more information, see [About teams and Agile tools](#).

## Prerequisites

 Expand table

Category	Requirements
Permissions	At least <a href="#">Contributor role</a> .

### Note

If the **Limit user visibility and collaboration to specific projects** preview feature is enabled for the organization, users added to the **Project-SScoped Users** group won't be able to access projects that they haven't been added to. For more information including important security-related call-outs, see [Manage your organization, Limit user visibility for projects and more](#).

## View and open a project

From the **Projects** page you can quickly navigate to a project that you have permissions to view.

1. Choose the  Azure DevOps logo to open **Projects**.

The screenshot shows the Azure DevOps interface. At the top, there's a navigation bar with icons for back, forward, refresh, and search, followed by a secure connection indicator and the URL <https://dev.azure.com/fabrikamfiber/Fabrikam%20Fiber>. Below the URL is a star icon and a gear icon. The main header says "Azure DevOps" with a blue square icon, followed by "fabrikam / Fabrikam Fiber / Overview / Summary". On the left, a sidebar lists "Fabrikam Fiber" (selected), "Overview", "Boards", "Repos", "Pipelines", and "Test Plans". The main content area features a large teal box with the letters "FF". To its right, the text "Fabrikam Fiber" is displayed with a yellow star icon, followed by "Web, voice, and phone apps". Below this is a button labeled "Add tags". A list of items follows, starting with "Fabrikam Fiber / README.md" with a red diamond icon. The list continues with "minor modification to test development section in mobile form", "Update this README.md file.", and a note about Markdown.

- Fabrikam Fiber / README.md
- minor modification to test development section in mobile form
- Update this README.md file.
- A README.md file is intended to quickly orient readers to what your project

[Learn more](#) ↗ about Markdown.

The projects you most recently viewed are displayed, followed by a list of all projects in alphabetic order.

2. Hover over the dots and you can open the service of interest for that project.

# Projects

Filter projects

+ Create project

FF

Fabrikam Fiber

Web, voice, and phone apps

M

MyFirstProject

All projects

A1

Agile 11

New agile project

D1

Demo 11

Agile team project



FF

Fabrikam Fiber

Web, voice, and phone apps



M

MyFirstProject



3. You can filter the project and team list using the *Filter projects* search box. Simply type a keyword contained within the name of a project or team. Here we type **Fabrikam** to find all projects or teams with *Fabrikam* in their name.

## Projects

Fabrikam

+ Create project

FF

**Fabrikam Fiber**

Web, voice, and phone apps



FT

**Fabrikam Test**

Project used to verify MyAgile process customizations



F

**FabrikamFiber**

Customer-focused apps under development based on Agile process.



4. Choose **Create Project** to add a project. Be an account administrator or a member of the Project Collection Administrators group to [add a project](#).

The screenshot shows the 'Projects' page within a project collection. On the left, there's a sidebar titled 'My accounts' listing three accounts: 'fabrikamfib' (selected), 'FabrikamFiber', and 'fabrikam-fiber'. The main area is titled 'Projects' and contains two project cards. The first card is for 'Fabrikam Fiber' (Web, voice, and phone apps) and the second is for 'MyFirstProject'. A search bar labeled 'Filter projects' and a blue 'Create project' button are also visible. The 'Create project' button is highlighted with a red box.

## View and open a repository

1. Choose **Repos>Files**.

A screenshot of the Azure DevOps interface showing a repository named 'MyGreatLibrary2'. The left sidebar has a 'Files' tab highlighted with a red box. The main area shows the contents of the 'MyGreatLibrary2' folder, including 'MyGreatLibrary.Tests', 'Properties', '.gitattributes', '.gitignore', 'Class1.cs', 'MyGreatLibrary.csproj', and 'MyGreatLibrary.sln'. A red box highlights the repository selector at the top right.

2. Select the repository of interest from the repository selector.

A screenshot of the Azure DevOps interface showing the repository selector expanded. A red box highlights the repository selector at the top right. A red arrow points from the repository selector to the expanded list of repositories below. The list includes 'breadth-of-trees', 'Compose', 'GVFS', 'MyGreatLibrary', 'MyGreatLibrary2' (which is highlighted with a red box), 'RedBot', 'Specs', 'VSCode', '+ New repository', '↑ Import repository', and 'Manage repositories'. The 'MyGreatLibrary2' entry has a yellow star icon next to it.

## Switch to a different team

From a user page, one under—**Boards, Repos, Pipelines, or Test Plans**—you can't switch to a different team, you can [only select team artifacts](#).

From a **Project Settings>Work>Team configuration** page, you select a team from the team selector breadcrumb.

Project Settings > Team configuration > **Fabrikam Fiber Team**

General Work Backlogs

See only the backlog

Backlog navigation

Epics     Features     Backlogs

**Fabrikam Fiber Team (Fabrikam Fib...)**

Management team (Fabrikam Fiber)

Email (Fabrikam Fiber)

Working days

Capacity and burndown are based on the days your team works.

Select days

Monday     Tuesday

## Related articles

- [Work across projects](#)
- [Add teams](#)

# Set personal or team favorites

Article • 01/28/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

As your code base, work tracking, developer operations, and organization grow, quickly navigating to important views becomes essential, which setting favorites helps with.

Favorite  the views you frequently access. You can favorite various Azure DevOps features and tools, such as projects, repositories, build pipelines, dashboards, backlogs, boards, or queries. Favorites can be set for yourself or your team.

Team favorites allow members to quickly access shared resources. Favorite an item for yourself by selecting the  star icon. The favorite item appears in one or more directory lists. Set team favorites through the context menu for the definition, view, or artifact.

## Prerequisites

 Expand table

Category	Requirements
Permissions	Member of the <b>Contributors</b> group or an administrative security group for the project.
Access levels	<ul style="list-style-type: none"><li>- To favorite projects, backlogs, boards, queries, dashboards, or pipeline views: At least <b>Stakeholder</b> access.</li><li>- To favorite repositories or delivery plans: At least <b>Basic</b> access.</li><li>- To favorite test plans: <b>Basic + Test Plans</b> or equivalent.</li></ul>

For more information, see [About access levels](#).

## View personal favorites

Access your personal favorites by choosing the  inbox icon, and then choosing **Favorites**.

The screenshot shows the 'Favorites' section of the Azure DevOps interface. At the top, there are navigation links for 'Work Items', 'Pull requests', and 'Favorites'. The 'Favorites' link is highlighted with a red box. Below this, the page is organized into sections: 'Projects', 'Teams', 'Dashboards', 'Plans', and 'Queries'. Each section contains a list of items, each accompanied by a yellow star icon.

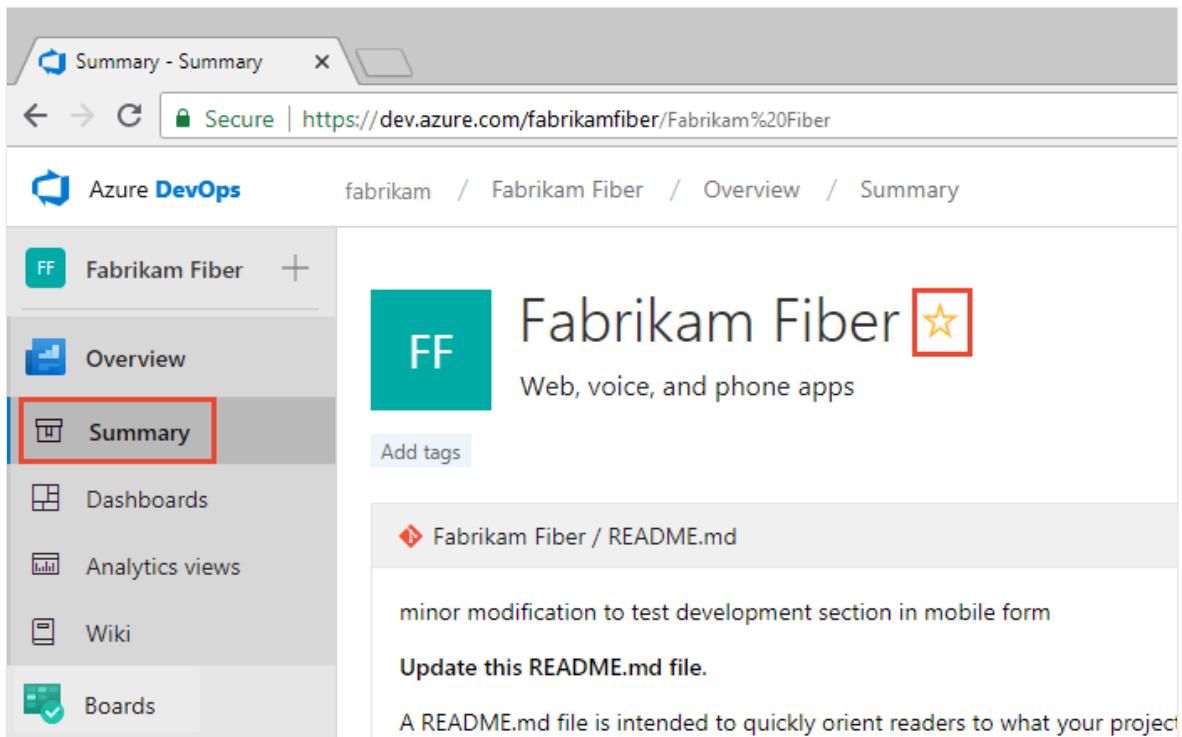
Section	Item	Star Icon
Projects	Fabrikam Fiber	★
	Phone	★
	Voice	★
Teams	Web	★
	Fabrikam Fiber Team Analytics	★
	Backlog team plans	★
Plans	Fabrikam Fiber Feature plans	★
	All items	★
	All items on all projects	★
Queries	Assigned to me	★

### ⓘ Note

If a service is disabled, then you can't favorite an artifact or view of that service. For example, if **Boards** is disabled, then the favorite groups—Plans, Boards, Backlogs, Analytics views, Sprints, and Queries and all Analytics widgets—are disabled. To re-enable a service, see [Turn an Azure DevOps service on or off](#).

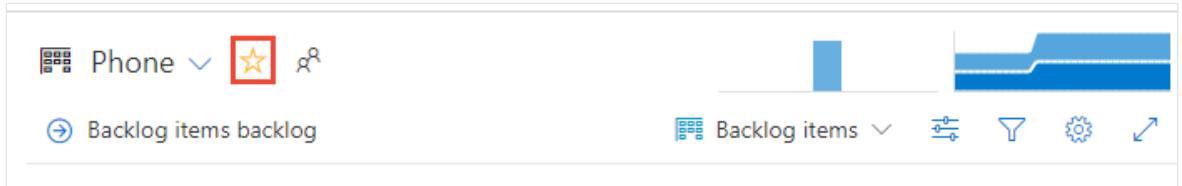
## Favorite a project or team

1. To favorite a project, open the project **Summary** page and choose the  star icon.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, a sidebar menu lists 'Overview', 'Summary' (which is selected and highlighted with a red box), 'Dashboards', 'Analytics views', 'Wiki', and 'Boards'. The main content area displays the project's logo ('FF'), its name 'Fabrikam Fiber' with a yellow star icon, and a brief description: 'Web, voice, and phone apps'. Below this, there's a section for 'Fabrikam Fiber / README.md' containing a note about minor modifications and instructions to update it. A link to the README file is provided.

2. To favorite a team artifact, open **Boards** > **Boards** or **Boards**> **Backlogs**. Select the team you want to favorite from the team selector and choose the  star icon.



The screenshot shows the 'Boards > Backlogs' page. It features a header with a team selector set to 'Phone' (with a yellow star icon) and a search bar. Below the header, a backlog item titled 'Backlog items backlog' is listed. To the right of the backlog item are several icons for filtering, sorting, and other backlog management functions.

3. To favorite other team artifacts, choose the  team icon, and then choose the  star icon next to one of the listed artifacts.

The screenshot shows the Microsoft Teams sidebar for the 'Phone' team. At the top, there's a purple circular icon with two stylized human figures. Below it, the team name 'Phone' and the organization 'Fabrikam Fiber' are displayed, along with a 'Team Settings' link. A horizontal navigation bar has 'Items' selected, followed by 'Members (1)'. A dropdown menu titled 'All Items' is open, showing three items: 'Boards', 'Backlogs', and 'Sprints', each accompanied by a yellow star icon.

::: moniker-end

## Favorite a dashboard

1. From Overview > Dashboards, open the selector and choose the **Browse all dashboards** option.

The screenshot shows the 'Fabrikam Team Overview' dashboard selector. At the top, there's a title bar with the dashboard name and a refresh button. Below it is a search bar labeled 'Search dashboards'. The main area is divided into sections: 'Favorites' (containing 'Fabrikam Team Analytics' with a yellow star), 'Account Management' (containing 'Account Management Overview'), 'Customer Profile' (containing 'Customer Profile Overview'), and 'Fabrikam Team' (containing 'Fabrikam Team Analytics' with a yellow star). At the bottom of the list, there are buttons for '+ New dashboard' and a red-highlighted 'Browse all dashboards' button.

2. The **Mine** page shows your favorite dashboards, and all dashboards of teams that you belong to. The **All** page lists all dashboards defined for the project in alphabetical order. You can filter the list by team or by keyword.

The screenshot shows the 'Dashboards' page with the 'All' tab selected (highlighted with a red box). At the top, there are buttons for 'Mine' and 'All', a '+ New dashboard' button, and a search icon. Below the header, there's a 'Filter dashboards' section with a search bar and a 'Filter by team' dropdown. A modal window titled 'Search' is open, listing various teams with checkboxes: Account Management, Customer Profile, Email, Fabrikam Team, Internet, Phone, Service Delivery, and Service Status. There's also a 'Clear' button at the bottom of the modal. The main table lists dashboards with columns for Name, Star icon, and Team. The 'Analytics' dashboard is highlighted with a blue background.

Name ↑	Team
Analytics	Fabrikam Team
Bug status	Fabrikam Team
Bugs	Internet
Overview	Account Management
Overview	Customer Profile
Overview	Email
Overview	Fabrikam Team
Overview	Internet
Overview	Phone
Overview	Service Delivery
Overview	Service Status
Team Guidance	Fabrikam Team
Work in Progress	Internet

### 💡 Tip

You can change the sort order of the list by choosing the column label.

3. To favorite a dashboard, hover over the dashboard and choose the star icon.

The screenshot shows a single dashboard card for 'Analytics'. It includes a 'Name ↑' column header, an 'Add to favorites' button (which is highlighted with a red box), and a 'Team' column showing 'Fabrikam Team'. The 'Analytics' card has a yellow star icon with a red border, indicating it is favorited.

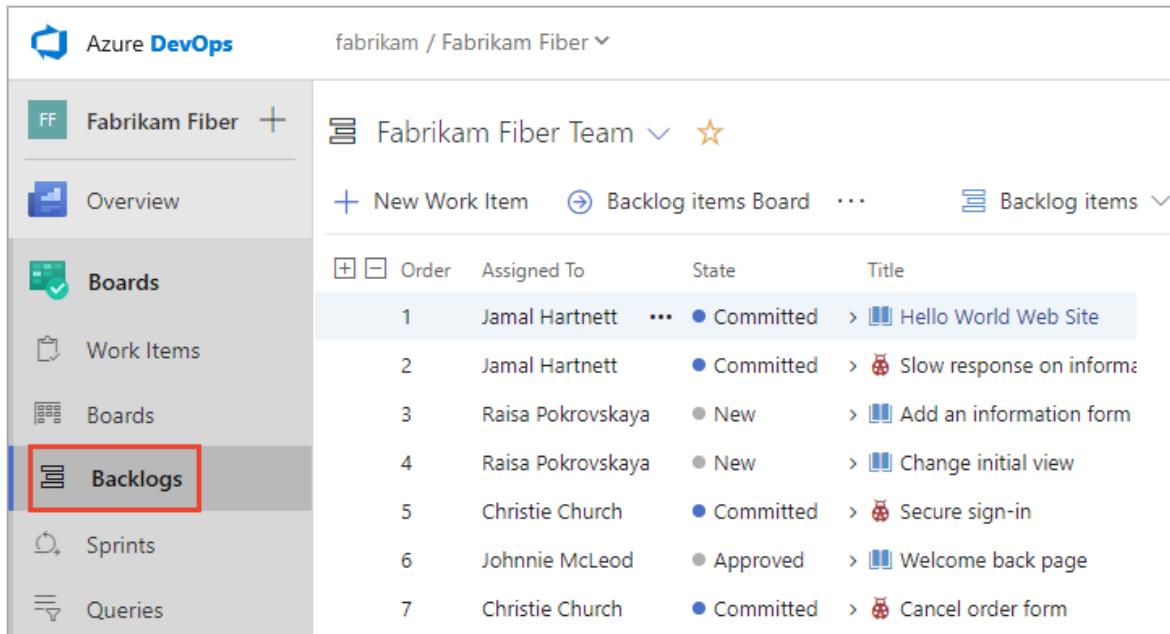
Favoriting a dashboard causes it to appear on your **Favorites** page and towards the top in the **Dashboards** selection menu.

## Favorite a team's backlog, board, or other view

You can favorite several Agile tools for a team from a **Boards** page.

1. Choose **Boards**, and then choose the page of interest, such as **Boards**, **Backlogs**, or **Sprints**.

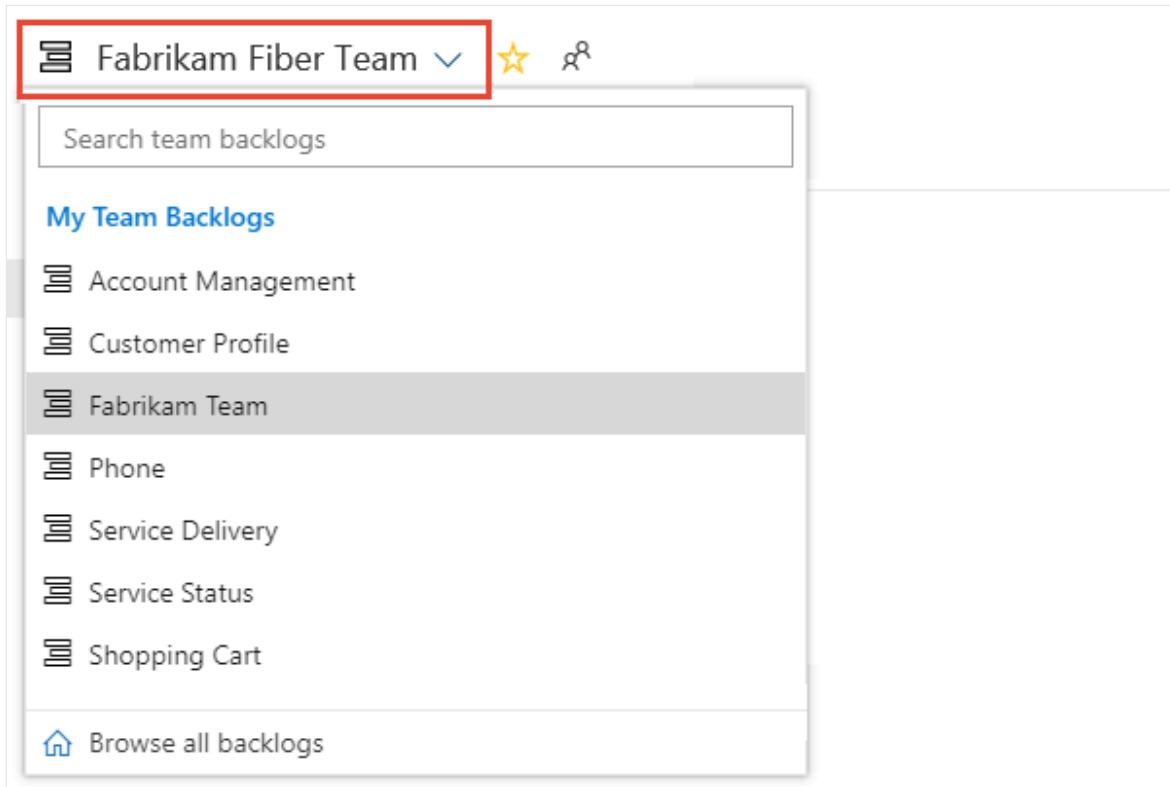
For example, here we choose (1) **Work** and then (2) **Backlogs**.



The screenshot shows the Azure DevOps interface for the project "fabrikam / Fabrikam Fiber". On the left, there's a sidebar with links for Overview, Boards, Work Items, Boards, Backlogs (which is highlighted with a red box), Sprints, and Queries. The main area shows a backlog for the "Fabrikam Fiber Team". At the top right of the backlog area, there's a "Backlog items" button with a dropdown arrow. Below it, a table lists seven backlog items:

	Order	Assigned To	State	Title
1	Jamal Hartnett	...	Committed	> Hello World Web Site
2	Jamal Hartnett	...	Committed	> Slow response on informa
3	Raisa Pokrovskaya	...	New	> Add an information form
4	Raisa Pokrovskaya	...	New	> Change initial view
5	Christie Church	...	Committed	> Secure sign-in
6	Johnnie McLeod	...	Approved	> Welcome back page
7	Christie Church	...	Committed	> Cancel order form

To choose a specific team backlog, open the selector and select a different team or choose the **Browse all team backlogs** option. Or, you can enter a keyword in the search box to filter the list of team backlogs for the project.



The screenshot shows a modal dialog titled "My Team Backlogs". At the top, there's a dropdown menu with "Fabrikam Fiber Team" selected, which is highlighted with a red box. Below the dropdown is a search bar with the placeholder "Search team backlogs". The main list contains several backlog items, each with a small icon and a title. The "Fabrikam Team" item is highlighted with a gray background. At the bottom of the list is a link to "Browse all backlogs".

- Account Management
- Customer Profile
- Fabrikam Team
- Phone
- Service Delivery
- Service Status
- Shopping Cart

[Browse all backlogs](#)

2. Choose the star icon to favorite a team backlog. Favorite artifacts ( favorite icon) appear on your **Favorites** page and towards the top of the team backlog selector menu.

## Favorite a shared query

Open **Boards > Queries** and choose the **All** page. Expand a folder as needed. Choose the star icon next to the query you want to favorite.

Or, open the context menu of the query, and then select **Add to Team Favorites**, and then select from the list of teams.

### Note

Be a member of at least one team for the **Add to Team Favorites** option to be visible. If not visible, ask your project administrator or team administrator to add you to a team.

The screenshot shows the 'Queries' page in Microsoft Teams. The 'All' tab is selected. A context menu is open over a query titled 'Blocked Tasks'. The 'Add to Team Favorites' option is highlighted with a red box. A secondary dropdown menu shows team names: Customer Service, Fabrikam Fiber Team, Management team, and Phone, with 'Phone' also highlighted with a red box.

You can also set a query as a personal favorite by opening the query and choosing the star icon.

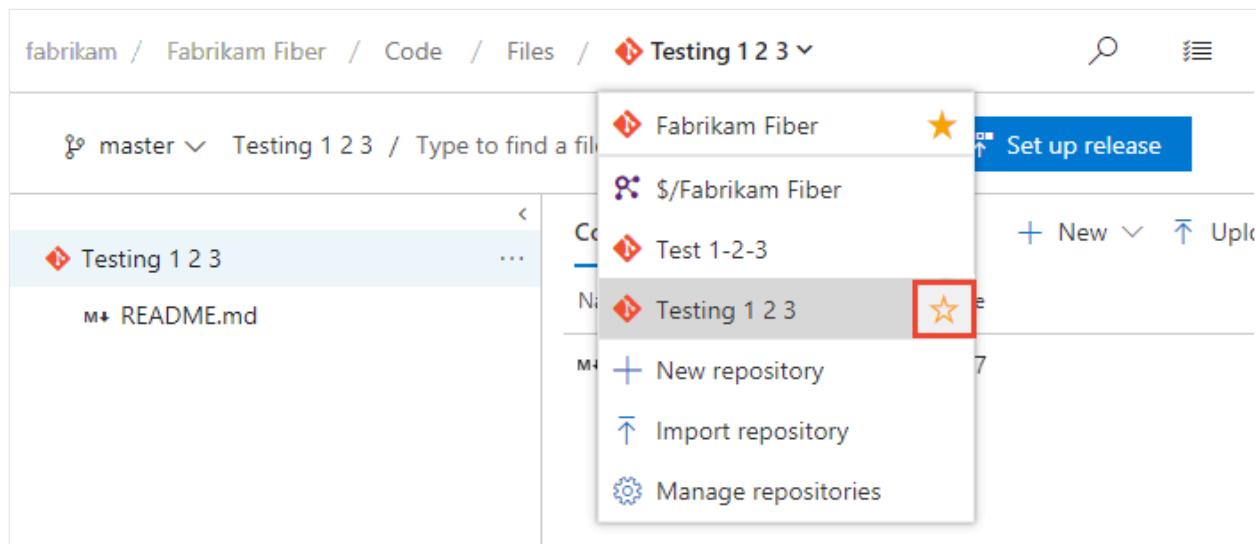
## Favorite a delivery plan

To learn more about delivery plans, see [Review team Delivery Plans](#).

To mark a delivery plan as a favorite, open the **Boards > Plans** page and choose the  star icon next to the Delivery Plan.

## Favorite a repository

From any **Repos** page, open the repository selector and choose the  star icon for the repository you want to favorite.



## Favorite a build pipeline

Open **Pipelines > Builds** and choose either **Mine** or **Definitions**. Choose the  star icon next to the build definition you want to favorite. Or, open the context menu of the build definition, and then select **Add to my favorites** or **Add to team favorites**.

The screenshot shows the 'Build Definitions' page in the Azure DevOps interface. At the top, there are tabs for 'Mine', 'Definitions', 'Queued', and 'XAML'. Below these are sections for 'Recently built', 'Status', 'Triggered by', and 'History'. A search bar at the top right contains 'Build ID or build number' and a magnifying glass icon. To the right of the search bar are buttons for '+ New' and '+ Import'. The main area lists two build definitions: 'fabrikam build' and 'Fabrikam Fiber-Cl'. For 'fabrikam build', a context menu is open, showing options like 'Queue new build...', 'Edit definition', 'Pause', 'View builds', 'Add to my favorites' (which is highlighted with a red box), 'Add to team favorites >', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', 'Security...', and '+ Add to dashboard >'. The 'fabrikam build' entry also has a yellow star icon next to it.

::: moniker-end

## Favorite a test plan

To learn more about test plans, see [Create a test plan and test suite](#).

To mark a test plan as a favorite, open **Test Plans > Test Plans** and choose the star icon next to a test plan from the menu that shows All test plans.

## Unfavorite a view

You can unfavorite an artifact from your **Favorites** page. Choose the inbox icon, and then choose **Favorites**. Choose the favorite icon of a favorite artifact.

The screenshot shows the Microsoft Teams sidebar. At the top, there are three tabs: "Work Items", "Pull requests", and "Favorites". The "Favorites" tab is highlighted with a red box. To the right of the tabs are icons for search, filter, and user profile. Below the tabs, the sidebar is organized into sections: "Projects", "Teams", "Dashboards", "Plans", and "Queries". Each section contains a list of items, each accompanied by a yellow star icon. In the "Projects" section, the item is "Fabrikam Fiber". In the "Teams" section, the items are "Phone", "Voice", and "Web". In the "Dashboards" section, the item is "Fabrikam Fiber Team Analytics". In the "Plans" section, the items are "Backlog team plans" and "Fabrikam Fiber Feature plans". In the "Queries" section, the items are "All items", "All items on all projects", and "Assigned to me".

Section	Item	Status
Projects	Fabrikam Fiber	Starred
Teams	Phone	Starred
	Voice	Starred
	Web	Starred
Dashboards	Fabrikam Fiber Team Analytics	Starred
Plans	Backlog team plans	Starred
	Fabrikam Fiber Feature plans	Starred
Queries	All items	Starred
	All items on all projects	Starred
	Assigned to me	Starred

Similarly, you can unfavorite an artifact from the same page where you marked it as a favorite.

## Next steps

Follow a user story, bug, issue, or other work item or pull request

## Related articles

- Manage personal notifications

- Set your preferences
- 

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Filter lists, boards, and directories

Article • 03/12/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Several applications and pages in Azure DevOps support filtering, which is useful when dealing with a large number of artifacts or items. Most directory views offer one or more filter functions to help you quickly find what you're looking for.

You can filter most items using keywords or a user name, either for the author of an item or where work is assigned to them. Filtering can be applied to lists and boards in the following areas:

- **Git repositories:** Branches, Commits, Commit history, Pull Requests, Pushes, and Repositories
- **Work tracking:** Work Items, Boards, Backlogs, Sprint Backlogs, and Taskboards
- **Directories:** Dashboards, Boards, Backlogs, Sprints, Queries, Builds, Releases

 **Note**

You might have fewer or other filter options based on the [enabled features](#) or the platform and version that you're working from.

## Prerequisites

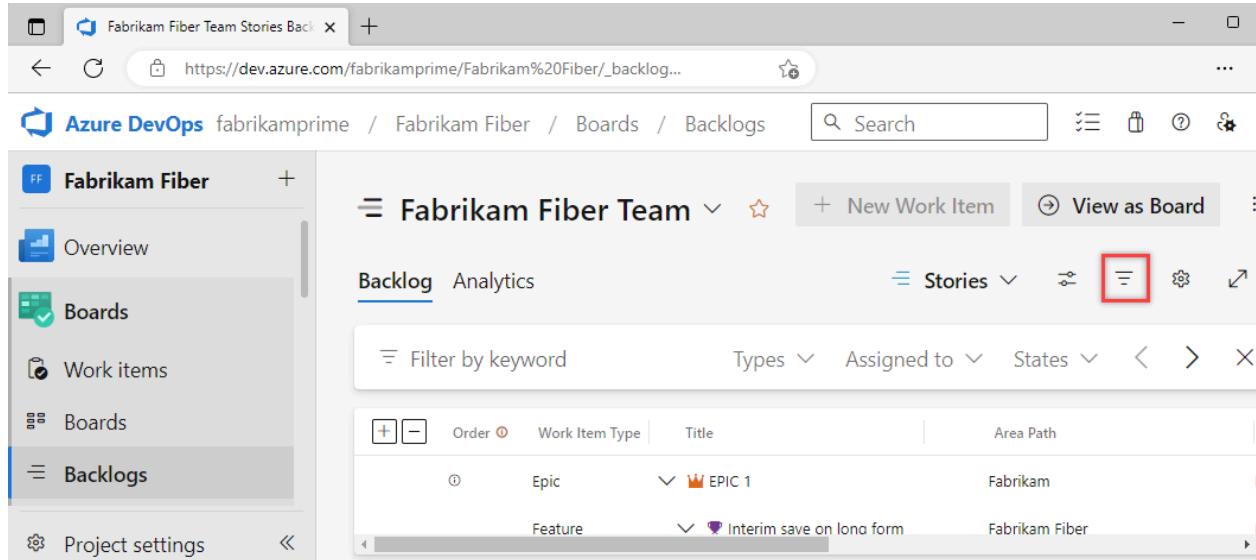
 Expand table

Category	Requirements
Permissions	Member of the <b>Contributors</b> group or similar permissions.
Access	- Member of the project where you want to apply filters. If you don't have access, request it from your project administrator. - At least <b>Basic</b> access to use filtering features. Users with Stakeholder access might experience limited filtering capabilities.

## Filter based on keywords, tags, or fields

To turn on filtering, choose the  filter icon.

You can filter work items by entering a keyword or using fields like work item type, assigned to, state, and tags. The filter lists work items based on any visible column or field, including tags. You can also enter an ID value, regardless of the visibility of the ID field.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar includes links for Overview, Boards, Work items, Boards, Backlogs, and Project settings. The main content area is titled 'Fabrikam Fiber Team' and shows a backlog of work items. The 'Backlog' tab is active. In the top right, there are buttons for '+ New Work Item' and 'View as Board'. Below these are filter options: 'Filter by keyword', 'Types', 'Assigned to', 'States', and a search bar. A red box highlights the filter icon (three horizontal lines) in the top right of the main content area. The backlog table has columns for Order, Work Item Type, Title, and Area Path. It lists one Epic ('EPIC 1') and one Feature ('Interim save on long form').

The filtered set is always a flat list, even if you selected to show parents.

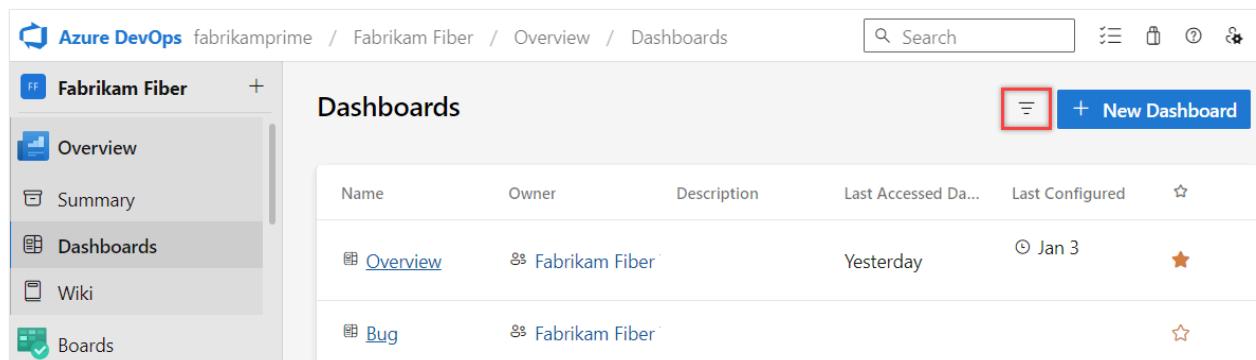
## Characters ignored by keyword filter criteria

The filter criteria ignore the following characters: , (comma), . (period), / (forward slash), and \ (back slash).

## Filter directories

Choose the  filter icon to filter a directory list by keyword, team, or other supported field. Keywords apply to titles, descriptions, and team names.

For example, here we turn on filtering for the dashboard directory.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The left sidebar includes links for Overview, Summary, Dashboards, Wiki, and Boards. The main content area is titled 'Dashboards' and shows a list of dashboards. The 'Dashboards' tab is active. In the top right, there are buttons for '+ New Dashboard' and a filter icon. Below these are filter options: 'Name', 'Owner', 'Description', 'Last Accessed Da...', 'Last Configured', and a star icon. A red box highlights the filter icon (three horizontal lines) in the top right of the main content area. The dashboard table has columns for Name, Owner, Description, Last Accessed Da..., Last Configured, and a star icon. It lists two dashboards: 'Overview' and 'Bug'.

## Related articles

- [Commit history](#)
  - [Working with Git tags](#)
  - [Filter backlogs and queries](#)
  - [Filter your board](#)
  - [Add tags to work items](#)
- 

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Get started with search

Article • 09/07/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

You can quickly find work items, code files, wiki pages, or packages based on a keyword, wildcards, and other supported search filters with the search function.

For more information, see the following links:

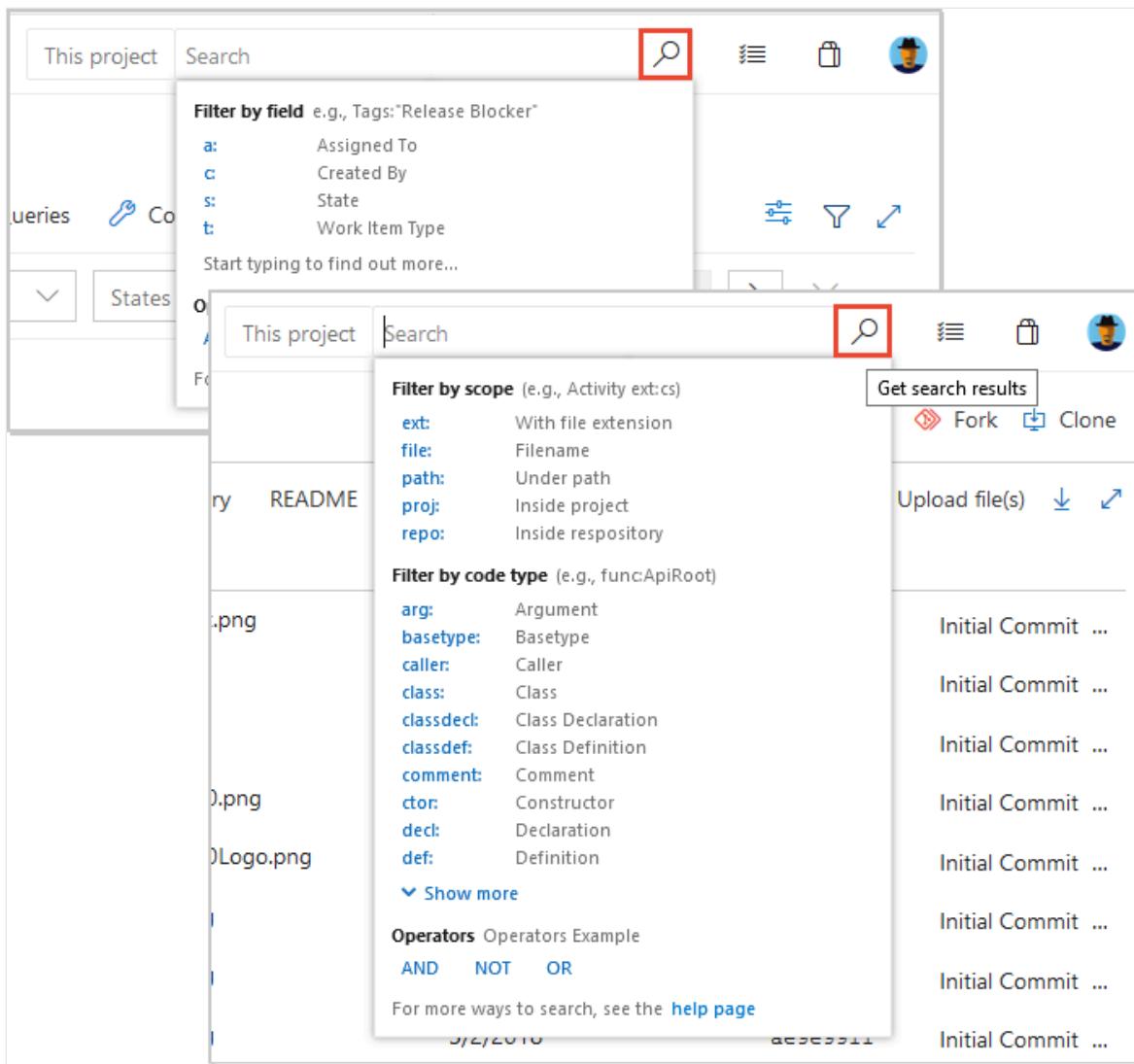
- [Functional code search](#)
- [Code Search extension ↗](#)
- [Functional work item search](#)
- [Functional package search](#)

## Prerequisites

- **Access levels:**
  - **All project members:** Every project member can use the search functions, including users with Stakeholder, Basic, and higher levels of access.
- **Search results:**
  - **Access-based results:** When you're searching across the organization or collection, only results for which a project member has access are listed.
  - **Stakeholder limitations:**
    - **Wiki search:** Stakeholder wiki search results are limited to provisioned wikis. Published wiki results don't appear because they require access to regular repositories, which Stakeholders don't have.
    - **Code search:** Code search results don't appear for Stakeholders.

## Search tips

- **Use keywords:** Start your search using a keyword. You can then apply other options, as needed, to broaden or narrow your search results.



- **Adjust filters:** If your initial search doesn't yield the desired results, try removing filters and searching again. Once you see the search results, you can narrow them down by applying appropriate filters and searching again.
- **Check spelling:** Ensure your search terms are spelled correctly, as work item search doesn't ignore spelling errors.
- **Refine wildcard searches:** If you receive a message that no matching files are found due to a wildcard search with too many hits, make your search more specific. Add more characters of the word or words you want to find, or use a condition or filter to restrict the number of possible matches.
- **Case insensitivity:** Searches aren't case-sensitive.

## Search features, usage, and examples

The following features apply to all searches, including work items, code, wikis, and packages.

### Search feature

## Usage

### Example

---

#### Keyword

Search based on one or more keywords.

`validate` finds instances that contain the word *validate*.

---

#### Exact match

Search based on an exact match, enclosed in double-quotes.

`"Client not found"` finds instances that contain the exact phrase match *Client not found*. Search might not handle special characters as expected. Try escaping special characters or simplifying the search phrase.

---

#### Wildcard

- Add wildcard characters, `*` and `?`, to keywords to extend the search criteria.
  - Add `*` at the end of a keyword to find items that start with the keyword.
  - Add `?` in the middle to represent any alphanumeric character.
  - Use wildcard characters anywhere in your search string except as a prefix. You can use prefix wildcards with the other search filter functions.
  - You can use more than one wildcard to match more than one character.
  - `alpha?version` finds instances of alpha1version and alphaXversion.
  - `Browser*` finds instances of BrowserEdge, BrowserIE, and BrowserFirefox.
  - `CodeSenseHttp*` finds files containing words that start with *CodeSenseHttp*, such as CodeSenseHttpClient and CodeSenseHttpClientTest.
- 

#### Boolean operators

- Find two or more keywords using Boolean operators: `AND`, `OR`, and `NOT` (must be uppercase).
- Add parenthesis to clauses to support logical groupings.

- Because `AND` is the default operator, an entry of two keywords with no operator is the same as an `AND` search.
  - `Validate AND revisit` finds files that contain both the words *validate* and *revisit*.
  - `Validate OR revisit` finds files that contain either of the words *validate* or *revisit*.
  - `Validate NOT revisit` finds files that contain the word *validate* but not the word, *revisit*.
  - `(Validate NOT revisit) OR "release delayed"` finds files that contain the word *validate* but not the word, \**revisit*, or files that contain the phrase *release delayed*.
- 

## Proximity

- Search for files based on vicinity using proximity operators: `NEAR`, `BEFORE`, and `AFTER` (must be uppercase).
  - By default, proximity search looks for terms within five tokens distance.
  - `term1 BEFORE term2` returns all files where `term1` occurs `BEFORE` `term2` within a distance of five tokens between them.
  - `term1 AFTER term2` returns the same results as `term2 BEFORE term1`.
  - `term1 NEAR term2` returns all files where `term1` is within five token distance from `term2` in any direction. `term1 NEAR term2` returns the same results as `term1 BEFORE term2 OR term2 BEFORE term1`.
- 

## Special characters

- Escape the special characters `(`, `)`, `[`, `]`, `:`, `*`, and `?` by enclosing them in a phrase delimited with double-quotes.
  - Include special characters in a search string, or search specifically for special characters, according to the following rules:
  - `CodeA23?R` finds files containing words that start with `CodeA23`
  - Have any alphanumeric character next, and end with `R`. For example, `CodeA234R` and `CodeA23QR`.
  - Search for any special character that isn't a part of the query language.
  - `"flatten()"` finds the literal string *flatten()*. Search for a literal occurrence of the double-quote character `"` by preceding it with the escape character `\` and enclosing the search string in double-quotes.
  - `"\"react-redux\\""` finds the literal string `"react-redux."`
-

# Search from a different page

You can search from any of the following pages:

- Organization project page: Starts a search across all projects.
- Project overview page: Automatically applies a filter to search within the selected project.
- Boards page for a project: Automatically displays recent work items and backlogs accessed by the user.
- Azure Repos, Pipelines, Test Plans, or an Artifacts page for a project: Automatically displays functional filters for code searches.
- Wiki page: Automatically go to a wiki page you recently opened.

For more information, see the following articles:

- [Filter backlogs, boards, and plans](#)
- [Provisioned vs. published wiki](#)

## 💡 Tip

### No results found for ...

Too many hits from a simple wildcard search can result in no matching files. You can narrow your search by adding more characters or using a condition or filter.

## More search functions

See the following table for more search tasks and actions.

### Search task

### Action

Find an organization setting

Go to your organization and select **Organization settings**.

Find a project setting

Go to your project and select **Project settings**.

---

Find a user setting

Go to your **User settings page**.

---

Find a user

Go to your organization and select **Organization settings > Users**, and then enter the name in the filter box.

---

Find an organization

Scroll through the left side of your screen, which lists all organizations.

---

Find a project

Go to your organization, and then enter the project name in the Filter projects box.

---

View file history and compare versions

Go to **Repos > Files**, highlight your file, and then select **History**.

---

 **Note**

When you search from the **Organization settings** page, your search results include both organization-level and project-level settings.

## Marketplace extensions

- [Code Search](#) - Extends search with fast, flexible, and precise search results across all your code. Required for searching repositories.

- [Azure Paths Search](#) - Adds a special search hub to Boards for searching within iterations and area paths without having to create and maintain custom queries.

① Note

Azure DevOps doesn't support some extensions. For more information or assistance, go to the [Visual Studio Marketplace](#).

## Next steps

[Functional code search](#)

## Related articles

- [Functional work item search](#)
- [Functional artifact or package search](#)
- [Code search blog posts](#)
- [Work item search blog posts](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Manage preview features

Article • 01/27/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

As some new features get introduced, you can turn them on or off. You can try them out, provide feedback, and work with the ones that meet your requirements. Some preview features provide access to new functionality, while others reflect a change to the user interface, but little or no change in functionality.

## ⓘ Note

It might take up to three weeks after a release to Azure DevOps for the preview feature to appear in your organization. The [latest release notes](#) usually provide information on new preview features. You can turn on or off select features for Azure DevOps. Preview features become available first on Azure DevOps Services and then become standard features with an update to Azure DevOps Server. At some point, the preview feature moves out of preview status and becomes a regular feature of the web portal.

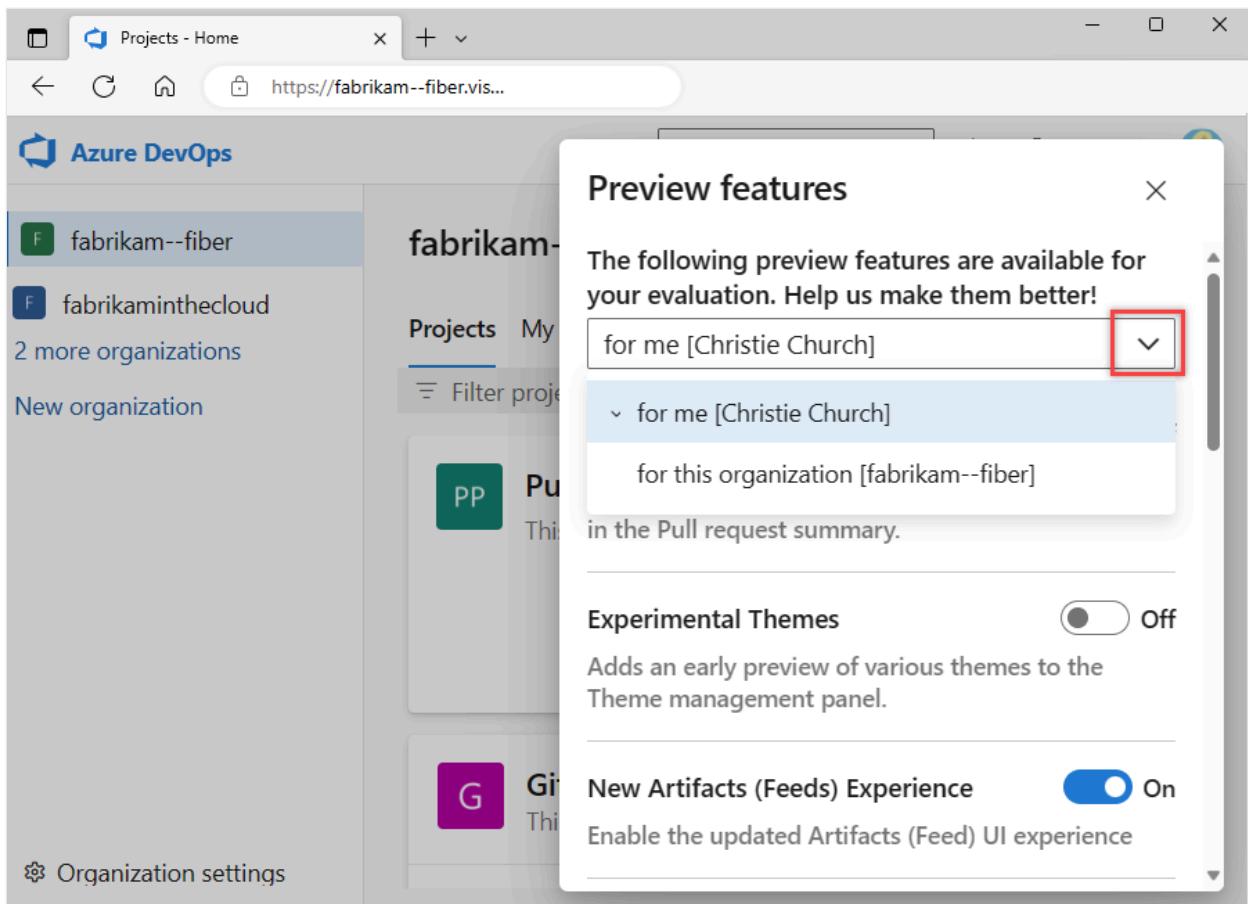
## Prerequisites

[ ] Expand table

Category	Requirements
Project access	Member of the <a href="#">project</a> where you want to enable or disable preview features.
Permissions	To enable or disable preview features for your organization: Member of the <a href="#">Project Administrators</a> group.
Access levels	At least <b>Basic</b> access.

## Turn on or off preview features

Select either your organization or personal settings from the dropdown menu and slide the toggle to **on** or **off** to change the feature status.



Enabling a feature at the organization level activates it for all users. They can still turn it off individually. Disabling a feature at the organization level doesn't affect user settings. Users can change feature status on their own. For more information, see [Set user preferences](#).

### Tip

If you don't see the **for this account** menu option, then you aren't a member of the Project Collection Administrators group. To get added as one, see [Change project collection-level permissions](#).

## Preview features

The following table lists the preview features that you can turn on or off based on your role: user, team member, or organization. Only Project Collection Administrators can manage organization-level features.

[+] Expand table

Preview features	Per user	Per organization
Pull Request Summary - Load of large files	✓	

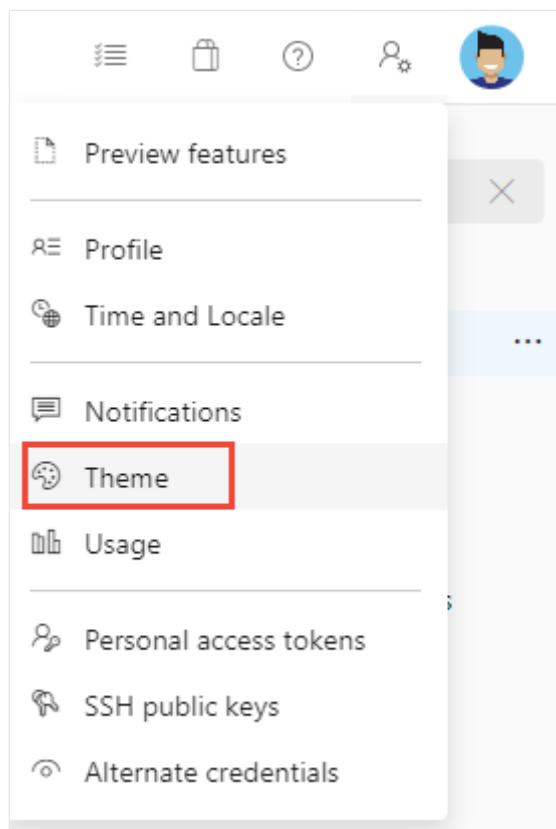
Preview features	Per user	Per organization
Microsoft Entra profile information	✓	
Experimental themes	✓	✓
Limit user visibility and collaboration to specific projects		✓
New Artifacts (Feeds) Experience (accessibility updates)	✓	✓
New Boards Hubs	✓	✓
New service connections experience	✓	✓
New Settings Search in the organization settings panel	✓	✓
New workflow identity authentication option	✓	✓
New Teams page	✓	✓
New Wiki experience	✓	✓
Organization Permissions Settings Page v2	✓	✓
Project Permissions Settings page	✓	✓
Task Insights for Failed Pipeline Runs	✓	✓
YAML templates editor	✓	✓

## Pull request summary - Load of large files

Turns on a file content load experience for large files in the Pull request summary.

## Experimental themes

When you select **Theme** from the Profile menu, you can select between **Dark** and **Light** themes for the display of Azure DevOps web portal.



With **Experimental themes** on, you can select from many other themes.

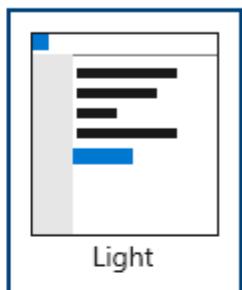
## Choose your theme

X

### Default themes



Dark



Light

### Custom themes



Blue



Dark editor



Fall



Gre

### Preview themes



High Contrast



Neptune



Red (dark)



Solar

## GA features for Azure DevOps

The following features are generally available for Azure DevOps.

### General

- New user hub
- New PAT experience
- New Navigation ↗
- Wiki
- Combine email recipients
- New experience in Code, Work Item, & Wiki search
- Out of the box notifications
- Team expansion for notifications
- Streamlined user management

## Azure Artifacts

- NuGet.org upstream sources
- Updated package experience

## Azure Boards, Dashboards, and Analytics

- Copy Dashboard Experience
- New Delivery Plans Experience
- Enable group by tags for work item chart widget on dashboard
- New Queries Experience
- New Work Items
- New Dashboards Experience
- New boards reports
- Analytics views

## Azure Repos

- New TFVC pages
- Git Forks
- New Repos pull request experience ↗
- New Repos settings experience
- New Repos landing pages
- Pull Request Status Policy

## Azure Pipelines

- Historical graph for agent pools
- Pipeline decorators
- Multi-stage pipelines
- Test tab in new web platform
- Test analytics in new web platform
- New builds hub
- Build with multiple queues ↗
- New Releases Hub
- Approval gates in releases - New Release Definition Editor
- Symbol server
- Task tool installers
- Workload Identity federation for Azure Resource Manager service connections

## Azure Test Plans

- [New Test Plans Page](#)
- [New Test Plan Experience](#)

## Transition of Preview Features to General Availability

While there's no fixed timeline for when a preview feature moves to general availability (GA), there are several indicators and resources you can use to stay informed about the status of preview features:

- **Azure DevOps roadmap and release notes:** The Azure DevOps roadmap provides insights into upcoming features and enhancements. It includes information about features currently in preview and their expected release timelines. Azure DevOps release notes provide detailed information about new features, improvements, and bug fixes. For more information, see the Relevant Links section at [Azure DevOps Blog ↗](#).
- **Azure DevOps blog:** The Azure DevOps blog often features posts about new releases, including when preview features transition to GA. Subscribing to the blog or regularly checking it can help you stay updated. For more information, see [Azure DevOps Blog ↗](#).

## Related articles

- [Set user preferences](#)

ⓘ **Note:** The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Get started with search

Article • 09/07/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

You can quickly find work items, code files, wiki pages, or packages based on a keyword, wildcards, and other supported search filters with the search function.

For more information, see the following links:

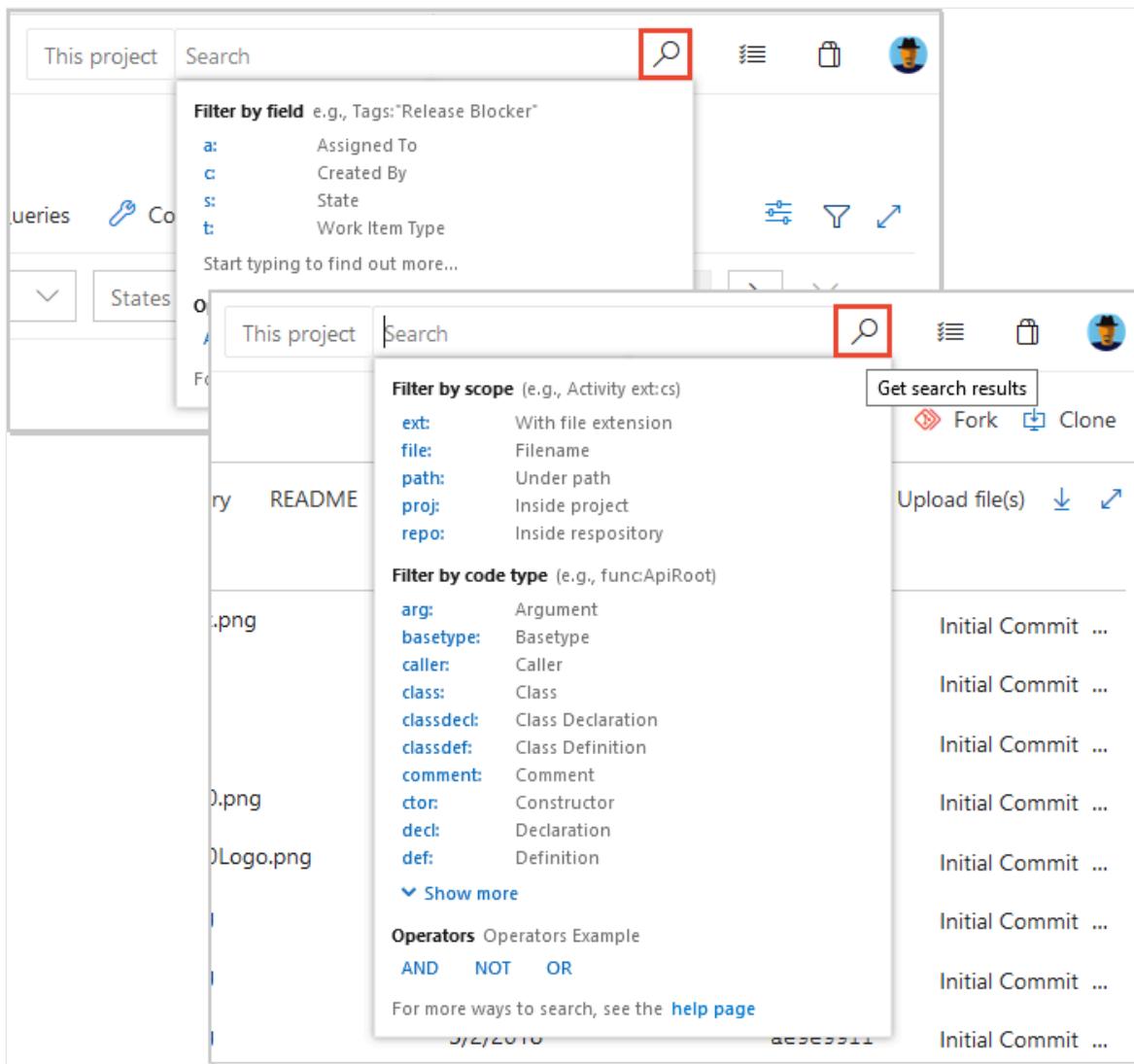
- [Functional code search](#)
- [Code Search extension ↗](#)
- [Functional work item search](#)
- [Functional package search](#)

## Prerequisites

- **Access levels:**
  - **All project members:** Every project member can use the search functions, including users with Stakeholder, Basic, and higher levels of access.
- **Search results:**
  - **Access-based results:** When you're searching across the organization or collection, only results for which a project member has access are listed.
  - **Stakeholder limitations:**
    - **Wiki search:** Stakeholder wiki search results are limited to provisioned wikis. Published wiki results don't appear because they require access to regular repositories, which Stakeholders don't have.
    - **Code search:** Code search results don't appear for Stakeholders.

## Search tips

- **Use keywords:** Start your search using a keyword. You can then apply other options, as needed, to broaden or narrow your search results.



- **Adjust filters:** If your initial search doesn't yield the desired results, try removing filters and searching again. Once you see the search results, you can narrow them down by applying appropriate filters and searching again.
- **Check spelling:** Ensure your search terms are spelled correctly, as work item search doesn't ignore spelling errors.
- **Refine wildcard searches:** If you receive a message that no matching files are found due to a wildcard search with too many hits, make your search more specific. Add more characters of the word or words you want to find, or use a condition or filter to restrict the number of possible matches.
- **Case insensitivity:** Searches aren't case-sensitive.

## Search features, usage, and examples

The following features apply to all searches, including work items, code, wikis, and packages.

### Search feature

## Usage

### Example

---

#### Keyword

Search based on one or more keywords.

`validate` finds instances that contain the word *validate*.

---

#### Exact match

Search based on an exact match, enclosed in double-quotes.

`"Client not found"` finds instances that contain the exact phrase match *Client not found*. Search might not handle special characters as expected. Try escaping special characters or simplifying the search phrase.

---

#### Wildcard

- Add wildcard characters, `*` and `?`, to keywords to extend the search criteria.
  - Add `*` at the end of a keyword to find items that start with the keyword.
  - Add `?` in the middle to represent any alphanumeric character.
  - Use wildcard characters anywhere in your search string except as a prefix. You can use prefix wildcards with the other search filter functions.
  - You can use more than one wildcard to match more than one character.
  - `alpha?version` finds instances of alpha1version and alphaXversion.
  - `Browser*` finds instances of BrowserEdge, BrowserIE, and BrowserFirefox.
  - `CodeSenseHttp*` finds files containing words that start with *CodeSenseHttp*, such as CodeSenseHttpClient and CodeSenseHttpClientTest.
- 

#### Boolean operators

- Find two or more keywords using Boolean operators: `AND`, `OR`, and `NOT` (must be uppercase).
- Add parenthesis to clauses to support logical groupings.

- Because `AND` is the default operator, an entry of two keywords with no operator is the same as an `AND` search.
  - `Validate AND revisit` finds files that contain both the words *validate* and *revisit*.
  - `Validate OR revisit` finds files that contain either of the words *validate* or *revisit*.
  - `Validate NOT revisit` finds files that contain the word *validate* but not the word, *revisit*.
  - `(Validate NOT revisit) OR "release delayed"` finds files that contain the word *validate* but not the word, \**revisit*, or files that contain the phrase *release delayed*.
- 

## Proximity

- Search for files based on vicinity using proximity operators: `NEAR`, `BEFORE`, and `AFTER` (must be uppercase).
  - By default, proximity search looks for terms within five tokens distance.
  - `term1 BEFORE term2` returns all files where `term1` occurs `BEFORE` `term2` within a distance of five tokens between them.
  - `term1 AFTER term2` returns the same results as `term2 BEFORE term1`.
  - `term1 NEAR term2` returns all files where `term1` is within five token distance from `term2` in any direction. `term1 NEAR term2` returns the same results as `term1 BEFORE term2 OR term2 BEFORE term1`.
- 

## Special characters

- Escape the special characters `(`, `)`, `[`, `]`, `:`, `*`, and `?` by enclosing them in a phrase delimited with double-quotes.
  - Include special characters in a search string, or search specifically for special characters, according to the following rules:
  - `CodeA23?R` finds files containing words that start with `CodeA23`
  - Have any alphanumeric character next, and end with `R`. For example, `CodeA234R` and `CodeA23QR`.
  - Search for any special character that isn't a part of the query language.
  - `"flatten()"` finds the literal string *flatten()*. Search for a literal occurrence of the double-quote character `"` by preceding it with the escape character `\` and enclosing the search string in double-quotes.
  - `"\"react-redux\\""` finds the literal string `"react-redux."`
-

# Search from a different page

You can search from any of the following pages:

- Organization project page: Starts a search across all projects.
- Project overview page: Automatically applies a filter to search within the selected project.
- Boards page for a project: Automatically displays recent work items and backlogs accessed by the user.
- Azure Repos, Pipelines, Test Plans, or an Artifacts page for a project: Automatically displays functional filters for code searches.
- Wiki page: Automatically go to a wiki page you recently opened.

For more information, see the following articles:

- [Filter backlogs, boards, and plans](#)
- [Provisioned vs. published wiki](#)

## 💡 Tip

### No results found for ...

Too many hits from a simple wildcard search can result in no matching files. You can narrow your search by adding more characters or using a condition or filter.

## More search functions

See the following table for more search tasks and actions.

### Search task

### Action

Find an organization setting

Go to your organization and select **Organization settings**.

Find a project setting

Go to your project and select **Project settings**.

---

Find a user setting

Go to your **User settings page**.

---

Find a user

Go to your organization and select **Organization settings > Users**, and then enter the name in the filter box.

---

Find an organization

Scroll through the left side of your screen, which lists all organizations.

---

Find a project

Go to your organization, and then enter the project name in the Filter projects box.

---

View file history and compare versions

Go to **Repos > Files**, highlight your file, and then select **History**.

---

 **Note**

When you search from the **Organization settings** page, your search results include both organization-level and project-level settings.

## Marketplace extensions

- [Code Search](#) - Extends search with fast, flexible, and precise search results across all your code. Required for searching repositories.

- [Azure Paths Search](#) - Adds a special search hub to Boards for searching within iterations and area paths without having to create and maintain custom queries.

 Note

Azure DevOps doesn't support some extensions. For more information or assistance, go to the [Visual Studio Marketplace](#).

## Next steps

[Functional code search](#)

## Related articles

- [Functional work item search](#)
- [Functional artifact or package search](#)
- [Code search blog posts](#)
- [Work item search blog posts](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Functional code search

Article • 01/28/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Find the code you need faster with functional code search. This article explains how to refine your search across repositories using code types and other functions with the [Code Search](#) Marketplace extension for Azure DevOps.

## Prerequisites

[+] Expand table

Category	Prerequisite
Access levels	<ul style="list-style-type: none"><li>- To use code search: At least <b>Basic</b> access.</li><li>- To access code in a private project: At least <b>Basic</b> access. Stakeholder access doesn't include code.</li><li>- To access code in a public project: At least <b>Stakeholder</b> access.</li></ul>
Search results	<b>Access-based results:</b> When you're searching across the organization or collection, only results for which a project member has access are listed.

## Code search best practices

- **Start broad:** Begin with a broad search and then use filter operators to narrow it down by project, repository, path, file name, and more.
- **Use wildcards and boolean operators:** If you don't know the exact term, use wildcards to expand your search and boolean operators to refine it.
- **Hover for more info:** To get more information about a code item, hover over it and use the shortcut menu to search for that text in all your projects and files.
- **Trace code functionality:** Use the shortcut menu to search for related items like definitions and references in a file or in the search results to trace how your code works.
- **Use code type filters:** To find the implementation of an API or other code element, use code type filters to search for specific kinds of code such as:
  - Definitions
  - References
  - Functions
  - Comments
  - Strings

- Namespaces, and more

 Note

Code search doesn't work for forked repositories.

## Functions to find specific types of code

To create your query faster, choose functions and keywords from the drop-down list as you enter text. Select **Show more** to see all the options. You can combine different functions as needed.

You can also use filters from the left column to narrow your search. **Show more** shows you all the functions and keywords.

Or, you can type the functions and parameters in the search box. The following table lists the functions for finding specific types or members in your C#, C, C++, Java, and Visual Basic.NET code.

[Expand table](#)

To find code where <i>findThis</i> appears as a ...	... search for argument arg: <i>findThis</i>
Argument	arg: <i>findThis</i> <small>Deprecated in July 2019</small>
Base type	basetype: <i>findThis</i>
Calling function	caller: <i>findThis</i> <small>Deprecated in July 2019</small>
Class definition or declaration	class: <i>findThis</i>
Class declaration	classdecl: <i>findThis</i> <small>Merged with class:</small>
Class definition	classdef: <i>findThis</i> <small>Merged with class:</small>
Comment	comment: <i>findThis</i>
Constructor	ctor: <i>findThis</i> <small>Merged with method:</small>
Declaration	decl: <i>findThis</i>
Definition	def: <i>findThis</i>
Destructor	dtr: <i>findThis</i> <small>Merged with method:</small>
Enumerator	enum: <i>findThis</i>

To find code where <i>findThis</i> appears as a ...	... search for argument arg: <i>findThis</i>
Extern	<code>extern:findThis</code> Deprecated in July 2019
Field	<code>field:findThis</code>
Friend function	<code>friend:findThis</code> Deprecated in July 2019
Function	<code>func:findThis</code> Merged with method:
Function declaration	<code>funcdecl:findThis</code> Merged with method:
Function definition	<code>funcdef:findThis</code> Merged with method:
Global	<code>global:findThis</code> Deprecated in July 2019
Header	<code>header:findThis</code> Deprecated in July 2019
Interface	<code>interface:findThis</code>
Macro	<code>macro:findThis</code>
Macro definition	<code>macrodef:findThis</code> Merged with macro:
Macro reference	<code>macroref:findThis</code> Merged with macro:
Method	<code>method:findThis</code>
Method declaration	<code>methoddecl:findThis</code> Merged with method:
Method definition	<code>methoddef:findThis</code> Merged with method:
Namespace	<code>namespace:findThis</code>
Property	<code>prop:findThis</code>
Reference	<code>ref:findThis</code>
String literal	<code>strlit:findThis</code>
Struct	<code>struct:findThis</code> Merged with type:
Struct declaration	<code>structdecl:findThis</code> Merged with type:
Struct definition	<code>structdef:findThis</code> Merged with type:
Template argument	<code>tmplarg:findThis</code> Deprecated in July 2019
Template specification	<code>tplspec:findThis</code> Deprecated in July 2019
Type	<code>type:findThis</code>
Typedef	<code>typedef:findThis</code> Merged with type:

To find code where `findThis` appears as a ...

... search for argument arg:`findThis`

Union

union:`findThis` Deprecated in July 2019

## Functions to select projects, repositories, paths, and files

Functions make it easy to narrow the search to specified locations, specific types of files within these locations, or specified filenames. Narrow the search to a specific location using the `proj`, `repo`, or `path` filters. Mix and match the following functions as required.

[+] Expand table

Usage	Example
Find all occurrences of the word <code>QueueJobsNow</code> in the <code>Fabrikam</code> project.	<code>QueueJobsNow proj:Fabrikam</code>
Find all occurrences of the word <code>QueueJobsNow</code> in the <code>Contoso</code> repository.	<code>QueueJobsNow repo:Contoso</code>
Find all occurrences of the word <code>QueueJobsNow</code> in the path <code>VisualStudio/Services/Framework</code> and its subpaths.	<code>QueueJobsNow</code> <code>path:VisualStudio/Services/Framework</code>
Find all occurrences of the word <code>QueueJobsNow</code> in the path <code>*/Doc*/Framework/*</code> and <code>*/Doc*/**/Framework/*</code> and its subpaths. Globbing Pattern <code>(**)</code> matches zero or more characters across multiple segments. For example, <code>path:*/Doc**/Framework</code> also matches <code>abc/DocTest/gh/ijk/mnop/Framework/</code>	<code>QueueJobsNow path:*/Doc*/Framework/*</code> <code>path:*/Doc*/**/Framework/*</code>
Find all occurrences of the word <code>QueueJobsNow</code> in the path <code>*/Doc*/Framework/*</code> and its subpaths and file name <code>Test*.txt</code> (Use Globbing Pattern <code>**</code> ). For example, <code>path:*/Doc*/Framework/**/Test*.txt</code> also matches <code>abc/def/DocA/gh/Framework/TestMisc.txt</code>	<code>QueueJobsNow</code> <code>path:*/Doc*/Framework/**/Test*.txt</code>
Enclose the argument to the filter in double-quotes if it contains a space.	<code>QueueJobsNow</code> <code>path:"VisualStudio/Windows Phones and Devices/Services"</code>
Find all occurrences of the word <code>QueueJobsNow</code> in all files where the filename starts with <code>queueRegister</code> .	<code>QueueJobsNow file:queueRegister*</code>
Find all files with the name <code>QueueRegister</code> without an extension. Use quotes to find files without extensions.	<code>file:"queueRegister"</code>

Usage	Example
Find all occurrences of the word <i>QueueJobsNow</i> in only C# source files. A plain text search string that doesn't include file type functions also finds files where the string matches part of the filename.	<code>QueueJobsNow ext:cs</code>

## Find related items or other terms

Code Search lets you interactively expand your search based on previous results. For example, you can widen your search to related files when you're tracing or debugging code.

Right-click on a term in the file and start a new search for other files with the same term. You can search for it as text, or as a definition or reference if it's an object name.

For more information, see [Get started with search](#).

## More code search operations

Here are some more code search functions. You can search for code types in C#, C, C++, Java, and Visual Basic.NET files. To open the search results in a new tab, select **Ctrl + Enter** from the main search box. To switch to the new tab in Google Chrome, select **Ctrl + Shift + Enter**.

[Expand table](#)

Usage	Example
Find all comments	<code>History:Keyword</code>
Find all instances of "ToDo" comments in your code	Select <code>comment:</code> and enter <code>todo</code>
Search in specific locations, such as within a particular path	Use a search string such as <code>Driver path:MyShuttle/Server</code>
Search for files by name or just by file extension	<code>Driver file:GreenCabs.cs</code> . The search string <code>error ext:resx</code> could be useful if you want to review all error strings in your code. Even if your plain text search string matches part of a filename, the file appears in the list of found files. This search works without matching specific file type functions.

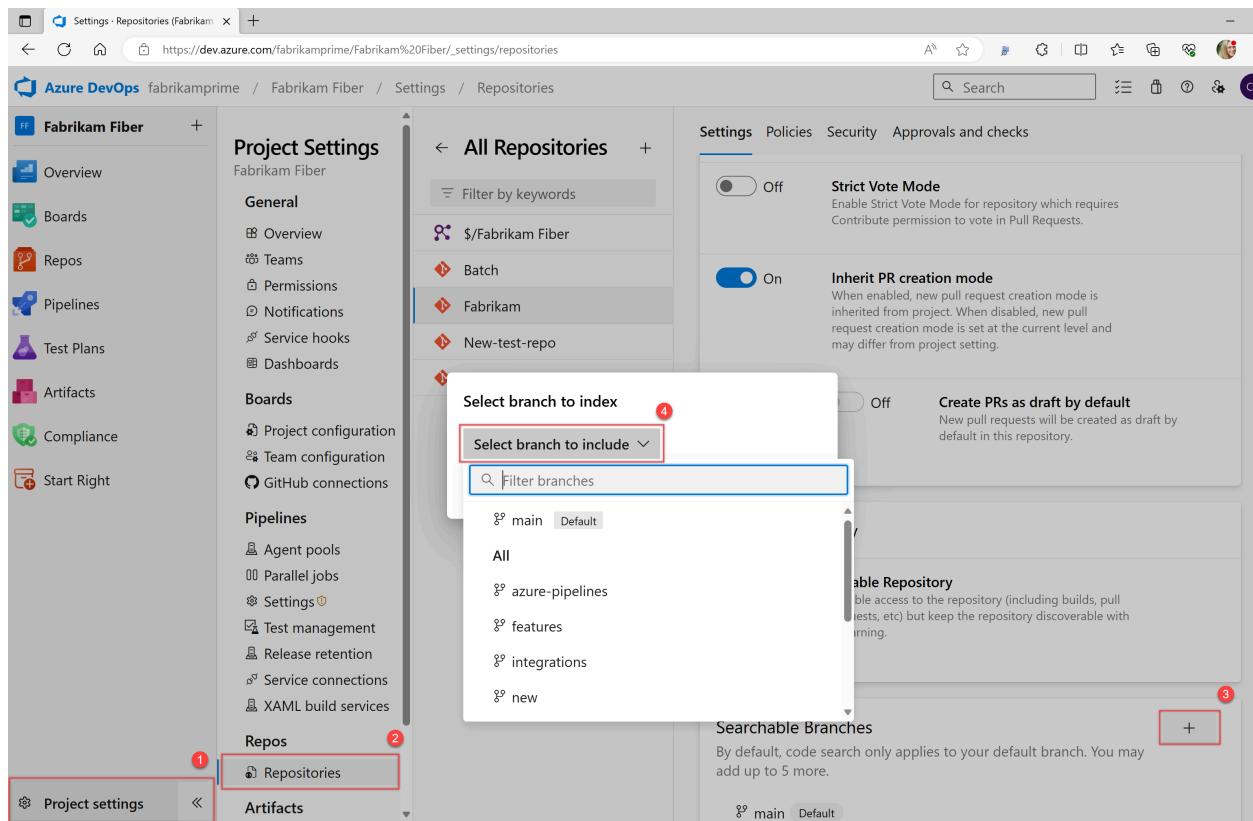
# Search Git projects and repositories

A Git project has a list of repositories. To expand your search, check the project and repository boxes. You can search all or more projects, or fewer projects and repositories. If there are many projects or repositories, select **Show more** to see them all.

Code Search can index different branches in a Git repository. It only indexes files in the default branch of your Git repositories by default. The default branch is main. To index other branches, go to the **Options** tab in the **Repositories** section of the [project settings page](#).

## ⓘ Note

By default, code search looks for the specified string in the main or default branch of a repository. But, you can narrow down the search by specifying a filter for a specific branch.



# Search TFVC projects

Team Foundation Version Control (TFVC) projects display only the folders that you can read. You can't see any other projects or folders. To filter your search, choose folders from the tree.

## 💡 Tip

Code Search saves your last settings, such as the project and repository or path that you searched in. When you want to search in a different scope, select **Clear all links** to clear the checkboxes and search across all projects. The first 100 hits or matches in the target files get highlighted by Code Search in the results pane.

# Search code with REST API

You can use APIs to extend or supplement the capabilities listed in this article. For information about Code Search with REST API, see [Fetch Code Search Results](#).

## Next steps

[Search work items](#)

## Related articles

- [Get started with Search](#)
- [Search artifacts and packages](#)
- [Search work items](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Functional work item search

Article • 10/17/2024

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Functional work item search command filters let you search for work items more precisely by assignment, work item type, specific fields, and more. For more filter functions, see [Get started with search](#).

Work Item Search lets you do the following tasks and more.

 Expand table

Search task	Description
<a href="#">Search over all your projects</a>	Search in your own and your partner teams' backlog. To search across your entire enterprise's work items, use cross-project searches. Narrow your search by using project and area path filters.
<a href="#">Search across all work item fields</a>	Quickly and easily find relevant work items by searching across all work item fields, including custom fields. Use a full text search across all fields to efficiently locate relevant work items. The snippet view indicates where matches were found.
<a href="#">Search in specific fields</a>	Use the quick in-line search filters to narrow down to a list of work items in seconds. Use the filters on any work item field. The list of suggestions helps complete your search faster. For example, a search such as <b>AssignedTo:Chris WorkItemType:Bug State:Active</b> finds all active bugs assigned to a user named Chris.
Search across test	Search across Test Plans, Test Suites, and other test work item types.
<a href="#">Take advantage of integration with work item tracking</a>	The Work Item Search interface integrates with familiar controls for managing your work items; letting you view, edit, comment, share, and more.

## Prerequisites

- **Access levels:**
  - **All project members:** Every project member can use the search functions, including users with Stakeholder, Basic, and higher levels of access.
- Work Item Search is available by default when the Boards service is installed and enabled.

## Search by work item ID

Enter the work item ID in the Azure DevOps title bar. You can read and edit the work item in a modal dialog.

The screenshot shows the Azure DevOps interface with a work item details page. At the top, there is a search bar with the placeholder "This project" and a red box highlighting the input field where "119" is typed. Below the search bar, the work item type is shown as "USER STORY 119". The title of the work item is "119 Login behaviour for booking". To the left of the title is a user icon, followed by "0 comments", "Save & Close" button, "Follow" button, and a three-dot menu. Below the title, there are tabs for "General" and other sections. Under "General", the "State" is "Closed" (indicated by a green dot) and the "Area" is "FabrikamFiber Web". The "Reason" is "Acceptance te ..." and the "Iteration" is "FabrikamFiber Web\Iteration 2". Below these fields is a "Details" button and a row of small icons. The main content area is titled "Description" and contains the text "Login behaviour for booking". Above the "Description" section is a toolbar with various rich text editing icons.

## Search across all fields

Search all work item fields, including custom ones, for natural searches. The following snippet view shows matches.

The screenshot shows a search results page with a blue header and body. The header contains the text "Search across all fields". The body contains the text "Easily search across all work item fields. The snippet indicates where the matches were found." To the right of this text is a white rectangular box containing a single vertical line, which is a visual representation of a snippet indicating a match was found.

- Use simple search strings for words or phrases. Work item search matches derived forms of your search terms; for example, a search for "updating" also finds instances of the word "updated" and "update." Searches aren't case-sensitive.
- Search from a project to, by default, search only within that project.
- Search from inside a team to, by default, search only within the default area path of that team.
  - Select a project to view a list of area paths in that project for which you have Read access.
  - Select area paths in the tree to narrow your search if necessary.
- View hit counts for all projects, even one that you don't select.
- Open the search results in a new browser tab from either the main search function or by selecting **Ctrl + Shift + Enter**.

## Best practices

- **Text search across all fields:** Use a text search across all fields to efficiently locate relevant work items. This search is useful for finding work items with similar exception traces.
- **Quick in-line search filters:** Use quick in-line search filters on any work item field to narrow down the list of work items in seconds. The list of suggestions helps you complete your search faster.

## Compare search vs. managed work item queries

The main search function and managed queries are two ways to find and list work items. For a single work item, use the main search. For a list of work items that you want to triage, update, chart, or share, use a managed query.

You can search more fields with the main search function than with managed queries.

---

### Use a managed query

#### Search

---

- List items to perform bulk updates to fields.
- Review work that's in progress or recently closed.
- Triage work: set priority, review, update.

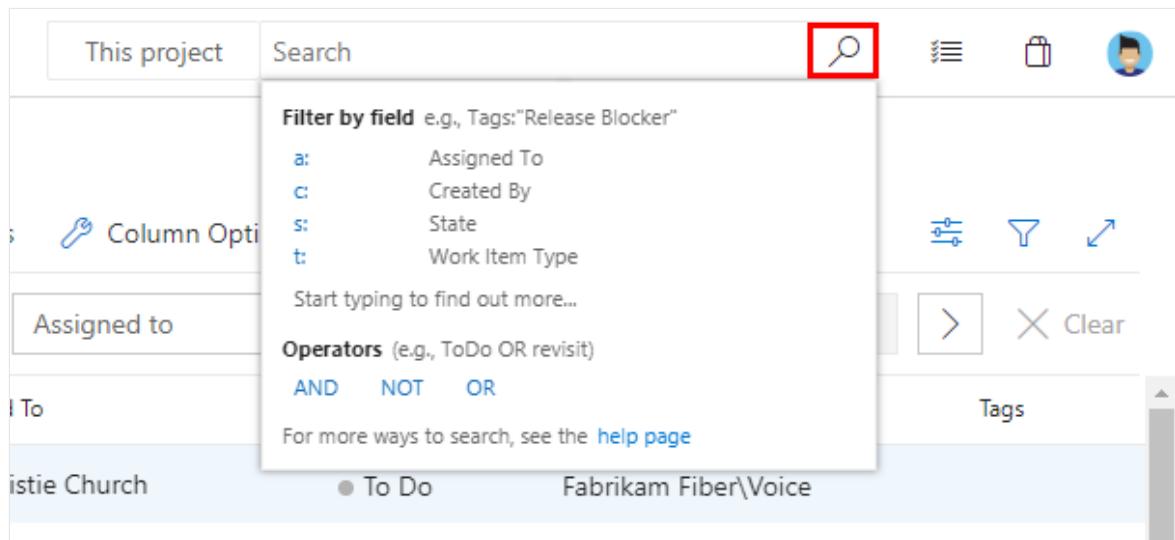
- Create a chart and add it to a dashboard.
  - Create a chart to get a count of items or sum a field.
  - Create a chart that shows a burndown or burnup over time.
  - View a tree of parent-child related work items.
  - List work items with link relationships.
  - List work items for a single project, multiple projects, or across all projects.
  - Find a specific work item using its ID or a keyword.
  - Find one or more work items across all projects in a fast, flexible manner.
  - Perform full text search across all work item fields.
  - Review work items assigned to a specific team member.
  - Search against specific work item fields to quickly narrow down a list of work items.
  - Determine what key words support a managed search.
  - List work items for a single project, multiple projects, or across all projects.
- 

For more information, see the following articles:

- [View and run a query](#)
- [Use search](#)
- [Define a query](#)
- [Query quick reference](#), [Example queries](#)

## Fine-tune your search

1. To fine-tune your search, specify fields. Search all assigned items by entering `a:` and a user name.



The screenshot shows the search interface in the Azure DevOps portal. A modal window is open over the search bar, which has a red box around its search icon. The modal title is "Filter by field e.g., Tags:'Release Blocker'" and contains the following fields:

- `a:` Assigned To
- `c:` Created By
- `s:` State
- `t:` Work Item Type

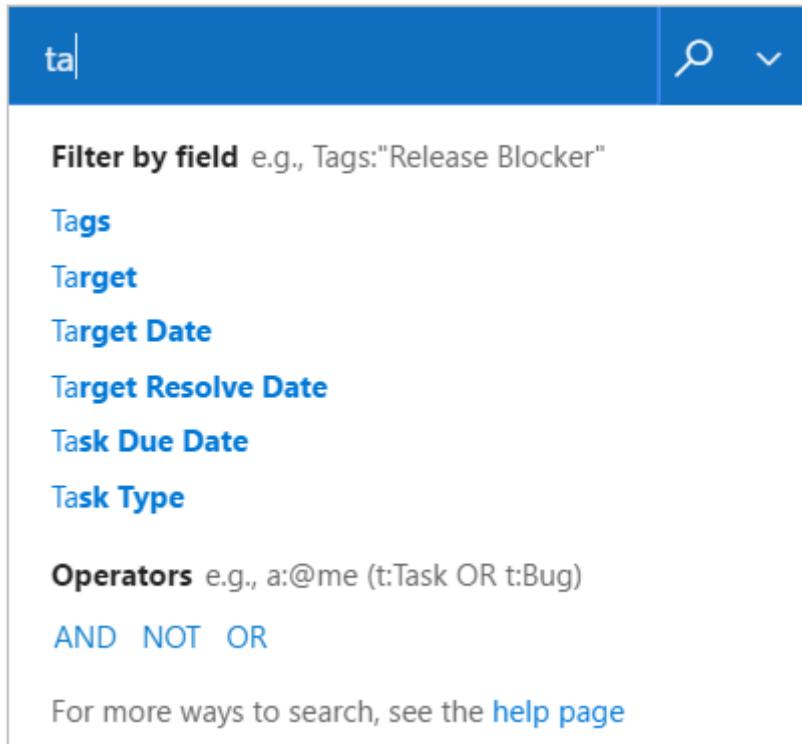
Below these fields is a text input placeholder "Start typing to find out more...". Further down are sections for "Operators (e.g., ToDo OR revisit)" with options for AND, NOT, OR, and a link to the "help page". At the bottom of the modal is a "Clear" button. The background shows a list of work items with columns for "This project", "Search", and various filters like "Column Options", "Assigned to", and "To". The "Assigned to" column shows a dropdown menu with "Fabrikam Fiber\\Voice" selected. The "To" column shows a dropdown menu with "Fabrikam Fiber\\Voice" selected. The "Search" column shows a search bar with the placeholder "Start typing to find out more..." and a search icon.

Quick filters:

- `a:` for Assigned to:

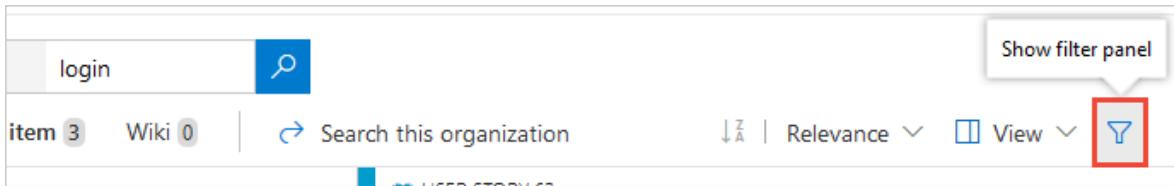
- `c:` for Created by:
- `s:` for State
- `t:` for Work item type

2. Start entering the name of a field in your work items; for example, enter `ta`.



The dropdown list shows work item field name suggestions that match user input. These suggestions help you complete the search faster. For example, a search such as `tags:Critical` finds all work items tagged 'Critical.'

3. Add more filters to further narrow your search, and use Boolean operators to combine terms if necessary. For example, `a: Chris t: Bug s: Active` finds all active bugs assigned to a user named Chris.
4. Narrow your search to specific types and states, by using the selector lists at the top of the results page.
5. Widen your search across all projects, or narrow it to specific types and states. Use the filter to show the selector lists.



6. Select the criteria you want in the drop-down selector lists, or search across the entire organization.

This screenshot shows the Azure DevOps search interface. At the top, there are buttons for 'This project' and 'login'. Below them are links for 'Code 0', 'Work item 3', and 'Wiki 0'. A search bar contains the text 'Search this organization'. To the right of the search bar are sorting options: 'Relevance' (down arrow) and 'Relevance' (down arrow). The main search results are for 'FabrikamFiber Web'. A dropdown menu for 'Area' shows 'FabrikamFiber Web' selected. Another dropdown for 'Types' shows 'All Types' selected. A third dropdown for 'States' shows 'All States' selected. The search results list three items: '119 Login behaviour for booking' (State: Closed), '62 Login page' (State: Resolved), and '97 Login and logout behaviours' (State: Closed).

- Sort the results with the drop-down list of field names, work item types, or by relevance.

This screenshot shows the same Azure DevOps search interface as above, but with the 'Sort by' dropdown menu open. The menu lists various fields: 'Assigned To', 'Changed Date', 'Created Date', 'ID', 'Relevance' (which is checked and highlighted in blue), 'State', 'Tags', 'Title', and 'Work Item Type'. The 'Relevance' option is currently selected.

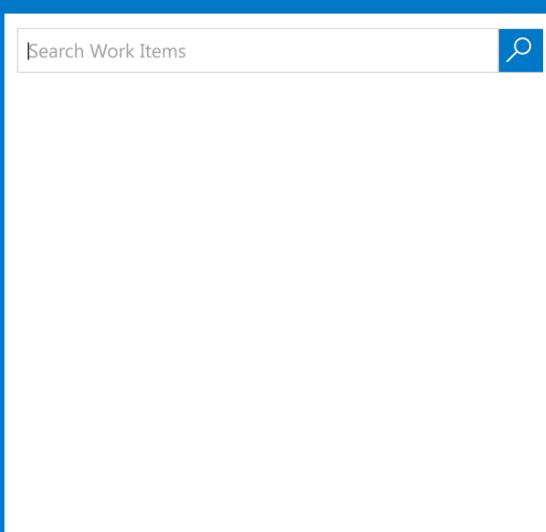
## Quick filters for matching in specific fields

Quick inline search filters let you refine work items in seconds. The dropdown list of suggestions helps complete your search faster. Mix and match the functions to create quick powerful searches.

[Expand table](#)

Usage	Example
Scope your search terms to match in any work item field, including custom fields. Enter the field name followed by the search terms.	<code>tags:Critical</code> finds work items with a 'tags' field containing the term 'Critical.'

Usage	Example
Use multiple inline search filters to scope your search by any work item field, including custom fields.	t: Bug path:"project\search" finds all bugs in the area path "project\search."
Use the operators >, >=, <, <=, =, and != for date, integer, and float fields.	t: Bug CreatedDate > @Today-7 finds all bugs created in the last week.
For search queries containing multiple terms, use quotes to group the terms. However, quotes don't yield exact matches as you might expect; results match any work items containing the grouped terms in any order.	BuildPath: "tools.demoproject.com" finds work items that contain the path "tools.demoproject.com."



**Quick Filters**

Quick in-line search filters lets you refine work items by specific criteria on any work item field, in seconds!

## Scope projects and area and iteration paths using filters

Filters make it easy to narrow the search to specified projects and area paths.

Narrow the search to a specific location using the proj, area, iteration, path, and comment filters:

[Expand table](#)

Usage	Example
Finds all occurrences of the word <b>Wiki</b> in the <b>Fabrikam</b> project.	Wiki proj:Fabrikam
Finds all occurrences of the word <b>Wiki</b> in the area path <b>Contoso/Mobile</b> and its subpaths.	Wiki area:Contoso/Mobile

Usage	Example
Finds all occurrences of the word <b>Wiki</b> in the iteration path <b>Contoso/Sprint101</b> and its subpaths.	<code>Wiki iteration:Contoso/Sprint101</code>
Enclose the argument to the filter in double-quotes if it contains a space.	<code>Wiki path:"Contoso/Windows Phones and Devices/Services"</code>
Finds backlog comments	<code>comment:todo</code>

## See more of the work item

You can quickly get a full screen view of the selected work item using  **expand** and  **shrink** in the toolbar. However, another way to see more of the work item, while you can still select work items from the list of matching results, is to hide the left column filter pane by choosing < at the top left of the column. Use > to restore the filter pane.

If you're using a portrait orientation screen, use the **Preview pane: Right** link at the top right of the window to display the code below the search results list.

### Tip

Search remembers the state of the filter pane, configuration of the work item view pane, and its position between sessions as part of your user preferences.

## Search work items with REST API

You can use APIs to extend or supplement the capabilities listed in this article. For information about Work Item Search with REST API, see [Fetch Work Item Search Results](#).

## Next steps

[Supported filter functions and more for work items](#)

## Related articles

- [Get started with Search](#)
- [Search code](#)
- [Search artifacts and packages](#)

 **Note:** The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Migration overview

Article • 02/18/2025

Moving from Azure DevOps Server to Azure DevOps Services is an essential step for organizations that want to take advantage of cloud-based collaboration, scalability, and enhanced features. In this overview, we explore the options for transferring your valuable data from the on-premises Azure DevOps Server to the cloud-based Azure DevOps Services.

For information about the main differences between on-premises Azure DevOps Server and the cloud-based Azure DevOps Services, see [Compare Azure DevOps Services with Azure DevOps Server - Azure DevOps](#).

Regardless of your selected migration option, we recommend that you determine your most important assets, such as source code and work items. You should think about your data size, organization complexity and make sure that you have enough time for test runs before actual migration for a smooth and successful transition.

## Approaches to migration

It's crucial to assess the pros and cons of each approach to migration, based on your specific motivations for adopting Azure DevOps Services. The right strategy depends on your unique context and requirements.

Expand table

Options	Recommended scenarios	Limitations
<a href="#">1: Manual migration</a>	Use for smaller projects or specific data subsets.	Not all data can be migrated with full fidelity and is subject to throttling. This migration doesn't support migrating XML templates, so you need to recreate process templates as inherited templates.
<a href="#">2: Azure DevOps Data Migration Tool</a>	Use for medium to large-scale migrations with varied data types and complex structures.	You can only "lift and shift" one Azure DevOps Server collection to one new Azure DevOps Services organization, with no modifications. For more information, see the <a href="#">Limitations section</a> .
<a href="#">3: API-based migration</a>	Offers flexibility and customization for organizations with unique migration requirements or automation needs.	Low fidelity, data loss, and ID changes can occur. For more information, see the <a href="#">Limitations section</a> .

## Option 1: Manual migration

For example, when the Azure DevOps team at Microsoft chose to move from Azure DevOps Server to Azure DevOps Services, we also decided to move from Team Foundation Version Control (TFVC) to Git. Migration required lots of planning, but when we migrated, we created a new Git repo using the "tip" version of our TFVC sources and left our history behind in Azure DevOps Server. We also moved our active work items, and left behind all our old bugs, completed user stories and tasks, and so on.

## Manual migration process

1. Identify the most important assets that you need to migrate - typically source code, work items, or both. Other assets in Azure DevOps Server - build pipelines, test plans, and so forth - are harder to manually migrate.
2. Identify a suitable time to make the transition.
3. Prepare your target organizations. Create the organizations and team projects that you need, provision users, and so on.
4. Migrate your data.
5. Consider making the source Azure DevOps Server deployments read-only. You can do so in the following ways:
  - [Adjust project-level permissions](#): Set the permissions for all users or groups to read-only at the project level, which you can do by modifying the security roles in **Project settings**.
  - [Modify repository settings](#): For each repository, you can change the settings to make them read-only, which involves adjusting the permissions for each user or group to only allow read actions.
  - [Use built-in security groups](#): Utilize the built-in security groups to manage permissions more efficiently. You can assign users to groups like "Readers" to provide read-only access.
  - Scripting permission changes: If you have many projects or repositories, you might need to script them. You can use the [Azure CLI DevOps extension](#) to list all permissions and update them as needed.
  - Disable repository feature: Disables access to the repository, including builds and pull requests, but keeps the repository discoverable with a warning. Go to **Project settings > Repositories** > your repo, and next to Disable Repository, move the toggle to **On**.

## Option 2: Azure DevOps Data Migration Tool

The [Azure DevOps Data Migration Tool](#) is a set of utilities provided by Microsoft to facilitate the migration of data from Azure DevOps Server to Azure DevOps Services. These tools offer a

streamlined approach to migrate various artifacts, including source code, work items, test cases, and other project-related data.

Before you initiate the migration process, the tools can perform a premigration analysis to assess the readiness of the source environment and identify potential issues or dependencies that might affect the migration. Assess readiness, so you can plan and mitigate potential challenges beforehand.

## Migration Tool limitations

The tool allows you to "lift and shift" one Azure DevOps Server Collection to one new Azure DevOps Service Organization, with no modifications for the following reasons:

- Data integrity and consistency:
  - When you migrate data, maintaining integrity and consistency is crucial. Allowing modifications during migration could lead to data corruption or inconsistencies.
  - The tool ensures that data remains intact during the transfer process, minimizing the risk of errors.
- Source data preservation:
  - The migration tool aims to faithfully replicate the source data in the target environment.
  - Modifications could alter the original data, potentially causing discrepancies between the migrated data and the source data.
- Predictable behavior:
  - By restricting modifications, the tool ensures predictable behavior during migration.
  - Users can rely on consistent results without unexpected changes.
- Migration focus, not transformation:
  - The primary purpose of the migration tool is to move data from one location to another.
  - Data transformation, such as modifying values, typically gets handled separately after migration.
- Supported migration scenarios:
  - Moving projects from one Azure DevOps Services organization to another Azure DevOps Services organization isn't currently supported.
  - Migrating from one Azure DevOps Server instance to another isn't supported.

You can purge data that you don't need before or after the migration.

## Migration Tool process

1. Complete the prerequisites such as updating Azure DevOps Server to one of the two most recent releases.
2. Validate each collection that you want to move to Azure DevOps Services.
3. Generate migration files.
4. Prepare everything for your migration execution.
5. Perform a test run.
6. Carry out a migration.
7. Confirm that your users and data got migrated, and the collection is functioning as expected.

## Option 3: API-based migration

If you can't use the Data Migration Tool but still want a higher fidelity migration than [Option 2](#), consider using various tools that leverage public APIs to move data. These tools include extensions available at the [Visual Studio Marketplace](#).

## API-based migration limitations

The following limitations occur with API-based migration:

- Low fidelity migration:
  - Limitation: API-based tools provide a higher fidelity than manual copying but are still relatively low fidelity.
  - Implication: While these tools offer some fidelity, they don't preserve all aspects of your data.
    - Example: None of them retain the original dates of TFVC changesets (Team Foundation Version Control).
    - Many don't preserve the changed dates of work item revisions either.
- Data loss and ID changes:
  - Limitation: During migration, the tools replay work item changes, TFVC changesets, package feeds, and pipeline artifacts.
  - Implication: This process might lead to data loss, generate new IDs, and alter creation, modification, and closure dates.
    - Example: Historical context tied to specific dates might get lost, affecting reporting and traceability.

## API-based migration process

In general, we only recommend this approach if extra fidelity beyond a manual copy is critical. If you decide to take this approach, you might consider hiring a consultant who has experience

with one or more of the tools and do a test migration before your final migration.

Many organizations need a very high-fidelity migration for only a subset of their work. New work could potentially start directly in Azure DevOps Services. Other work, with less stringent fidelity requirements, could be migrated using one of the other approaches.

## Supported process models

Azure DevOps Services supports the following process models:

- [Inherited](#)
- [Hosted XML](#)

By default, Hosted XML is turned **off** in Azure DevOps Services. We turn on the Hosted XML process model during migration only if you customized a project in Azure DevOps Server. Once your project is on Hosted XML, you can [upgrade it to inherited post migration](#).

## Key principles

When migrating into Azure DevOps Services, keep in mind the following key principles and limitations:

- **Azure DevOps Services is English only:** Azure DevOps Server supports multiple languages, however today, Azure DevOps Services only supports English. If your collection uses the non-English language or used non-English in the past and you converted the language to English during an upgrade, you can't use the Data Migration Tool.
- **Inheritance:** A project, which was created from the Agile, Scrum or CMMI process template and was never customized, is on the Inheritance process model after the migration.
- **Hosted XML:** Any project with customizations uses the Hosted XML process model.
- **Process per customized project:** Although Azure DevOps Services allows projects to share a process, the Data Migration Tool creates a Hosted XML process for each customized team project. For example, if you have 30 customized projects, you have 30 Hosted XML processes to manage. If you want to further customize your Hosted XML process for all your projects, you must update each Hosted XML process separately.
- **Process validation:** The process validation of the Data Migration Tool detects the target process model for each project. Before you can migrate, you need to fix any process validation errors for the Hosted XML projects. You might want to consider updating the process of your projects to match one of our processes (Agile, Scrum or CMMI) to take

advantage of the Inheritance process model. Learn more on the process validation types in our documentation.

## Resources

- [Report an issue in the Developer Community ↗](#)
- [Get support and provide feedback](#)

## Next steps

[Get started with the Azure DevOps Data Migration Tool](#)

## Related articles

- [Complete prerequisites for migration](#)
- [Validate and prepare for migration](#)
- [Prepare for test run](#)
- [Do test run migration](#)
- [Migrate to Azure DevOps Services](#)
- [Complete post-migration tasks](#)

# Get started with Azure DevOps Data Migration Tool

Article • 12/26/2024

Before you use the [Azure DevOps Data Migration Tool](#) to migrate your database with high fidelity, learn some of the basic concepts in this article.



## Learn which data gets migrated

Not all data gets migrated. Separate databases outside the collection, for example, reporting and SharePoint data, don't get migrated. The following sections list more detail about which data gets migrated.

### Included data

The following table shows data included in migration.

[ ] Expand table

Included data	Description
Collection mapping	Each collection in Azure DevOps Server corresponds to one database. During migration, the whole collection—including work items, history, Team Foundation Version Control (TFVC) changesets, Git data, build definitions, and more—get migrated to Azure DevOps Services. Work item, TFVC changeset, and Git commit numbers/IDs remain unchanged.

### Excluded data

The following table shows specific data exclusions in migration.

[ ] Expand table

Excluded data	Description
Extensions	Extensions must be reinstalled post-migration. You should publish local extensions to the Marketplace as private extensions and shared with the organization.

<b>Excluded data</b>	<b>Description</b>
	account.
Service Hooks	Service Hooks data isn't included in the migration; reconfigure after migration.
Load test	Load test data isn't brought over; reconfigure load tests after migration.
Pipeline agents and agent pools	Reconfigure pipeline agents and agent pools after migration.
Mentions	User mentions in work item discussions retain on-premises identity, not the new Microsoft Entra ID. Hovering on usernames doesn't display contact cards, and some hyperlinks might be invalid.
Project Server integrations	Not available for Azure DevOps Services. For example, XAML Builds, Microsoft Test Manager, SharePoint, SQL Data Warehouse, and so on.
Preview features	Some Azure DevOps Server features can be previewed during migration to Azure DevOps Services.

## Project limits

If your collection contains numerous projects, Azure DevOps Services imposes a limit of 1,000 projects per organization, although we recommend 300 or less. Beyond this threshold, certain experiences—such as connecting to the organization from Visual Studio—might degrade. To stay within the limit, consider either splitting the collection or deleting older projects.

## Understand the relationship between on-premises databases and Azure DevOps organizations.

Before you dive too deeply into planning your migration, it's important to understand at an elevated level how the database migration process functions. Migrations operate on the following main concepts:

- **Team Project Collection:** Collections in Azure DevOps Server are a physical container for team projects and their artifacts. Each collection equates to a single SQL database and is the source of migrations to Azure DevOps Services.
- **Azure DevOps Services organization:** Organizations are the management unit in the cloud-hosted service. Logically they map 1:1 to the concept of a team project collection in Azure DevOps Server. Therefore, organizations are the destination of

migrations to Azure DevOps Services. For example, Azure DevOps Services organizations are represented as <https://dev.azure.com/Contoso> where Contoso represents the name of the Azure DevOps Services organization.

When you migrate a team project collection SQL database, the Data Migration Tool creates a new Azure DevOps organization with a user-provided name. Migrating a collection database into an existing Azure DevOps Services organization or consolidating multiple collection databases into a single Azure DevOps Services organization isn't possible. The mapping is strictly one-to-one between team project collections and Azure DevOps Services organizations.

## Choose data center

When you set up your Azure DevOps Services organization, you can choose the location for your data. During initial sign-up and organization creation, select a region that suits your needs. To use later for migration, make a note of the region's shorthand code. For more information, see [Supported regions for migration](#).

## Understand pricing

A question that typically comes up with migration is what type of licensing a company needs to use Azure DevOps Services. The good news is you're likely to have all the licenses you already need. We created an example worksheet that should cover most cases. If you have any specific questions about your situation, reach out to your Developer Solution Sales Specialist or Microsoft Reseller. For more information, see [Pricing for Azure DevOps](#).

## User licenses worksheet

[ ] [Expand table](#)

#	Column 1	Column 2
1	Number of team members	
2	Number of stakeholders	
3	Subtract the value in line 2 from the value in line 1*	
4	# of Visual Studio subscribers**	
5	Subtract the value in line 4 from the value in line 3	

#	Column 1	Column 2
6	Subtract the value in line 5 from the value in line 5***	

- \*Stakeholders are free
- \*\* Visual Studio Subscribers have Azure DevOps Services included as a benefit of the subscription
- \*\*\*Each Azure DevOps Services organization gets five free users

For more information about cost-effective options for accessing features, see the [Billing overview](#) and the [Azure Pricing Calculator](#).

Buy any needed Azure DevOps Services user licenses through the Visual Studio Marketplace or the Azure portal. We delve into this process during the [Prepare for test run phase](#).

In addition to the core features, the following value-added services are available in Azure DevOps that you might find beneficial:

- Hosted load testing services: If you need to simulate and analyze the performance of your applications under load, Azure DevOps provides hosted load testing services. These services allow you to stress-test your applications and identify bottlenecks or performance issues.
- Test Manager extensions: For comprehensive test management, consider using Test Manager extensions. These extensions enhance your testing capabilities by providing features like test case management, exploratory testing, and test execution tracking.
- More features: Azure DevOps offers various extensions and integrations that cater to specific needs. Whether it's integrating with non-Microsoft tools, enhancing security, or automating deployment pipelines, there's a wide range of options.

Some of these services might come with extra costs, so it's essential to evaluate your requirements and budget accordingly. These costs appear on your bill under the associated subscription. For more information, see [Set up billing](#). If you have specific questions about your situation, contact your DevOps Partner, Microsoft Reseller, or your Microsoft Developer Solutions Sales Specialist for personalized guidance.

## Reserve your new organization

Considering the migration project's timeline, we recommend that you reserve the name of your organization early on to ensure that your desired name is available for your final migration.

For instance, if your company is Contoso and you want an organization with a matching name, for example, <https://dev.azure.com/contoso>, you can create an organization with that name now. But keep in mind that you can only migrate into a brand-new Azure DevOps Services organization.

Do the following steps to reserve your organization name.

1. Initial reservation:
  - a. Create an organization with a temporary name, for example, <https://dev.azure.com/contoso-temporary>.
  - b. Reserve this temporary name for your future migration.
2. Final migration:
  - a. When you're ready to begin the final migration, perform it into the <https://dev.azure.com/contoso-temporary> organization.
  - b. After successful migration, rename the reserved organization to open your desired name for the imported organization. Rename it rather than deleting it because a deletion can take up to an hour to release the name, when renaming it's immediate.
  - c. Immediately rename the migrated organization to the desire name, for example, <https://dev.azure.com/contoso>, that you just cleared by renaming.
  - d. Optionally, you can delete the originally reserved and renamed organization at this point.

By following this approach, you have a smooth transition while ensuring your preferred organization name remains available.

## Next steps

[Complete prerequisites for migration](#)

## Related articles

- [Validate and prepare for migration](#)
- [Prepare for test run](#)
- [Do test run migration](#)
- [Migrate to Azure DevOps Services](#)
- [Complete post-migration tasks](#)

ⓘ Note: The author created this article with assistance from AI. [Learn more](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Complete prerequisites for migration

Article • 01/09/2025

As you move to the second phase of migrating to Azure DevOps Services with the Azure DevOps Data Migration Tool, you must complete the prerequisites for transferring your data to the cloud. If your organization already meets these prerequisites, you can skip this phase entirely.



## Update Azure DevOps Server

The Data Migration Tool for Azure DevOps supports the [two latest releases of Azure DevOps Server](#) at a given time. Releases include updates and major releases.

It can take up to 2-3 weeks after a new RTW version of Azure DevOps Server is released for migration support to come online for that version. Consider this possibility when you choose to upgrade shortly after a new RTW Azure DevOps Server release.

The Data Migration Tool doesn't support migration from Azure DevOps Server release candidates (RC). If you're planning to migrate your collection database to Azure DevOps Services using this service, it's important that you don't upgrade your production database to an RC release. If you upgrade, then you must wait and upgrade to the release to web (RTW) version when it's available. Or, restore a backup copy of your database from a previous Azure DevOps Server version to migrate. You can't downgrade to a previous version of Azure DevOps, but must revert using a backup of the database at that version.

Normal release cadence for new Azure DevOps Server versions is once every three to four months. Meaning that support for a given version of Azure DevOps Server for migration to Azure DevOps Services should last for anywhere between six-to-eight months. It's important to ensure that your plan accounts for this support window to avoid having to suddenly upgrade to migrate.

## Implement Microsoft Entra ID

Ensure your team has a functional Microsoft Entra ID tenant for authenticating members in your Azure DevOps Services organization. In Azure DevOps Services, user authentication relies on a Microsoft Entra ID tenant like Azure DevOps Server user authentication relies on Active Directory. During the Test Run phase([link](#)), you verify an

identity map log file to match your on-premises Active Directory organizations with Microsoft Entra ID organizations. This file isn't used by the migration service. This action ensures individual history visibility, security permissions preservation, and access to personal settings.

### 💡 Tip

- We recommend that you use the same Microsoft Entra ID tenant as other Microsoft Cloud services. If your company already has Microsoft Entra ID, skip this step.
- While Microsoft accounts (MSAs) work for Azure DevOps Services authentication, they can't be mapped during Azure DevOps Server database migration.

## Synchronize identities and groups with Microsoft Entra ID Connect

Synchronize your on-premises Active Directory with Microsoft Entra ID, so your team members can use the same credentials to authenticate. Also, your Azure DevOps Services administrators can use your Active Directory groups for setting permissions within your organization.

To set up the synchronization, do the following steps:

1. Utilize the [Microsoft Entra ID Connect](#) technology.
2. To configure Microsoft Entra ID Connect with your on-premises environment, collaborate with your IT department, DevOps Partner, Microsoft Premier Support, or Microsoft Consulting Services.

For more information on setting up Microsoft Entra ID Connect, see [Microsoft Entra Connect Sync](#).

Also, explore how you can configure Azure DevOps Services to use Microsoft Entra ID by visiting this page. Although the steps in that article don't align exactly with your Team Foundation Server database migration, it serves as valuable reference information. The Data Migration Tool establishes the link to your Microsoft Entra ID tenant during the creation of your Azure DevOps Services organization at the start of the migration process.

### ⚠ Note

DirSync was a predecessor technology to Microsoft Entra ID Connect. Upgrade to Microsoft Entra ID Connect if you're using DirSync.

## Download Azure DevOps Data Migration Tool

The bulk of the work throughout the migration to Azure DevOps Services gets handled by the Data Migration Tool. The tool gets used with the following high-level steps:

1. Validate a team project collection.
2. Generate the files used to customize the migration.
3. Queue migration of an Azure DevOps Server database to Azure DevOps Services.

Have the following items:

- TFSEXECROLE role in SQL Server.
- Permissions to connect to both the Azure DevOps Server configuration and collection databases.
- An established link between your Azure DevOps Services organization and your Microsoft Entra ID tenant.

## Download the tool

1. Download the latest version of the [Data Migration Tool](#).
2. Copy the zip file to one of your Azure DevOps Server application tiers.
3. Unzip the file. You can also run the tool from a different machine without Azure DevOps Server installed, if it can connect to the configuration database of the Azure DevOps Server instance.  
1. Open a Command Prompt window on the server and go to the directory where the Data Migration Tool is stored.
4. Review the help content for the tool:
  - a. To view the top-level help and guidance, run the following command:  
`Migrator /help`
  - b. View the help text for the validation command: `Migrator validate /help` For your first time validating a collection, keep it simple. Your command should have the following structure: `Migrator validate /collection:{collection URL} /tenantDomainName:{name} /region:{region}`
5. Replace {name} with the name of your Microsoft Entra tenant. For example, to run against the DefaultCollection and the fabrikam tenant, the command would look like this: `Migrator validate /collection:[^1^][4] (http://localhost:8080/DefaultCollection) /tenantDomainName:fabrikam.OnMicrosoft.com /region:{region}` If you need to run

the tool from a machine other than the Azure DevOps Server, use the `/connectionString` parameter.

## Next steps

[Validate and prepare for migration](#)

## Related articles

- [Prepare for test run](#)
- [Do test run migration](#)
- [Migrate to Azure DevOps Services](#)
- [Complete post-migration tasks](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Validate and prepare server environment for migration

Article • 06/11/2024

Validation involves preparing your upgraded Azure DevOps Server environment for migration. This article assists you in troubleshooting common issues. If there were no errors and all the validation checks passed, then your team project collection is ready and you can move on to the next phase. Look through the log files to find any errors if not all checks passed.



## Prerequisites

Download the latest [Data Migration Tool](#).

## Learn process validation types

During validation, the Data Migration Tool determines the target process model for each project. It automatically assigns one of the following two process models to each project in the collection:

- **Inherited process model:** If the project was created with the Agile, Scrum, or Capability Maturity Model Integration (CMMI) process template and was never customized.
- **Hosted XML process model:** If the project process appears to be customized. A customized process contains custom fields, work item types, or other types of customizations.

When the Hosted XML process is the targeted process model, the Data Migration Tool validates if the customizations can be migrated. The Data Migration Tool generates two files during the validation:

- **DataMigrationTool.log:** Contains the set of process validation errors found in the collection. Fix all process errors found to proceed with your migration.
- **TryMatchOobProcesses.log:** Lists for each project the target process model - Inheritance or Hosted XML. For projects that are set to target the Hosted XML process model, it explains why they're considered to be customized. You don't have to fix these errors, but they give you guidance what to do in case you want to

migrate to the Inheritance process model. Once a collection gets migrated, you can migrate a project to an Inheritance process model.

## Validate a team project collection

Since each team project collection corresponds to its own SQL database, the validation process examines various aspects of your collection, including:

- Size of your collection database
- Collation of the SQL database
- Identities of users in the collection
- Template customizations (process)

To start validation, use the migrator tool. We recommend running the migrator tool from one of the application tier (AT) servers in your Azure DevOps Server environment.

For specific command-line options, request help text using the following command:

```
cmdline
```

```
    Migrator validate /help
```

The most common way to start validation is by specifying the URL of the team project collection with the following structure:

```
cmdline
```

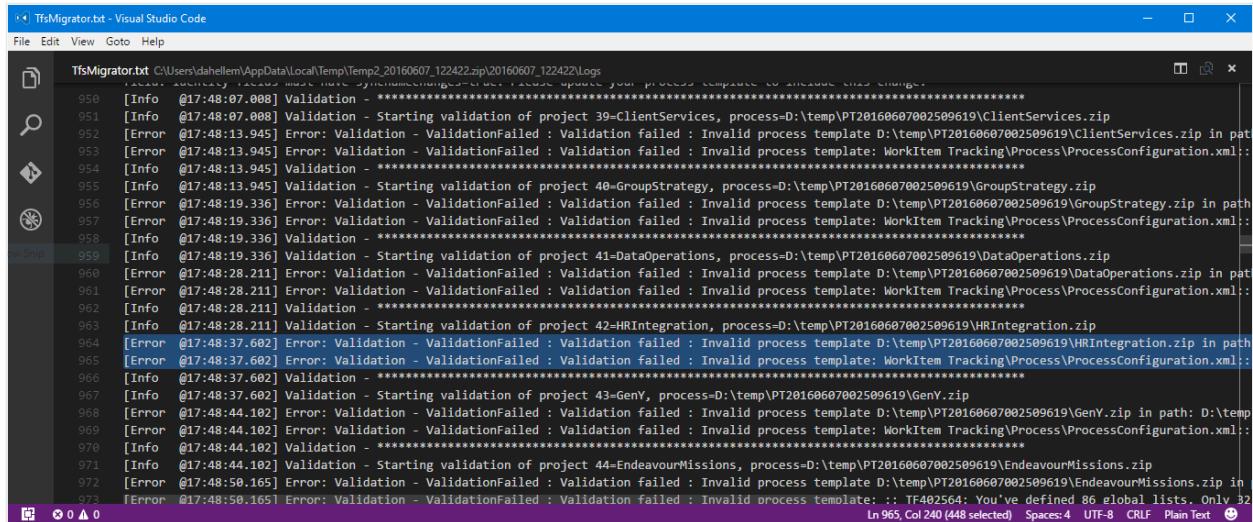
```
    Migrator validate  
    /collection:http://localhost:8080/tfs/DefaultCollection
```

## View validation warnings and errors

When the migrator tool completes, it generates log files and results displayed on the command prompt screen. If no errors occur and all validation checks pass, your team project collection is ready for the next phase. In case validation checks fail, review the log files to identify errors, and then address them.

Focus on the `Migrator.log` file, which contains essential details about the validation checks and helps you preserve customization. The other files correspond to specific validation errors based on their names. Search for the string "Validation - Starting validation of project 1." Each project is validated. Scan through all the projects and search for any lines that contain a prefix of `[Error ...]`

Also, the `TryMatchOobProcesses.log` lists errors related to projects that use Out-of-Box (OOB) processes (such as Agile, Scrum, or CMMI). If a project uses an OOB process without customizations, the project is included in the inherited model. Importantly, errors in this file don't hinder the migration process.



```
TfsMigrator.txt C:\Users\dahelle\appData\Local\Temp\20160607_122422.zip\20160607_122422\Logs
[Info] @17:48:07.008 Validation - ****
[Info] @17:48:07.008 Validation - Starting validation of project 39-ClientServices, process=D:\temp\PT20160607002509619\ClientServices.zip
[Error] @17:48:13.945 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\ClientServices.zip in path
[Error] @17:48:13.945 Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
[Info] @17:48:13.945 Validation - ****
[Info] @17:48:13.945 Validation - Starting validation of project 40-GroupStrategy, process=D:\temp\PT20160607002509619\GroupStrategy.zip
[Error] @17:48:19.336 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\GroupStrategy.zip in path
[Error] @17:48:19.336 Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
[Info] @17:48:19.336 Validation - ****
[Info] @17:48:19.336 Validation - Starting validation of project 41-DataOperations, process=D:\temp\PT20160607002509619\DataOperations.zip
[Error] @17:48:28.211 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\DataOperations.zip in path
[Error] @17:48:28.211 Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
[Info] @17:48:28.211 Validation - ****
[Info] @17:48:28.211 Validation - Starting validation of project 42-HRIntegration, process=D:\temp\PT20160607002509619\HRIntegration.zip
[Error] @17:48:37.602 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\HRIntegration.zip in path
[Error] @17:48:37.602 Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
[Info] @17:48:37.602 Validation - ****
[Info] @17:48:37.602 Validation - Starting validation of project 43-GenY, process=D:\temp\PT20160607002509619\GenY.zip
[Error] @17:48:44.102 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\GenY.zip in path: D:\temp
[Error] @17:48:44.102 Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
[Info] @17:48:44.102 Validation - ****
[Info] @17:48:44.102 Validation - Starting validation of project 44-EndeavourMissions, process=D:\temp\PT20160607002509619\EndeavourMissions.zip
[Error] @17:48:50.165 Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\EndeavourMissions.zip in path
[Error] @17:48:50.165 Error: Validation - ValidationFailed : Validation failed : Invalid process template: :: TF402564: You've defined 86 global lists. Only 32
Ln 965, Col 240 (448 selected) Spaces:4 UTF-8 CRLF Plain Text
```

For a list of validation errors, see [Resolve validation errors](#). For each validation error, we provided the error number, description, and the method to resolve. Various error types might appear in the validation check logs. Seek assistance from your trained DevOps Partner, Microsoft Consulting Services, or Microsoft Premier Support for resolving encountered errors.

## Resolve process template errors

The primary errors we find are process template issues. These issues stem from either outdated team projects not incorporating Azure DevOps Server's latest features or unsupported customizations by Azure DevOps Services. But, Azure DevOps Services does support a range of customizations, and the validation only flags those requiring resolution premigration. The Data Migration Tool performs a comprehensive check of your templates for Azure DevOps Services compatibility, but some modifications might be necessary.

- Customized process templates or outdated templates might cause process validation errors during migration.
- If you use an OOB Agile, Scrum, or CMMI process, check the `TryMatchOobProcesses.log` for errors. Error-free projects map to OOB processes.
- Some customizations don't work in Azure DevOps Services. Review the supported customization list.
- For projects using older templates, run the [Configure Features Wizard](#) to update templates with recent features and reduce error count.

- Ensure `witadmin` is available on the machine where you fix process errors. It's essential for making changes to process templates.
- For and Not rules should be commented out or removed from the process template before attempting the migration. These rules are supported in Azure DevOps Service, but they are not supported as part of the migration process. Once your collection is migrated, you can add these rules back to the process template.

Consider the following tools for resolving process errors:

- Utilize the `witadmin.exe` command-line tool included with Visual Studio installations. Detailed technical documentation on addressing these errors is available at this link.
- Automate exporting process templates for each team project using an undocumented migrator tool command: Migrator validates `/collection:http://localhost:8080/tfs/DefaultCollection /SaveProcesses`.
- Explore the TFS Team Project Manager on GitHub ([link](#)). It allows you to compare team projects with known process templates, including out-of-the-box templates.

To fix the errors, change the XML syntax and apply the changes back to the project.

#### 💡 Tip

We recommend that you modify the XML manually, rather than using TFS Power Tools.

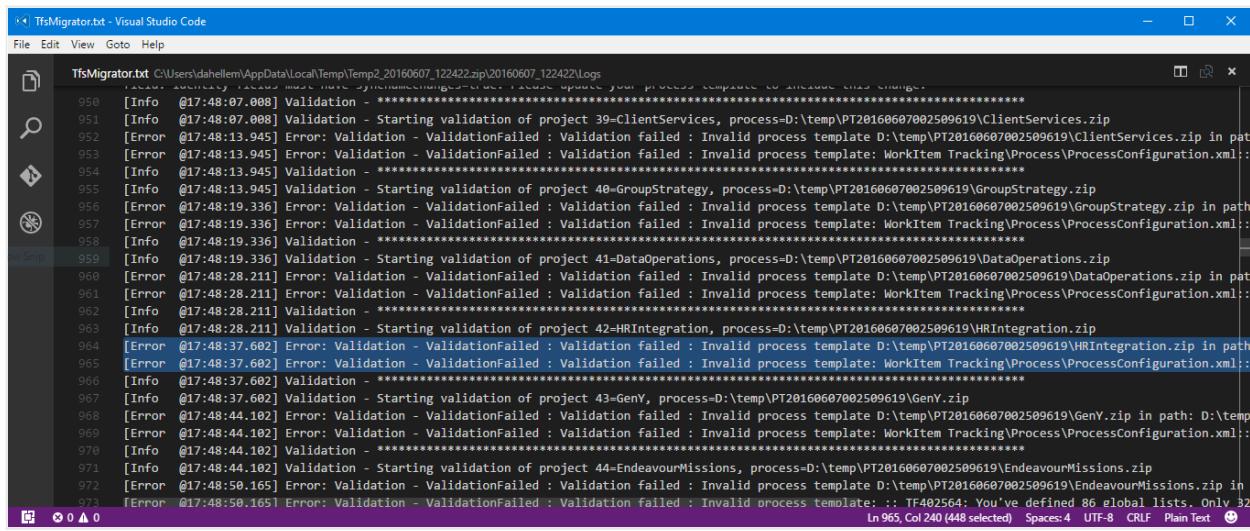
To get the process template from the project, add the `/SaveProcesses` parameter when you run the Data Migration Tool command.

cmdline

```
Migrator validate /collection:{collection URL} /tenantDomainName:{name}
/region:{region} /SaveProcesses
```

This command extracts the XML from the project and places it into the same folder as the logs. Extract the zip files to your local machine so that you can edit the files.

Now, fix the XML. Use the logs from the `DataMigrationTool.log` file to determine the errors for each project.



The screenshot shows a Visual Studio Code window with the title 'TfsMigrator.txt - Visual Studio Code'. The file contains a log of validation errors from a Data Migration Tool. The errors are primarily ValidationFailed exceptions related to project validation. The log spans from line 950 to 973. The last few lines include a warning about global lists and the number of selected items.

```
950 [Info @17:48:07.008] Validation - ****
951 [Info @17:48:07.008] Validation - Starting validation of project 39-ClientServices, process=D:\temp\PT20160607002509619\ClientServices.zip
952 [Error @17:48:13.945] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\ClientServices.zip in path
953 [Error @17:48:13.945] Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
954 [Info @17:48:13.945] Validation - ****
955 [Info @17:48:13.945] Validation - Starting validation of project 40-GroupStrategy, process=D:\temp\PT20160607002509619\GroupStrategy.zip
956 [Error @17:48:19.336] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\GroupStrategy.zip in path
957 [Error @17:48:19.336] Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
958 [Info @17:48:19.336] Validation - ****
959 [Info @17:48:19.336] Validation - Starting validation of project 41-DataOperations, process=D:\temp\PT20160607002509619\DataOperations.zip
960 [Error @17:48:28.211] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\DataOperations.zip in path
961 [Error @17:48:28.211] Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
962 [Info @17:48:28.211] Validation - ****
963 [Info @17:48:28.211] Validation - Starting validation of project 42-HRIntegration, process=D:\temp\PT20160607002509619\HRIntegration.zip
964 [Error @17:48:37.602] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\HRIntegration.zip in path
965 [Error @17:48:37.602] Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
966 [Info @17:48:37.602] Validation - ****
967 [Info @17:48:37.602] Validation - Starting validation of project 43=GenY, process=D:\temp\PT20160607002509619\GenY.zip
968 [Error @17:48:44.102] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\GenY.zip in path: D:\temp
969 [Error @17:48:44.102] Error: Validation - ValidationFailed : Validation failed : Invalid process template: WorkItem Tracking\Process\ProcessConfiguration.xml:::
970 [Info @17:48:44.102] Validation - ****
971 [Info @17:48:44.102] Validation - Starting validation of project 44-EndeavourMissions, process=D:\temp\PT20160607002509619\EndeavourMissions.zip
972 [Error @17:48:50.165] Error: Validation - ValidationFailed : Validation failed : Invalid process template D:\temp\PT20160607002509619\EndeavourMissions.zip in path
973 [Error @17:48:50.165] Error: Validation - ValidationFailed : Validation failed : Invalid process template: :: TF402564: You've defined 86 global lists. Only 32
```

Some errors require you to do use a `witadmin changefield` command. Changing a field name is the most common example. To save yourself some time, we recommend you run the `witadmin changefield` command and then rerun the Data Migration Tool. Doing so re-exports the XML with the corrected names. Otherwise, manually fix the fields in the XML syntax as well.

Once you make a fix, apply the changes back to the Azure DevOps Server. Depending on the changes you made, you need to run one or more `witadmin` commands. We created a PowerShell script to automate this process. The script contains all of the `witadmin` commands needed to confirm the entire process.

You can get the scripts at Process Customization Scripts. Use the `import/ConformProject.ps1` script.

```
cmdline

.\conformproject.ps1 "<collection url>" "<project name>" "<process template folder>"
```

When the script completes, rerun the Data Migration Tool to validate the collection. Follow steps 1 through 3 until the Data Migration Tool generates no more validation errors.

```
PS C:\Process\import> .\ConformProject.ps1 "http://localhost:8080/tfs/DefaultCollection" "foo" "C:\Process\B  
Unable to find witadmin.exe on your path. Attempting VS install directories  
Testing for C:\Program Files (x86)\Microsoft Visual Studio 14.0\Common7\IDE\witadmin.exe  
Step 1: Preparing Conform  
Operation Complete  
Step 1: Complete  
Step 2: Validating Work Items  
Step 2: Complete  
Step 3: Conform project - Link Types  
Importing Link Type: MicrosoftVSTSCommonAffects.xml  
The link types were imported successfully.  
Importing Link Type: MicrosoftVSTSCommonTestedBy.xml  
The link types were imported successfully.  
Importing Link Type: MicrosoftVSTSTestCaseSharedParameterReferencedBy.xml  
The link types were imported successfully.  
Importing Link Type: MicrosoftVSTSTestCaseSharedStepReferencedBy.xml  
The link types were imported successfully.  
Step 3: Complete  
Step 4: Conform project - Type Definitions  
Importing Work Item Type: Bug.xml  
|
```

### Tip

If you're new to XML and witadmin, we suggest you make one fix at a time and then conform. Continue this loop until all errors are resolved.

## Update to a system process

If you began with an older version of Azure DevOps Server, your projects likely use an older process template. If these projects weren't updated using the [Configure Features Wizard](#), the Data Migration Tool detects process errors. In rare cases, even the wizard might not resolve old process-related issues.

You might receive some of the following sample error messages:

no-highlight

```
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402571: Required element  
PortfolioBacklog is missing from Process Configuration.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402571: Required element  
BugWorkItems is missing from Process Configuration.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402571: Required element  
FeedbackRequestWorkItems is missing from Process Configuration.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402571: Required element  
FeedbackResponseWorkItems is missing from Process Configuration.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField Team.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField RemainingWork.  
Invalid process template: WorkItem
```

```
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField Order.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField Effort.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField Activity.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField ApplicationStartInformation.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField ApplicationLaunchInstructions.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF402574: ProcessConfiguration  
doesn't specify required TypeField ApplicationType.  
Invalid process template: WorkItem  
Tracking\Process\ProcessConfiguration.xml:: TF400572: The Project Process  
Settings must be configured for this feature to be used.
```

If you didn't customize your project (for example, added fields, work item types, and so on.), fixing these errors is straightforward. But, if you customized your process, this approach doesn't suffice. You need to manually adjust the process templates to preserve your customizations from being overwritten.

Do the following steps, for each project, to align your process:

1. Identify the initial process your project started with (Scrum, Agile, or CMMI).
2. Visit the Process Customization Scripts on GitHub and download the repository.
3. Focus on the contents in the Migration folder.
4. Utilize the following `ConformProject.ps1` script to align a project of your choice with the Agile system process. This action updates the entire project to be Agile.

cmdline

```
.\ConformProject.ps1 "<collection url>" "<project name>" "c:\process-  
customization-scripts\import\agile"
```

## Common validation errors

**VS402841: Field X in work item type Bug has syncnamechanges=false but has rules making it an identity field. Identity fields must have**

## **syncnamechanges=true. Please update your process template to include this change.**

In Azure DevOps Services, we added a rule so that every identity field must have the `syncnamechanges=true` attribute. In Azure DevOps Server that rule doesn't apply.

Therefore, the Data Migration Tool identifies this as an issue. Making this change on Azure DevOps Server on-premises doesn't cause any harm.

Run the `witadmin changefield` command. Syntax for the command looks like the following example.

```
cmdline
```

```
witadmin changefield  
/collection:http://AdventureWorksServer:8080/tfs/DefaultCollection  
/n:fieldname /syncnamechanges:true
```

For more information on the `witadmin changefield` command, see [Manage work item fields](#).

## **TF402556: For field System.IterationId to be well defined, you must name it Iteration ID and set its type to Integer.**

This error is often associated with outdated process templates. To address it, you can run the [Configure Features Wizard](#) for each project. Alternatively, you might execute the following command to automate the process.

```
cmdline
```

```
witadmin changefield  
/collection:http://AdventureWorksServer:8080/tfs/DefaultCollection  
/n:fieldname /name:newname
```

## **TF402571: Required element BugWorkItems is missing from Process Configuration.**

This error is commonly seen when a process wasn't updated for some time. To fix it, run the [Configure Features Wizard](#) for each project.

## **TF402564: You've defined XX global lists. Only 64 are allowed**

Azure DevOps Services natively supports 64 global lists. This error typically arises when there's an extensive number of build pipelines, as each new pipeline creates a global list named `Builds - TeamProjectName`. To resolve this error, remove any outdated global lists.

## Repeat validation checks

In each iteration, address errors and conduct validation checks to resolve them, as indicated by the validation log files. Persist with this cycle until all errors are rectified and you receive confirmation that the collection validation checks are successful.

## Next steps

[Prepare for test run](#)

## Related articles

- [witadmin: Customize and manage objects for tracking work](#)
- [Differences between Azure DevOps Services and Azure DevOps Server process template customizations](#)
- [Configure features after Azure DevOps Server upgrade](#)
- [Resolve validation errors](#)
- [Define global lists in Azure DevOps Server](#)
- [Process customization PowerShell scripts ↗](#)

---

## Feedback

Was this page helpful?

 Yes

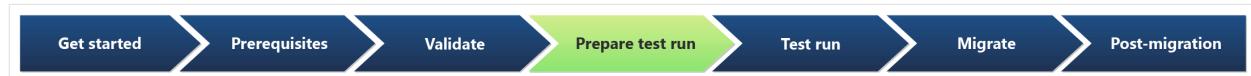
 No

[Provide product feedback ↗](#)

# Prepare for test run migration

Article • 10/25/2024

This article focuses on team preparation and file generation required by the Data Migration Tool.



## Prerequisites

Complete the [Validate phase](#) before you begin to prepare for test run migration.

## Generate migration settings

Do the following steps to generate the migration specification and related files to queue the migration of your collection database.

1. Run the Data Migration Tool prepare command with the following parameters:

```
/collection:http://localhost:8080/tfs/DefaultCollection/  
tenantDomainName:contoso.com /Region:CUS
```

- The tenant domain name option is the name of your company's Microsoft Entra ID tenant.
- The prepare command requires internet access. If your Azure DevOps Server lacks internet connectivity, run the command from a different computer.
- The term "organization region" refers to the location where you plan to migrate your collection into Azure DevOps Services. You previously selected a region and recorded its shorthand code. Use this code in the prepare command.

2. Sign in with a user from the tenant who has permission to read information about all users in the Microsoft Entra ID tenant.

## Configure the migration specification file

The migration specification file is a JSON file that instructs the Data Migration Tool how to do the following actions.

- Configure your migrated organization

- Specify the source locations
- Customize the migration

Many of the fields are auto populated during the prepare step but you must configure the following fields:

- **Organization name:** The name of the organization you want to create for migrating your data.
- **Location:** A backup of your database and migration files to be uploaded to an Azure storage container. This field specifies the SAS key used by the migration tool to securely connect to and read the source files from the Azure storage container. Creating the storage container is covered later in Phase 5 and generating a SAS key is covered in Phase 6 before you queue for a new migration.
- **DACPAC:** A file that packages up your collection's SQL database.
- **Migration type:** The type of migration: Test run or Production run.

Each migration specification file is meant for a single collection. If you try to use a migration specification file generated for another collection, the migration doesn't start. You need to prepare a test run for each collection you wish to migrate and use the generated migration specification file to queue the migration.

## Review the identity map log file

The identity map log is crucial, as important as the actual data that you migrate. When you examine the log file, understand how identity migration functions and the potential outcomes. When you migrate an identity, it can be either active or historical. Active identities can sign in to Azure DevOps Services, while historical identities can't. The service decides which type gets used.

### Note

Once an identity gets migrated as a historical identity, there's no way to convert it to an active one.

## Active identities

Active identities refer to user identities in Azure DevOps Services post-migration. In Azure DevOps Services, these identities are licensed and are displayed as users in the organization. The identities are marked as active in the **Expected Import Status** column in the identity map log file.

## Historical identities

Historical identities are mapped as such in the Expected Import Status column in the identity map log file. Identities without a line entry in the file also become historical. An example of an identity without a line entry might be an employee who no longer works at a company.

Unlike active identities, historical identities:

- Don't have access to an organization after migration.
- Don't have licenses.
- Don't show up as users in the organization. All that persists is the notion of that identity's name in the organization, so that its history can be searched later. We recommend that you use historical identities for users who no longer work at the company or who don't need further access to the organization.

### ⓘ Note

After an identity migrates as historical, you can't make it active.

## Licenses

During migration, licenses get assigned automatically for all users displayed as "active" in the Expected Import Status column of identity mapping log. If automatic license assignment is incorrect, you can change it by editing the "access level" of one or more users after migration completes.

Assignment might not always be perfect, so you have until the first of the following month to reassign licenses as needed. If by the first of the next month you don't link a subscription to your organization and purchased the correct number of licenses, all your grace period licenses get revoked. Alternatively, if auto assignment assigned more licenses than you purchased for next month, then we don't charge you for the extra licenses, but we revoke all unpaid licenses.

To avoid losing access, we recommend you link a subscription and purchase needed licenses before the first of the month, as billing runs monthly. For all test runs, licenses are free for as long as the organization is active.

## Azure DevOps subscriptions

Visual Studio Subscriptions aren't assigned by default for migrations. Instead, users with Visual Studio Subscriptions automatically get upgraded to use that license. If a user's work organization is linked correctly, Azure DevOps Services automatically applies their Visual Studio subscription benefits on their first sign-in post migration.

You don't need to repeat a test run migration if users don't automatically get upgraded to use their Visual Studio Subscription in Azure DevOps Services. Visual Studio Subscription linking is something that happens outside of the scope of a migration. If the work organization gets linked correctly before or after the migration, then the user automatically has their license upgraded on the next sign in. Once they're upgraded, next time you migrate the user automatically gets upgraded upon initial sign-in to the organization.

## Restrict access to Azure DevOps Services IPs only

- [Option 1: Use Service Tags](#)
- [Option 2: Use IP List](#)

Restrict access to your Azure Storage account to only IPs from Azure DevOps Services. You can restrict access by only allowing connections from Azure DevOps Services IPs that are involved in the collection database migration process. The IPs that need to be granted access to your storage account depend on the region you're migrating into.

### Option 1: Use Service Tags

You can easily allow connections from all Azure DevOps Services regions by adding the `azuredevops` Service Tag to your network security groups or firewalls either through the portal or programmatically.

### Option 2: Use IP List

Use the `IpList` command to get the list of IPs that need to be granted access to allow connections from a specific Azure DevOps Services region.

Included in the help documentation are instructions and examples for running Migrator from the Azure DevOps Server instance itself and a remote machine. If you're running the command from one of the Azure DevOps Server instance's application tiers, your command should have the following structure:

```
cmdline
```

```
Migrator IpList /collection:{CollectionURI} /tenantDomainName:{name}  
/region:{region}
```

You can add the list of IPs to your network security groups or firewalls either through the portal or programmatically.

## Configure IP firewall exceptions for SQL Azure

This section only applies to configuring firewall exceptions for SQL Azure. For DACPAC migrations, see [Configure Azure Storage firewalls and virtual networks](#).

The Data Migration Tool requires the Azure DevOps Services IPs get configured for inbound connections only on port 1433.

Do the following steps to grant exceptions for the necessary IPs handled at the Azure networking layer for your SQL Azure VM.

1. Sign in to the Azure portal.
2. Go to your SQL Azure VM.
3. In **Settings**, select **Networking**.
4. Select **Add inbound port rule**.



PROTOCOL	SOURCE	DESTINATION	ACTION	
TCP	Any	Any	<input checked="" type="checkbox"/> Allow	...
TCP	Any	Any	<input checked="" type="checkbox"/> Allow	...
Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow	...
Any	AzureLoadBalancer	Any	<input checked="" type="checkbox"/> Allow	...
Any	Any	Any	<input checked="" type="checkbox"/> Deny	...

5. Select **Advanced** to configure an inbound port rule for a specific IP.

The screenshot shows the 'Add inbound security rule' dialog box. At the top, there's a 'Service' dropdown set to 'Custom'. Below it is a 'Port range' input field containing '8080' with a green checkmark. A 'Priority' input field contains '1510'. The 'Name' input field contains 'Port\_8080' with a green checkmark. A 'Description' text area is empty. The 'Advanced' button at the top left is highlighted with a red box.

6. In the **Source** drop-down list, select **IP Addresses**, enter an IP address that needs to be granted an exception, set the **Destination port range** to **1433** and, in the **Name** box, enter a name that best describes the exception you're configuring.

Depending on other configured inbound port rules, you might need to change the default priority for the Azure DevOps Services exceptions, so they don't get ignored. For example, if you have a "deny on all inbound connections to 1433" rule with a higher priority than your Azure DevOps Services exceptions, the Data Migration Tool might be unable to make a successful connection to your database.

\* Source 

IP Addresses



\* Source IP address range 



\* Source port range 

\*



\* Destination 

Any



\* Destination port range 

1433



\* Protocol

Any	TCP	UDP
-----	-----	-----

\* Action

Allow	Deny
-------	------

\* Priority 

1010



\* Name

--	--	--	--	--	--	--	--



## Description

Repeat adding inbound port rules until all necessary Azure DevOps Services IPs are granted an exception. Missing one IP could result in your migration failing to start.

## Migrate large collections

For databases that the Data Migration Tool warns are too large, a different data packaging approach is required to migrate to Azure DevOps Services. If you're unsure whether your collection exceeds the size threshold, you should run a Data Migration Tool validation on the collection. The validation lets you know whether you need to use the SQL Azure VM method for migration.

### Determine if you can reduce the collection size

Check to see whether you can clean up old data. Over time, collections can build up large volumes of data. This growth is a natural part of the DevOps process, but you might find you don't need to retain all the data. Some common examples of no longer relevant data are older workspaces and build results.

The Data Migration Tool scans your collection and compares it to the limits mentioned previously. It then reports whether your collection is eligible for DACPAC or SQL migration method. In general, the idea is that if your collection is small enough to fit within the DACPAC limits, you can use the faster and simpler DACPAC approach. However, if your collection is too large, you need to use the SQL migration method, which involves setting up a SQL Azure VM and migrating the database manually.

### Size limits

The current limits are:

- 150 GB total database size (database metadata + blobs) for DACPAC, if you exceed this limit, then you need to perform the SQL migration method.

- 30 GB individual table size (database metadata + blobs) for DACPAC, if any single table exceeds this limit, then you need to perform the SQL migration method.
- 1,536 GB database metadata size for SQL migration method. Exceeding this limit issues a warning, we advise that you keep under this size to have a successful migration.
- 2,048 GB database metadata size for SQL migration method. Exceeding this limit results in an error, so you can't perform a migration.
- No limit for blob sizes for SQL migration method.

When you clean older, no-longer-relevant artifacts, it could remove a lot more space than you might expect, and it could determine whether you use the DACPAC migration method or a SQL Azure VM.

 **Important**

Once you delete older data, you can't recover it unless you restore an older backup of the collection.

If you're under the DACPAC threshold, follow the instructions to generate a DACPAC for migration. If you still can't get the database under the DACPAC threshold, you need to set up a SQL Azure VM to migrate to Azure DevOps Services.

## Set up a SQL Azure VM to migrate to Azure DevOps Services

Do the following high-level steps to set up a SQL Azure virtual machine (VM) to migrate to Azure DevOps Services.

1. [Set up a SQL Azure VM](#)
2. [Configure IP firewall exceptions](#)
3. [Restore your database on the VM](#)
4. [\[Configure your collection for migration\]](#)
5. [Configure the migration specification file to target the VM](#)

## Set up a SQL Azure VM

You can set up a SQL Azure VM from the Azure portal quickly. For more information, see [Use the Azure portal to provision a Windows virtual machine with SQL Server](#).

The performance of your SQL Azure VM and attached data disks have a significant impact on the performance of the migration. For this reason, we highly recommend

doing the following tasks:

- Select a VM Size at the level of `D8s_v5_*` or greater.
- Use managed disks.
- Consult [virtual machine and disk performance](#). Ensure your infrastructure is configured so that the VM IOPS (input/output per second) and storage IOPS don't become a bottleneck on the performance of the migration. For example, ensure the number of data disks attached to your VM is sufficient to support the IOPS from the VM.

Azure DevOps Services is available in several [Azure regions across the globe](#). To ensure that the migration starts successfully, it's critical to place your data in the correct region. If you set up your SQL Azure VM in a wrong location, the migration fails to start.

 **Important**

The Azure VM requires a public IP address.

If you're using this migration method, create your VM in a supported region. Although Azure DevOps Services is available in multiple regions in the United States (US), only the Central United States region accepts new organizations. You can't migrate your data into other US Azure regions now.

 **Note**

DACPAC customers should consult the region table in the "Step 3: Upload the [DACPAC file](migration-test-run.md#)" section. The preceding guidelines are for SQL Azure VMs only. If you're a DACPAC customer, see [supported Azure regions for migration](#).

Use the following SQL Azure VM configurations:

- Configure the SQL temporary database to use a drive other than drive C. Ideally the drive should have ample free space; at least equivalent to your database's largest table.
- If your source database is still over 1 terabyte (TB) after you reduced its size, you need to attach more 1-TB disks and combine them into a single partition to restore your database on the VM.
- If your collection databases are over 1 TB in size, consider using an SSD (solid state hard drives) for both the temporary database and collection database. Also,

consider using larger VMs with 16 virtual CPUs (vCPUs) and 128 GB (gigabytes) of RAM (random access memory).

## Restore your database on the VM

After you set up and configure an Azure VM, you need to take your detached backup from your Azure DevOps Server instance to your Azure VM. The collection database needs to be restored on your SQL instance and doesn't require Azure DevOps Server to be installed on the VM.

## Configure your collection for migration

After your collection database restores on your Azure VM, configure a SQL sign-in to allow Azure DevOps Services to connect to the database to migrate the data. This sign-in allows only read access to a single database.

1. Open SQL Server Management Studio on the VM, and then open a new query window against the database to be migrated.
2. Set the database's recovery to simple:

SQL

```
ALTER DATABASE [<Database name>] SET RECOVERY SIMPLE;
```

3. Create a SQL sign-in for the database, and assign that sign-in the 'TFSEXECROLE', like the following example.

SQL

```
USE [<database name>]
CREATE LOGIN <pick a username> WITH PASSWORD = '<pick a password>'
CREATE USER <username> FOR LOGIN <username> WITH DEFAULT_SCHEMA=[dbo]
EXEC sp_addrolemember @rolename='TFSEXECROLE', @membername='<username>'
```

See the following example of the SQL command:

SQL

```
ALTER DATABASE [Foo] SET RECOVERY SIMPLE;

USE [Foo]
CREATE LOGIN fabrikam WITH PASSWORD = 'fabrikampassword'
```

```
CREATE USER fabrikam FOR LOGIN fabrikam WITH DEFAULT_SCHEMA=[dbo]
EXEC sp_addrolemember @rolename='TFSEXECROLE', @membername='fabrikam'
```

### ⓘ Important

Enable SQL Server and Windows authentication mode in SQL Server Management Studio on the VM. If you don't enable authentication mode, the migration fails.

## Configure the migration specification file to target the VM

Update the migration specification file to include information about how to connect to the SQL Server instance. Open your migration specification file and make the following updates:

1. Remove the DACPAC parameter from the source files object. The migration specification before the change looks like the following example code.

```
"Source": {
  "Location": "<Provide the SASKey to the Azure storage container with the collection and import files.>",
  "Files": {
    "Dacpac": " _DefaultCollection.dacpac"
  }
},
```

The migration specification after the change looks like the following example code.

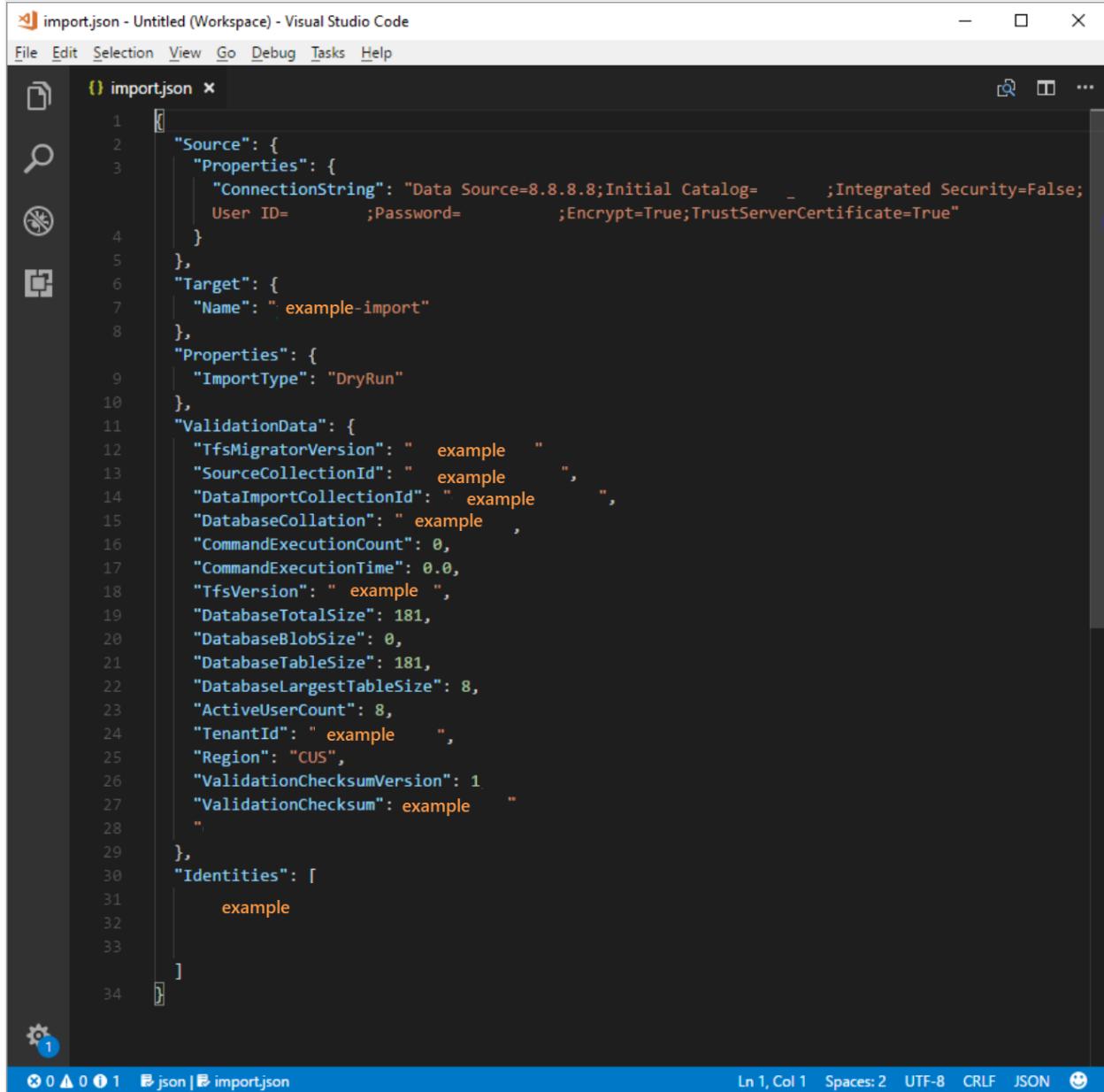
```
"Source": {
  "Properties": {
    "ConnectionString": "Data Source=8.8.8.8;Initial Catalog= _ ;Integrated Security=False;
      User ID= ;Password= !;Encrypt=True;TrustServerCertificate=True"
  }
},
```

2. Enter the required parameters and add the following properties object within your source object in the specification file.

JSON

```
"Properties": {
  "ConnectionString": "Data Source={SQL Azure VM Public IP};Initial Catalog={Database Name};Integrated Security=False;User ID={SQL Login Username};Password={SQL Login Password};Encrypt=True;TrustServerCertificate=True"
}
```

After you apply the changes, the migration specification looks like the following example.



The screenshot shows a Visual Studio Code window with the title "import.json - Untitled (Workspace) - Visual Studio Code". The code editor displays the following JSON configuration:

```
import.json
{
  "Source": {
    "Properties": {
      "ConnectionString": "Data Source=8.8.8.8;Initial Catalog= ;Integrated Security=False;User ID= ;Password= ;Encrypt=True;TrustServerCertificate=True"
    }
  },
  "Target": {
    "Name": "example-import"
  },
  "Properties": {
    "ImportType": "DryRun"
  },
  "ValidationData": {
    "TfsMigratorVersion": " example ",
    "SourceCollectionId": " example ", "DataImportCollectionId": " example ", "DatabaseCollation": " example ", "CommandExecutionCount": 0, "CommandExecutionTime": 0.0, "TfsVersion": " example ", "DatabaseTotalSize": 181, "DatabaseBlobSize": 0, "DatabaseTableSize": 181, "DatabaseLargestTableSize": 8, "ActiveUserCount": 8, "TenantId": " example ", "Region": "CUS", "ValidationChecksumVersion": 1, "ValidationChecksum": "example "
  },
  "Identities": [
    "example"
  ]
}
```

The status bar at the bottom shows "Ln 1, Col 1" and "Spaces: 2" and "UTF-8 CRLF JSON".

Your migration specification is now configured to use a SQL Azure VM for migration. Proceed with the rest of the preparation steps for migration. After the migration finishes, be sure to delete the SQL sign-in or rotate the password. Microsoft doesn't retain the sign-in information after the migration completes.

## Create an Azure Storage Container in chosen data center

Using the Data Migration Tool for Azure DevOps requires having an Azure Storage container in the same Azure data center as the final Azure DevOps Services organization. For example, if you intend for your Azure DevOps Services organization to be created in the Central United States data center, then create the Azure Storage

container in that same data center. This action drastically speeds up the time that it takes to migrate the SQL database, since the transfer occurs within the same data center.

For more information, see [Create a storage account](#).

## Set up billing

A grace period is placed on the newly migrated Azure DevOps Services organization to allow your team to finish any steps it needs and correct license assignments. If you anticipate that you might want to purchase any more user plans, build or deployment pipelines, hosted build services, hosted load test services, for example, we highly recommend that you make sure you have an Azure Subscription ready for linking to your migrated organization. The grace period ends on the first day of the following month after you completed your migration.

We remind you again in the Post-migration phase([link](#)) for when you need to do the linking. This preparation step is more about making sure that you know which Azure Subscription you use in that later step. For more information, see [Set up billing for your organization](#).

## Next steps

[Do test run migration](#)

## Related articles

- [Migrate to Azure DevOps Services](#)
- [Complete post-migration tasks](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Do test run migration

Article • 04/04/2025

Your team is now ready to begin the process of starting a test run of your migration and then finally a full production migration. In this phase, we discuss the final steps to queue a migration in addition to other tasks that typically come up at the end of the migration project.



## Prerequisites

Complete the [Prepare test run phase](#) before you begin a test run migration.

### i Important

To ensure a smooth migration process, perform one or more test run imports. A test run import lasts for 45 days for testing and validation. After 45 days, the test run times out and gets removed, requiring you to start over if needed. The more time that passes between the test run and production run, the more the service might change, potentially introducing errors that a fresh test run would catch. You can rerun the test run import as many times as needed. Each import begins from the initial state of the imported database, as it's not possible for changes from one import to persist to another. Note the following points:

- You can't extend a test run indefinitely
- You can't promote a test run to a production run
- A test run gets deleted if any of the following occur:
  - The test run times out
  - A new test run with the same name is run
  - A production run starts
  - The organization is manually deleted via organization settings

## Validate a collection

Validate each collection that you want to migrate to Azure DevOps Services. The validation step examines various aspects of your collection, including, but not limited to, size, collation, identity, and processes.

Run the validation by using the Data Migration Tool.

1. Download the Data Migration Tool [↗](#).
2. Copy the zip file to one of your Azure DevOps Server application tiers.
3. Unzip the file. You can also run the tool from a different machine without Azure DevOps Server installed, as long as the machine can connect to the configuration database of the Azure DevOps Server instance.
4. Open a Command Prompt window on the server, and enter a cd command to change to the directory where the Data Migration Tool is stored. Take a few moments to review the help content for the tool.
  - a. To view the top-level help and guidance, run the following command.

```
cmdline
```

```
Migrator /help
```

- b. View the help text for the command.

```
cmdline
```

```
Migrator validate /help
```

5. As your first time validating a collection, your command should have the following simple structure.

```
cmdline
```

```
Migrator validate /collection:{collection URL} /tenantDomainName:{name}  
/region:{region}
```

Where `{name}` provides the name of your Microsoft Entra tenant, for example, to run against the *DefaultCollection* and the *fabrikam* tenant, the command would look like the following example.

```
cmdline
```

```
Migrator validate /collection:http://localhost:8080/DefaultCollection  
/tenantDomainName:fabrikam.OnMicrosoft.com /region:{region}
```

6. To run the tool from a machine other than the Azure DevOps Server, you need the `/connectionString` parameter. The connection string parameter points to your Azure

DevOps Server configuration database. As an example, if the validated command runs by the Fabrikam corporation, the command would look like.

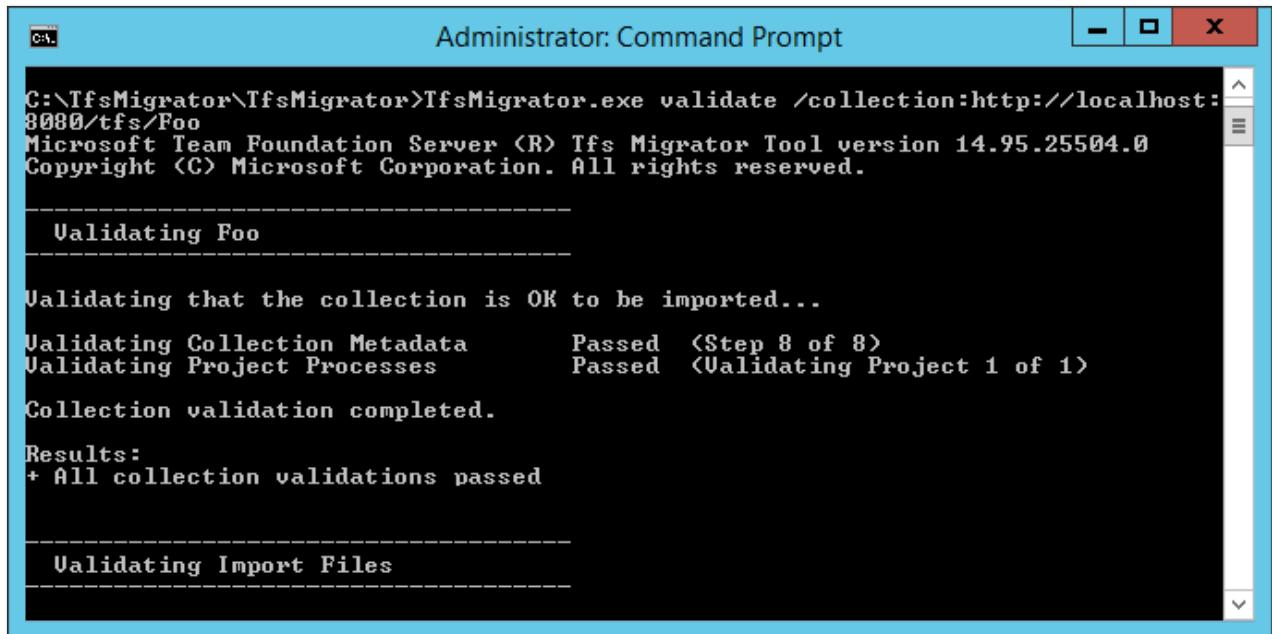
```
cmdline
```

```
Migrator validate /collection:http://fabrikam:8080/DefaultCollection  
/tenantDomainName:fabrikam.OnMicrosoft.com /region:{region}  
/connectionString:"Data Source=fabrikam;Initial  
Catalog=Configuration;Integrated Security=True"
```

### Important

The Data Migration Tool *does not* edit any data or structures in the collection. It reads the collection only to identify issues.

7. After the validation is complete, you can view the log files and results.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "C:\TfsMigrator\TfsMigrator>TfsMigrator.exe validate /collection:http://localhost:8080/tfs/Foo". The output displays the Microsoft Team Foundation Server (R) Tfs Migrator Tool version 14.95.25504.0 and copyright information. It then proceeds to validate the collection "Foo", reporting that the collection is OK to be imported, validating collection metadata and project processes (both passed), and confirming that collection validation completed successfully with all validations passed. Finally, it begins validating import files.

```
C:\TfsMigrator\TfsMigrator>TfsMigrator.exe validate /collection:http://localhost:8080/tfs/Foo
Microsoft Team Foundation Server (R) Tfs Migrator Tool version 14.95.25504.0
Copyright (C) Microsoft Corporation. All rights reserved.

-----
Validating Foo

Validating that the collection is OK to be imported...
Validating Collection Metadata      Passed  (Step 8 of 8)
Validating Project Processes        Passed  (Validating Project 1 of 1)

Collection validation completed.

Results:
* All collection validations passed

-----
Validating Import Files
```

During validation, you receive a warning if some of your pipelines contain per-pipeline retention rules. Azure DevOps Services uses a [project-based retention model](#) and doesn't support per-pipeline retention policies. If you proceed with the migration, the policies aren't carried over to the hosted version. Instead, the default project-level retention policies apply. Retain builds important to you to avoid their loss.

After all the validations pass, you can move to the [next step of the migration process](#). If the Data Migration Tool flags any errors, correct them before you proceed. For guidance on correcting validation errors, see [Troubleshoot migration and migration errors](#).

## Import log files

When you open the log directory, you might notice several logging files.

The main log file is named *DataMigrationTool.log*. It contains details about everything that was run. To make it easier for you to focus on specific areas, a log generates for each major validation operation.

For example, if TfsMigrator reports an error in the "Validating Project Processes" step, you can open the *ProjectProcessMap.log* file to view everything that was run for that step instead of having to scroll through the entire log.

Review the *TryMatchOobProcesses.log* file only if you're trying to migration your project processes to use the inherited model. If you don't want to use the inherited model, you can ignore these errors, because they don't prevent you from importing to Azure DevOps Services. For more information, see the [Validate phase of migration](#).

## Generate migration files

The Data Migration Tool validated the collection and it's returning a result of "All collection validations passed." Before you take a collection offline to migrate it, generate the migration files. When you run the `prepare` command, you generate two migration files:

- *IdentityMapLog.csv*: Outlines your identity map between Active Directory and Microsoft Entra ID.
- *migration.json*: Requires you to fill out the migration specification you want to use to kick off your migration.

## Prepare command

The `prepare` command assists with generating the required migration files. Essentially, this command scans the collection to find a list of all users to populate the identity map log, *IdentityMapLog.csv*, and then tries to connect to Microsoft Entra ID to find each identity's match. To do so, your company needs to use the [Microsoft Entra Connect tool](#) (formerly known as the Directory Synchronization tool, Directory Sync tool, or DirSync.exe tool).

If directory synchronization is set up, the Data Migration Tool should find the matching identities and mark them as *Active*. If there are no matches, the identity is marked as *Historical* in the identity map log, so you must investigate why the user isn't included in your directory sync. The migration specification file, *migration.json*, should be populated before the migration.

Unlike the `validate` command, `prepare` does require an internet connection, because it needs to connect to Microsoft Entra ID to populate the identity map log file. If your Azure DevOps Server instance doesn't have internet access, run the tool from a machine that does. As long as

you can find a machine with an intranet connection to your Azure DevOps Server instance and an internet connection, you can run this command. For help with the `prepare` command, run the following command:

```
cmdline
```

```
Migrator prepare /help
```

Included in the help documentation are instructions and examples for running the `Migrator` command from the Azure DevOps Server instance itself and a remote machine. If you're running the command from one of the Azure DevOps Server instance's application tiers, your command should have the following structure:

```
cmdline
```

```
Migrator prepare /collection:{collection URL} /tenantDomainName:{name} /region:{region}
```

```
cmdline
```

```
Migrator prepare /collection:{collection URL} /tenantDomainName:{name} /region:{region} /connectionString:"Data Source={sqlserver};Initial Catalog=Configuration;Integrated Security=True"
```

The `ConnectionString` parameter is a pointer to the configuration database of your Azure DevOps Server instance. As an example, if the Fabrikam corporation runs the `prepare` command, the command looks like the following example:

```
cmdline
```

```
Migrator prepare /collection:http://fabrikam:8080/DefaultCollection /tenantDomainName:fabrikam.OnMicrosoft.com /region:{region} /connectionString:"Data Source=fabrikam;Initial Catalog=Configuration;Integrated Security=True"
```

When the Data Migration Tool runs the `prepare` command, it runs a complete validation to ensure that nothing changed with your collection since the last full validation. If any new issues are detected, no migration files are generated.

Shortly after the command starts running, a Microsoft Entra sign-in window displays. Sign in with an identity that belongs to the tenant domain, which is specified in the command. Make sure that the specified Microsoft Entra tenant is the one you want your future organization to

be backed with. In our Fabrikam example, a user enters credentials that are similar to the following example screenshot.

**ⓘ Important**

Don't use a test Microsoft Entra tenant for a test migration and your production Microsoft Entra tenant for the production run. Using a test Microsoft Entra tenant can result in identity migration issues when you begin your production run with your organization's production Microsoft Entra tenant.

When you run the `prepare` command successfully in the Data Migration Tool, the results window displays a set of logs and two migration files. In the log directory, find a logs folder and two files:

- *migration.json* is the migration specification file. We recommend that you take time to fill it out.
- *IdentityMapLog.csv* contains the generated mapping of Active Directory to Microsoft Entra identities. Review it for completeness before you kick off a migration.

The two files are described in greater detail in the next sections.

## The migration specification file

The migration specification, *migration.json*, is a JSON file that provides migration settings. It includes the desired organization name, storage account information, and other information. Most of the fields are autopopulated, and some fields require your input before you attempt a migration.

```
import.json - Untitled (Workspace) - Visual Studio Code
File Edit Selection View Go Debug Tasks Help
import.json x
{
  "Source": {
    "Location": "<Provide the SASKey to the Azure storage container with the collection and import files.>",

    "Files": {
      "Dacpac": "Tfs_DefaultCollection.dacpac"
    }
  },
  "Target": {
    "Name": "fabrikam-import"
  },
  "Properties": {
    "ImportType": "<Provide the Type of Import: DryRun, ProductionRun>"
  },
  "ValidationData": {
    "TfsMigratorVersion": "16.255.65000 a",
    "SourceCollectionId": "example",
    "DataImportCollectionId": "example",
    "DatabaseCollation": "example",
    "CommandExecutionCount": 0,
    "CommandExecutionTime": 0.0,
    "TfsVersion": "example",
    "DatabaseTotalSize": 181,
    "DatabaseBlobSize": 0,
    "DatabaseTableSize": 181,
    "DatabaseLargestTableSize": 8,
    "ActiveUserCount": 8,
    "TenantId": "example",
    "Region": "CUS",
    "ValidationChecksumVersion": 1,
    "ValidationChecksum": "example"
  },
  "Identities": [
    "example"
  ]
}
Ln 1, Col 1  Spaces: 2  UTF-8  CRLF  JSON  ☺
```

The *migration.json* file's displayed fields and required actions are described in the following table:

[Expand table](#)

Field	Description	Required action
Source	Information about the location and names of the source data files that are used for migration.	No action required. Review information for the subfield actions to follow.
Location	The shared access signature key to the Azure storage account that hosts the data-tier application package (DACPAC).	No action required. This field is covered in a later step.

Field	Description	Required action
Files	The names of the files containing migration data.	No action required. Review information for the subfield actions to follow.
DACPAC	A DACPAC file that packages the collection database to be used to bring in the data during the migration.	No action required. In a later step, you create this file by using your collection and then upload it to an Azure storage account. Update the file based on the name you use when you generate it later in this process.
Target	Properties of the new organization to migration into.	No action required. Review information for the subfield actions to follow.
Name	The name of the organization to be created during the migration.	<p>Provide a name. The name can be quickly changed later after the migration completed.</p> <p><b>NOTE:</b> <i>Don't</i> create an organization with this name before you run the migration. The organization is created as part of the migration process.</p>
ImportType	The type of migration that you want to run.	No action required. In a later step, select the type of migration to run.
Validation Data	Information needed to help drive your migration experience.	The Data Migration Tool generates the "ValidationData" section. It contains information to help drive your migration experience. Don't* edit the values in this section, or your migration could fail to start.

After you complete the preceding process, you should have a file that looks like the following example.

The screenshot shows a Visual Studio Code window with the title bar "import.json - Untitled (Workspace) - Visual Studio Code". The menu bar includes File, Edit, Selection, View, Go, Debug, Tasks, and Help. The left sidebar has icons for file operations like Open, Save, Find, and Refresh. The main editor area contains the following JSON code:

```
1  [
2    "Source": {
3      "Location": "<Provide the SASKey to the Azure storage container with the collection and import files.>",
4      "Files": {
5        "Dacpac": "Tfs_DefaultCollection.dacpac"
6      }
7    },
8    "Target": {
9      "Name": "fabrikam-import"
10 },
11 "Properties": {
12   "ImportType": "<Provide the Type of Import: DryRun, ProductionRun>"
13 },
14 "ValidationData": {
15   "TfsMigratorVersion": "16.255.65000 a",
16   "SourceCollectionId": "example      ",
17   "DataImportCollectionId": "example      ",
18   "DatabaseCollation": "example      ",
19   "CommandExecutionCount": 0,
20   "CommandExecutionTime": 0.0,
21   "TfsVersion": "example      ",
22   "DatabaseTotalSize": 181,
23   "DatabaseBlobSize": 0,
24   "DatabaseTableSize": 181,
25   "DatabaseLargestTableSize": 8,
26   "ActiveUserCount": 8,
27   "TenantId": "example      ",
28   "Region": "CUS",
29   "ValidationChecksumVersion": 1,
30   "ValidationChecksum": "example      "
31 },
32 "Identities": {
33   "example      "
34 },
35 },
36 ],
37 ]
```

The status bar at the bottom shows "0 0 0 0 1 json | import.json" on the left and "Ln 1, Col 1 Spaces: 2 UTF-8 CRLF JSON 😊" on the right.

In the preceding image, the planner of the Fabrikam migration added the organization name *fabrikam-import* and selected CUS (Central United States) as the geographical location for migration. Other values were left as is to be modified just before the planner took the collection offline for the migration.

### (!) Note

Test run imports have a '-dryrun' automatically appended to the end of the organization name, which you can change after the migration.

## Supported Azure regions for migration

Azure DevOps Services is available in several [Azure geographical locations](#). But, not all locations where Azure DevOps Services is available are supported for migration. The following table lists the Azure geographical locations that you can select for migration. Also included is the value that you need to place in the migration specification file to target that geography for migration.

 Expand table

Geographical location	Azure geographical location	Import specification value
United States	Central United States	CUS
Europe	Western Europe	WEU
United Kingdom	United Kingdom South	UKS
Australia	Australia East	EAU
South America	Brazil South	SBR
Asia Pacific	South India	MA
Asia Pacific	Southeast Asia (Singapore)	SEA
Canada	Central Canada	CC

## The identity map log

The identity map log is of equal importance to the actual data that you migrate to Azure DevOps Services. As you're reviewing the file, it's important to understand how identity migration operates and what the potential results could entail. When you migrate an identity, it can become either *active* or *historical*. Active identities can sign in to Azure DevOps Services, but historical identities can't.

### Active identities

Active identities refer to user identities in Azure DevOps Services post-migration. In Azure DevOps Services, these identities are licensed and are displayed as users in the organization. The identities are marked as *active* in the **Expected Import Status** column in the identity map log file.

### Historical identities

Historical identities are mapped as such in the **Expected Import Status** column in the identity map log file. Identities without a line entry in the file also become historical. An example of an identity without a line entry might be an employee who no longer works at a company.

Unlike active identities, historical identities:

- *Don't have access to an organization after migration.*
- *Don't have licenses.*
- *Don't show up as users in the organization. All that persists is the notion of that identity's name in the organization, so that its history can be searched later. We recommend that you use historical identities for users who no longer work at the company or who don't need further access to the organization.*

 **Note**

After an identity is imported as historical, it *can't* become active.

## Understand the identity map log file

The identity map log file is similar to the example shown here:

AD: User(TFS)	AD: Security Identifier	AAD: Expected Import User(VSTS)	Expected Import Status	Validation Date
FABRIKAM\Jamal Hartnett	example	No Match Found (Check AAD Sync)	Historical	2017-10-31T21:15:44Z
FABRIKAM\Raisa Pokrovskaya	example	example @fabrikam.com	Active	2017-10-31T21:15:44Z

The columns in the identity map log file are described in the following table:

You and your Microsoft Entra admin must investigate users marked as *No Match Found (Check Microsoft Entra ID Sync)* to understand why they aren't part of your Microsoft Entra Connect Sync.

 [Expand table](#)

Column	Description
Active Directory: User (Azure DevOps Server)	The friendly display name used by the identity in Azure DevOps Server. This name makes it easier to identify which user the line in the map is referencing.
Active Directory: Security Identifier	The unique identifier for the on-premises Active Directory identity in Azure DevOps Server. This column is used to identify users in the collection.
Microsoft Entra ID: Expected Import User (Azure DevOps Services)	Either the expected sign-in address of the matched soon-to-be-active user or <i>No Match Found (Check Microsoft Entra ID Sync)</i> , which indicates that the identity got lost during the Microsoft Entra ID Sync and is imported as historical.

Column	Description
Expected Import Status	The expected user migration status: either <i>Active</i> if there's a match between your Active Directory and Microsoft Entra ID, or <i>Historical</i> if there isn't a match.
Validation Date	The last time the identity map log was validated.

As you read through the file, notice whether the value in the **Expected Import Status** column is *Active* or *Historical*. *Active* indicates that the identity on this row maps correctly on migration becomes active. *Historical* means that the identities become historical on migration. It's important to review the generated mapping file for completeness and correctness.

### i Important

The migration fails if major changes occur to your Microsoft Entra Connect security ID sync between migration attempts. You can add new users between test runs, and you can make corrections to ensure that previously imported historical identities become active. But, you can't change an existing user that was previously imported as active. Doing so causes your migration to fail. An example of a change is completing a test run migration, deleting an actively imported identity from Microsoft Entra ID, re-creating the user in Microsoft Entra ID, and then attempting another migration. In this case, an active identity migration attempts between the Active Directory and newly created Microsoft Entra identity, but causes a migration failure.

1. Review the correctly matched identities. Are all the expected identities present? Are the users mapped to the correct Microsoft Entra identity?

If any values need to be updated, contact your Microsoft Entra administrator to ensure the on-premises Active Directory identity is synced with Microsoft Entra ID and configured correctly. For more information, see [Integrate your on-premises identities with Microsoft Entra ID](#).

2. Next, review the identities that are labeled as *historical*. This labeling implies that a matching Microsoft Entra identity couldn't be found, for any of the following reasons:

- The identity isn't set up for sync between on-premises Active Directory and Microsoft Entra ID.
- The identity isn't populated in your Microsoft Entra ID yet (for example, there's a new employee).
- The identity doesn't exist in your Microsoft Entra instance.
- The user who owns that identity no longer works at the company.

To address the first three reasons, set up the intended on-premises Active Directory identity to sync with Microsoft Entra ID. For more information, see [Integrate your on-premises identities with Microsoft Entra ID](#). You must set up and run Microsoft Entra Connect for identities to be imported as *active* in Azure DevOps Services.

You can ignore the fourth reason, because employees who are no longer at the company should be imported as *historical*.

## Historical identities (small teams)

### ! Note

Only small teams should consider the identity migration strategy proposed in this section.

If Microsoft Entra Connect isn't configured, all users in the identity map log file are marked as *historical*. Running a migration this way results in all users being imported as *historical*. We strongly recommend that you configure [Microsoft Entra Connect](#) to ensure that your users are imported as *active*.

Running a migration with all historical identities has consequences that need to be considered carefully. Only teams with a few users and for which the cost of setting up Microsoft Entra Connect is deemed too high should consider.

To migration all identities as historical, follow the steps outlined in later sections. When you queue a migration, the identity used to queue the migration is bootstrapped into the organization as the organization owner. All other users are imported as historical. Organization owners can then [add the users back in](#) by using their Microsoft Entra identity. The added users are treated as new users. They don't\* own any of their history, and there's no way to reparent this history to the Microsoft Entra identity. However, users can still look up their premigration history by searching for their `\<domain>\<Active Directory username>`.

The Data Migration Tool displays a warning if it detects the complete historical identities scenario. If you decide to go down this migration path, you need to consent in the tool to the limitations.

## Visual Studio subscriptions

The Data Migration Tool can't detect Visual Studio subscriptions (formerly known as MSDN benefits) when it generates the identity map log file. Instead, we recommend that you apply the auto license upgrade feature after the migration. As long as users' work accounts are [linked](#) correctly, Azure DevOps Services automatically applies their Visual Studio subscription benefits

at their first sign-in after the migration. You're never charged for licenses that are assigned during the migration, so you can safely handle subscriptions afterward.

You don't need to repeat a test run migration if users' Visual Studio subscriptions aren't automatically upgraded in Azure DevOps Services. Visual Studio subscription linking happens outside the scope of a migration. As long as their work account is linked correctly before or after the migration, users' licenses are automatically upgraded on their next sign-in. After their licenses are upgraded successfully, the next time you run a migration, the users are upgraded automatically on their first sign-in to the organization.

## Prepare for migration

Now you have everything ready to execute on your test run migration. Schedule downtime with your team to take the collection offline for the migration. When you agree upon a time to run the migration, upload the required assets you generated and a copy of the database to Azure. Preparing for migration consists of the following five steps.

Step 1: [Take the collection offline and detach it.](#) Step 2: [Generate a DACPAC file from the collection you're going to migrate.](#)

Step 3: [Upload the DACPAC file and migration files to an Azure storage account.](#)

Step 4: [Generate an SAS token to access the storage account.](#)

Step 5: [Complete the migration specification.](#)

### !Note

Before performing a production migration, we *strongly* recommend completing a test run migration. A test run allows you to validate that the migration process works for your collection and ensures there are no unique data shapes or issues that could cause a production migration to fail.

## Step 1: Detach your collection

[Detaching the collection](#) is a crucial step in the migration process. Identity data for the collection resides in the Azure DevOps Server instance's configuration database while the collection is attached and online. When a collection is detached from the Azure DevOps Server instance, it takes a copy of that identity data and packages it with the collection for transport. Without this data, the identity portion of the migration *can't* be executed.

### 💡Tip

Keep the collection detached until the migration completes to avoid losing any changes made during the migration, as these changes can't get migrated afterward. After backing up your collection for migration, you can reattach it. However, any changes made after the backup aren't included in the migration, which might raise concerns about having the most current data. You can use an offline detach for test runs, but this process might not align with recommended migration practices. Review the documentation on [offline detach](#) to fully understand its implications and how it fits into your migration strategy.

It's important to weigh the cost of choosing to incur zero downtime for a test run. It requires taking backups of the collection and configuration database, restoring them on a SQL instance, and then creating a detached backup. A cost analysis could prove that taking just a few hours of downtime to directly take the detached backup is better in the end.

## Step 2: Generate a DACPAC file

DACPACs offer a fast and relatively easy method for moving collections into Azure DevOps Services. However, after a collection database size exceeds a certain threshold, the benefits of using a DACPAC start to diminish.

### Note

If the Data Migration Tool displays a warning that you can't use the DACPAC method, you have to perform the migration by using the SQL Azure virtual machine (VM) method. Skip steps 2 to 5 in that case and follow instructions in the [Prepare test run phase, Migrate large collections section](#), and then continue to [determine the migration type](#). If the Data Migration Tool doesn't display a warning, use the DACPAC method described in this step.

**DACPAC** is a feature of SQL Server that allows databases to be packaged into a single file and deployed to other instances of SQL Server. A DACPAC file can also be restored directly to Azure DevOps Services, so you can use it as the packaging method for getting your collection's data in the cloud.

### Important

- When you use SqlPackage.exe, you must use the .NET Framework version of SqlPackage.exe to prepare the DACPAC. The MSI Installer must be used to install the .NET Framework version of SqlPackage.exe. Don't use the dotnet CLI or .zip (Windows .NET 6) versions of SqlPackage.exe because those versions might generate DACPACs that are incompatible with Azure DevOps Services.

- Version 161 of SqlPackage encrypts database connections by default and might not connect. If you receive a sign-in process error, add `;Encrypt=False;TrustServerCertificate=True` to the connection string of the SqlPackage statement.

Download and install SqlPackage.exe using the latest MSI Installer from the [SqlPackage release notes](#).

After you use the MSI Installer, SqlPackage.exe installs in a path similar to

`%PROGRAMFILES%\Microsoft SQL Server\160\DAC\bin\`.

When you generate a DACPAC, keep two considerations in mind: the disk that the DACPAC is saved on and the disk space on the machine that's generating the DACPAC. You want to ensure that you have enough disk space to complete the operation.

As it creates the package, SqlPackage.exe temporarily stores data from your collection in the temp directory on drive C of the machine you're initiating the packaging request from.

You might find that your drive C is too small to support creating a DACPAC. You can estimate the amount of space you need by looking for the largest table in your collection database. DACPACs are created one table at a time. The maximum space requirement to run the generation is roughly equivalent to the size of the largest table in the collection's database. If you save the generated DACPAC to drive C, consider the size of the collection database as reported in the *DataMigrationTool.log* file from a validation run.

The *DataMigrationTool.log* file provides a list of the largest tables in the collection each time the command is run. For an example of table sizes for a collection, see the following output. Compare the size of the largest table with the free space on the drive that hosts your temporary directory.

### Important

Before you proceed with generating a DACPAC file, ensure that your collection is [detached](#).

cmdline

		Size in MB
[Info	@08:23:59.539]	Table name
[Info	@08:23:59.539]	dbo.tbl_Content
[Info	@08:23:59.539]	dbo.tbl_LocalVersion
[Info	@08:23:59.539]	dbo.tbl_Version
[Info	@08:23:59.539]	dbo.tbl_FileReference

[Info @08:23:59.539] dbo.Rules	68
[Info @08:23:59.539] dbo.tbl_FileMetadata	61

Ensure that the drive that hosts your temporary directory has at least as much free space. If it doesn't, you need to redirect the temp directory by setting an environment variable.

cmdline

```
SET TEMP={location on disk}
```

Another consideration is where the DACPAC data is saved. Pointing the saved location to a far-off remote drive could result in longer generation times. If a fast drive such as a solid-state drive (SSD) is available locally, we recommend that you target the drive as the DACPAC save location. Otherwise, it's always faster to use a disk that's on the machine where the collection database resides rather than a remote drive.

Now that you identified the target location for the DACPAC and ensured that you have enough space, it's time to generate the DACPAC file.

Open a Command Prompt window and go to the SqlPackage.exe location. To generate the DACPAC, replace the placeholder values with the required values, and then run the following command:

cmdline

```
SqlPackage.exe /sourceconnectionstring:"Data Source={database server name};Initial Catalog={Database Name};Integrated Security=True" /targetFile:{Location & File name} /action:extract /p:ExtractAllTableData=true /p:IgnoreUserLoginMappings=true /p:IgnorePermissions=true /p:Storage=Memory
```

- **Data Source:** The SQL Server instance that hosts your Azure DevOps Server collection database.
- **Initial Catalog:** The name of the collection database.
- **targetFile:** The location on the disk and the DACPAC file name.

A DACPAC generation command that's running on the Azure DevOps Server data tier itself is shown in the following example:

cmdline

```
SqlPackage.exe /sourceconnectionstring:"Data Source=localhost;Initial Catalog=Foo;Integrated Security=True" /targetFile:C:\DACPAC\Foo.dacpac /action:extract /p:ExtractAllTableData=true /p:IgnoreUserLoginMappings=true /p:IgnorePermissions=true /p:Storage=Memory
```

The output of the command is a DACPAC file, generated from the collection database *Foo* called *Foo.dacpac*.

## Configure your collection for migration

After your collection database restores on your Azure VM, configure a SQL sign-in to allow Azure DevOps Services to connect to the database to migration the data. This sign-in allows only *read* access to a single database.

To start, open SQL Server Management Studio on the VM, and then open a new query window against the database to be imported.

Set the database's recovery to simple:

SQL

```
ALTER DATABASE [<Database name>] SET RECOVERY SIMPLE;
```

Create a SQL sign-in for the database, and assign that sign-in the 'TFSEXECROLE':

SQL

```
USE [<database name>]
CREATE LOGIN <pick a username> WITH PASSWORD = '<pick a password>'
CREATE USER <username> FOR LOGIN <username> WITH DEFAULT_SCHEMA=[dbo]
EXEC sp_addrolemember @rolename='TFSEXECROLE', @membername='<username>'
```

Following our Fabrikam example, the two SQL commands would look like the following example:

SQL

```
ALTER DATABASE [Fabrikam] SET RECOVERY SIMPLE;

USE [Foo]
CREATE LOGIN fabrikam WITH PASSWORD = 'fabrikampassword'
CREATE USER fabrikam FOR LOGIN fabrikam WITH DEFAULT_SCHEMA=[dbo]
EXEC sp_addrolemember @rolename='TFSEXECROLE', @membername='fabrikam'
```

### ! Note

Enable [SQL Server and Windows authentication mode](#) in SQL Server Management Studio on the VM. If you don't enable authentication mode, the migration fails.

## Configure the migration specification file to target the VM

Update the migration specification file to include information about how to connect to the SQL Server instance. Open your migration specification file and make the following updates.

1. Remove the DACPAC parameter from the source files object.

The migration specification before the change is shown in the following code.

```
"Source": {  
    "Location": "<Provide the SASKey to the Azure storage container with the collection and  
import files.>",  
    "Files": {  
        "Dacpac": "    _DefaultCollection.dacpac"  
    }  
},
```

The migration specification after the change is shown in the following code.

```
"Source": {  
    "Properties": {  
        "ConnectionString": "Data Source=8.8.8.8;Initial Catalog= _ ;Integrated Security=False;  
User ID=      ;Password=      !;Encrypt=True;TrustServerCertificate=True"  
    }  
},
```

2. Fill out the required parameters and add the following properties object within your source object in the specification file.

JSON

```
"Properties":  
{  
    "ConnectionString": "Data Source={SQL Azure VM Public IP};Initial  
Catalog={Database Name};Integrated Security=False;User ID={SQL Login  
Username};Password={SQL Login  
Password};Encrypt=True;TrustServerCertificate=True"  
}
```

After you apply the changes, the migration specification looks like the following example.

```
import.json - Untitled (Workspace) - Visual Studio Code
File Edit Selection View Go Debug Tasks Help
import.json x
1 [
2   "Source": {
3     "Properties": {
4       "ConnectionString": "Data Source=8.8.8.8;Initial Catalog= ;Integrated Security=False;
5         User ID= ;Password= ;Encrypt=True;TrustServerCertificate=True"
6     }
7   },
8   "Target": {
9     "Name": "example-import"
10 },
11   "Properties": {
12     "ImportType": "DryRun"
13   },
14   "ValidationData": {
15     "TfsMigratorVersion": " example ",
16     "SourceCollectionId": " example ", 
17     "DataImportCollectionId": " example ", 
18     "DatabaseCollation": " example ", 
19     "CommandExecutionCount": 0,
20     "CommandExecutionTime": 0.0,
21     "TfsVersion": " example ",
22     "DatabaseTotalSize": 181,
23     "DatabaseBlobSize": 0,
24     "DatabaseTableSize": 181,
25     "DatabaseLargestTableSize": 8,
26     "ActiveUserCount": 8,
27     "TenantId": " example ", 
28     "Region": "CUS",
29     "ValidationChecksumVersion": 1,
30     "ValidationChecksum": example "
31   },
32   "Identities": [
33     example
34   ]
35 ]
```

Ln 1, Col 1 Spaces: 2 UTF-8 CRLF JSON ☺

Your migration specification is now configured to use a SQL Azure VM for migration. Proceed with the rest of preparation steps to migration to Azure DevOps Services. After the migration finishes, be sure to delete the SQL sign-in or rotate the password. Microsoft doesn't retain the sign-in information after the migration finished.

## Step 3: Upload the DACPAC file

### ! Note

If you're using the SQL Azure VM method, you need to provide only the connection string. You don't have to upload any files, and you can skip this step.

Your DACPAC must be placed in an Azure storage container, which can be an existing container or one created specifically for your migration effort. It's important to ensure that your container is created in the right geographical locations.

Azure DevOps Services is available in multiple [geographical locations](#). When you're importing to these locations, it's critical to place your data correctly to ensure that the migration can start successfully. Your data must be placed in the same geographical location that you're importing to. Placing the data anywhere else results in the migration being unable to start. The following table lists the acceptable geographical locations for creating your storage account and uploading your data.

[+] [Expand table](#)

Desired migration geographical location	Storage account geographical location
Central United States	Central United States
Western Europe	Western Europe
United Kingdom	United Kingdom South
Australia East	Australia East
Brazil South	Brazil South
India South	India South
Canada Central	Canada Central
Asia Pacific (Singapore)	Asia Pacific (Singapore)

Although Azure DevOps Services is available in multiple geographical locations in the US, only the Central United States location accepts new Azure DevOps Services. You can't migrate your data into other US Azure locations at this time.

[Create a blob container](#) from the Azure portal. After you create the container, upload the Collection DACPAC file.

After the migration finishes, delete the blob container and accompanying storage account with tools such as [AzCopy](#) or any other Azure storage explorer tool.

! **Note**

If your DACPAC file is larger than 10 GB, we recommend that you use [AzCopy](#), as it has multithreaded upload support for faster uploads.

## Step 4: Generate an SAS token

A [shared access signature \(SAS\) token](#) provides delegated access to resources in a storage account. The token allows you to give Microsoft the lowest level of privilege required to access your data for executing the migration.

You can generate SAS tokens [using the Azure portal](#). From a security point-of-view, we recommend doing the following tasks:

1. Select only **Read** and **List** as permissions for your SAS token. No other permissions are required.
2. Set an expiry time no further than seven days into the future.
3. [Restrict access to Azure DevOps Services IPs only](#).
4. Treat the SAS key as a secret. Don't leave the key in an insecure location as it grants read and list access to any data stored in the container.

## Step 5: Complete the migration specification

Earlier in the process you partially filled out the migration specification file, known as *migration.json*. At this point, you have enough information to complete all the remaining fields except for the migration type. The migration type is covered later, in the migration section.

In the *migration.json* specification file, under **Source**, complete the following fields.

- **Location:** Paste the SAS key you generated from the script and then copied in the preceding step.
- **Dacpac:** Ensure that the file, including the *.dacpac* file extension, has the same name as the DACPAC file you uploaded to the storage account.

The final migration specification file should look like the following example.

```
import.json - Untitled (Workspace) - Visual Studio Code
File Edit Selection View Go Debug Tasks Help
import.json x
{
  "Source": {
    "Location": "https://fabrikam.blob.core.windows.net/fabrikam",
    "Files": {
      "Dacpac": "Tfs_DefaultCollection.dacpac"
    }
  },
  "Target": {
    "Name": "fabrikam-import"
  },
  "Properties": {
    "ImportType": "<Provide the Type of Import: DryRun, ProductionRun>"
  },
  "ValidationData": {
    "TfsMigratorVersion": "16.255.65000 a",
    "SourceCollectionId": "example",
    "DataImportCollectionId": "example",
    "DatabaseCollation": "example",
    "CommandExecutionCount": 0,
    "CommandExecutionTime": 0.0,
    "TfsVersion": "example",
    "DatabaseTotalSize": 181,
    "DatabaseBlobSize": 0,
    "DatabaseTableSize": 181,
    "DatabaseLargestTableSize": 8,
    "ActiveUserCount": 8,
    "TenantId": "example",
    "Region": "CUS",
    "ValidationChecksumVersion": 1,
    "ValidationChecksum": "example"
  },
  "Identities": {
    "example"
  }
}
Ln 1, Col 1  Spaces: 2  UTF-8  CRLF  JSON  ☺
```

## Determine the migration type

Imports can be queued as either a test run (`DryRun`) or a production run (`ProductionRun`). The `ImportType` parameter determines the migration type:

- **DryRun:** Also referred to as a test run. Use for test and validation purposes. The system deletes test runs after 45 days.
- **ProductionRun:** Use a production run when you want to keep the resulting migration and use the organization full time in Azure DevOps Services after the migration finishes.

### 💡 Tip

We always recommend that you complete a test run migration first.

## Test run organizations

Test run organizations help teams test the migration of their collections. Before a production migration can be run, any completed [test run organizations must be deleted](#). All test run organizations have a *limited existence and are automatically deleted after a set period of time*. Information about when the organization is deleted is included in the success email you should receive after the migration finishes. Be sure to take note of this date and plan accordingly.

Test run organizations have 45 days before they're deleted. After the specified time period, the test run organization is deleted. You can repeat test run imports as many times as you need before you do a production migration.

## Delete test runs

Delete any previous test runs before you attempt a new one. When your team is ready to perform a production migration, you need to manually delete the test run organization. Before you can run a second test run migration or the final production migration, make sure you delete any previous Azure DevOps Services organizations that you created in a previous test run. For more information, see [Delete organization](#).

### Tip

Optional information to help a user be more successfulAny test run migration that follows the first is expected to take longer given the extra time required to clean up resources from previous test runs.

It can take up to one hour for an organization name to become available after deleting or renaming. For more information, see the [Post migration tasks](#) article.

If you encounter any migration problems, see [Troubleshoot migration and migration errors](#).

## Run a migration

Your team is now ready to begin the process of running a migration. We recommend that you start with a successful test run migration before you attempt a production-run migration. With test run imports, you can see in advance how a migration looks, identify potential issues, and gain experience before you head into your production run.

## Note

- If you need to repeat a completed production-run migration for a collection, such as due to a rollback, contact Azure DevOps Services [Customer Support](#) before you queue another migration.

- Azure administrators can prevent users from creating new Azure DevOps organizations. If the Microsoft Entra tenant policy is turned on, your migration fails to finish. Before you begin, verify that the policy isn't set or that there's an exception for the user that is performing the migration. For more information, see [Restrict organization creation via Microsoft Entra tenant policy](#).
- Azure DevOps Services doesn't support per-pipeline retention policies, and they aren't carried over to the hosted version.

## Considerations for rollback plans

A common concern for teams doing a final production run is their rollback plan, if anything goes wrong with migration. We highly recommend doing a test run to make sure that you can test the migration settings you provide to the Data Migration Tool for Azure DevOps.

Rollback for the final production run is fairly simple. Before you queue the migration, detach the team project collection from Azure DevOps Server, which makes it unavailable to your team members. If for any reason you need to roll back the production run and bring the on-premises server back online for your team members, you can do so. Attach the team project collection on-premises again and inform your team that they continue to work normally while your team regroups to understand any potential failures.

You can then contact Azure DevOps Services customer support for help with understanding the failure's cause if you can't determine the cause. For more information, see the [Troubleshooting article](#). Customer support tickets can be opened from the following page <https://aka.ms/AzureDevOpsImportSupport>. If the issue requires product group engineers to engage, those cases get handled during regular business hours.

## Detach your team project collection from Azure DevOps Server to prepare it for migration.

Before you generate a backup of your SQL database, you must completely detach the collection from Azure DevOps Server (not SQL) using the Data Migration Tool. The detach process in Azure DevOps Server transfers user identity information stored outside of the

collection database, making it portable for moving to a new server or, in this case, to Azure DevOps Services.

Detaching a collection is easily done from the Azure DevOps Server Administration Console on your Azure DevOps Server instance. For more information, see [Move project collection, Detach the collection](#).

## Queue the migration

### Important

Before you proceed, ensure that your collection was [detached](#) before you generate a DACPAC file or upload the collection database to a SQL Azure VM. If you don't complete this step, the migration fails. If your migration fails, see [Resolve migration errors](#).

Start a migration by using the Data Migration Tool's **import** command. The import command takes a migration specification file as input. It parses the file to ensure that the provided values are valid and, if successful, it queues a migration to Azure DevOps Services. The import command requires an internet connection, but doesn't\* require a connection to your Azure DevOps Server instance.

To get started, open a Command Prompt window, and change directories to the path to the Data Migration Tool. We recommended that you review the help text provided with the tool. Run the following command to see the guidance and help for the import command:

```
cmdline
```

```
Migrator import /help
```

The command to queue a migration has the following structure:

```
cmdline
```

```
Migrator import /importFile:{location of migration specification file}
```

The following example shows a completed import command:

```
cmdline
```

```
Migrator import /importFile:C:\DataMigrationToolFiles\migration.json
```

After the validation passes, sign in to Microsoft Entra ID with an identity that's a member of the same Microsoft Entra tenant as the identity map log file was built against. The signed in user is the owner of the imported organization.

 **Note**

Each Microsoft Entra tenant is limited to five imports per 24-hour period. Only imports that are queued count against this cap.

When your team initiates a migration, an email notification is sent to the user that queued the migration. About 5 to 10 minutes after it queues the migration, your team can go to the organization to check on the status. After the migration finishes, your team is directed to sign in, and an email notification is sent to the organization owner.

The Data Migration Tool flags errors that you need to correct before migration. This article describes the most common warnings and errors that you might receive when you're preparing to migrate. After you correct each error, run the **migrator validate** command again to verify resolution.

## Next steps

[Resolve migration errors](#)

## Related articles

- [Migration overview](#)
- [Post migration tasks](#)

 **Note:** The author created this article with assistance from AI. [Learn more](#)

# Migrate to Azure DevOps Services

Article • 05/20/2024

You completed the [Test run](#) phase and familiarized yourself with the process. Now, it's time to embark on the actual journey of migrating to Azure DevOps Services.



## Prerequisites

Ensure your test runs result in zero errors before you officially migrate to Azure DevOps Services.

## Queue the migration

Do the following steps to queue the migration with the Data Migration Tool.

1. Ensure the migration specification file is complete.
2. Use the following command to queue the migration: `Migration /importFile:C:\TFSDataImportFiles\import.json`.
  - Ownership: The user who queued the migration owns the migrated organization.
  - Notifications: The owner receives an email for migration success or [failure](#).

## Next steps

[Complete post-migration tasks](#)

## Related articles

- [Validate and prepare for migration](#)
- [Prepare for test run](#)
- [Do test run migration](#)

---

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# Complete post migration tasks

Article • 05/20/2024

When migration completes, an email gets sent to the organization owner and at this point, anyone with access can sign in to the newly migrated Azure DevOps Services organization. But, before you make the organization available to all users, you should complete the common tasks listed within this article.



## Spot check

Immediately after the organization becomes available, take a small team and do spot checks on the organization. We recommend that this team consists of the project collection administrators. This check shouldn't be in-depth, but rather making sure that major pieces from your collection were brought over.

- **Source code:** Verify that your source code repositories migrated correctly.
- **Build history:** Ensure your build history made it over.
- **Area paths:** Confirm that all area paths are still present.

These quick checks help you catch any missing or incomplete data before opening the organization to your entire user base.

## Rename organization (optional)

In the [Get started phase](#), you might have already created organizations with the final Azure DevOps Services organization names that you want to use. If this is your final migration, you can rename your newly migrated Azure DevOps Services organization to that desired name. For more information, see [Rename your organization](#).

## Set up billing

To pay for users or services in Azure DevOps, like hosted build and deployment agents, you need to set up billing for your organization. If you migrate more than one collection, you should ensure all your organizations are set up for billing with the same Azure subscription, and that your subscription is enabled for [multi-organization billing](#). You can then assign as many Basic users as you need free of charge during the calendar month in which you run the migration.

# Configure build agents

If you used automated build or deployment servers in your Azure DevOps Server environment, you can connect them to your Azure DevOps Services organization. As part of the migration, all your build definitions got migrated, but you must reconfigure agents and pools against your new Azure DevOps Services organization.

For more information, see [Azure Pipelines agents](#).

If you plan to use your existing on-premises private build agents, you must clear their cache, which ensures that you don't encounter any build issues related to older Team Foundation Version Control (TFVC) or Git pointers to your on-premises collection. For more information, see [refreshing caches on client computers](#).

## Tip

If you used Release Management in Azure DevOps Server, then your release pipelines and history data migrated. But like with builds, you must reconfigure your agents(link again) and pools against the new organization.

# Use Azure Artifacts

Azure Artifacts is included with Azure DevOps Services for all users granted a Basic license. There's no need to install an extension. Your Azure Artifacts data should be available post migration. For more information, see [Azure Artifacts overview](#).

# Customize Azure Boards

If you have an existing GitHub Enterprise Server connection associated with your Azure DevOps Server, it doesn't work as expected. Work items mentioned within GitHub might be delayed or never show up in Azure DevOps Services. This problem occurs because the callback URL associated with GitHub is no longer valid.

To resolve the problem, consider the following tasks:

- **Remove and re-create the connection:** Remove and re-create the connection to the GitHub Enterprise Server repository. Follow the sequence of steps provided in [Connect from Azure Boards documentation](#).
- **Fix the webhook URL:** Go to GitHub's repository settings page and edit the webhook URL to point to the migrated Azure DevOps Services organization URL:

[https://dev.azure.com/{OrganizationName}/\\_apis/work/events?api-version=5.2-preview](https://dev.azure.com/{OrganizationName}/_apis/work/events?api-version=5.2-preview).

For more information, see [Configure and customize Azure Boards](#).

## Review permissions

Your organization includes five free users with [Basic](#) access. For more information, see [Add organization users and manage access](#).

## Notify your teams

After your builds are running and license subscription is configured, we recommend that you open the organization to all users for validation. Then individual users can ensure that all the content is in place, has the right access level, and they can pull code.

Users of TFVC with local workspaces must remap their workspaces against the new organization, and Git users must reconfigure their remotes to pull code.

If anything is missing from the migrated organization, [contact Support](#).

## Next steps

[Get Azure DevOps Services extensions \(optional\)](#)

## Related articles

- [Validate and prepare for migration](#)
- [Prepare for test run](#)
- [Do test run migration](#)
- [Migrate to Azure DevOps Services](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Resolve migration errors

Article • 12/26/2024

The Data Migration Tool flags errors that you need to correct before you import to Azure DevOps Services. This article describes the most common warnings and errors that you might receive when you're preparing to import. After you correct each error, run the **migrator validate** command again to verify resolution.

For more help, refer to the [FAQs section](#) at the end of this article.

## Resolve size warnings

Extra-large collections might generate one of the following messages after running the Data Migration Tool. If you receive any of these warnings or errors, we recommend that you try to [reduce your database's size](#).

### Database size over recommended size

The following warning means you need to use the SQL Azure VM method to complete your migration. Once a database reaches a certain size, it becomes faster to set up a SQL Azure VM to complete the migration to Azure DevOps Services. To set up the VM and complete your migration, follow the instructions linked from the warning message.

cmdline

The database is currently {Database Size}GBs. This is above the recommended size of {DACPAC Size Limit}GBs to use the DACPAC migration method. Please see the following page to learn how to migration using a SQL Azure VM:  
<https://aka.ms/AzureDevOpsImportLargeCollection>

This warning **DOES NOT** mean that your collection is too large for migration.

### Table size over recommended size

Similar to the previous warning, the following warning means you must use the SQL Azure Virtual Machine (VM) method to complete the migration. To set up the VM and complete your migration, follow the instructions linked from the warning message.

cmdline

The largest table size is currently {Table size}GBs. This is above the recommended size of {Size limit}GBs to use the DACPAC migration method.

Please see the following page to learn how to migration using a SQL Azure VM: <https://aka.ms/AzureDevOpsImportLargeCollection>

This warning **DOES NOT** mean that your collection is too large for migration.

## Database metadata size over recommended size

The following warning means that your database is approaching the limit for total metadata size. Metadata size refers to the size of your database without including files, code, and other binary data. We recommend that you [reduce the size](#) of your database before migration. Reducing the size provides the other benefit of speeding up your migration.

cmdline

The database metadata size is currently {Metadata Size}GBs. This is above the recommended size of {Warning Size}GBs. It's recommended that you consider cleaning up older data as described in [Cleaning up old data] (/azure/devops/server/upgrade/clean-up-data).

The warning **DOES NOT** mean that your collection is too large for migration, rather its metadata size is larger than most other databases.

## Database metadata size over maximum supported size

Unlike the previous warnings, the following error **WILL** block you from moving forward with your migration.

It indicates that the volume of metadata in your collection is too large. To proceed with the migration, you need to [reduce](#) the size below the indicated limit.

cmdline

The database metadata size is currently {Metadata Size}GBs. This is above the maximum supported size of {Metadata Limit}GBs.

## Resolve collation warnings

Collation warnings refer to your collection database's collation. Collations control the way string values are sorted and compared. Collections that aren't using either `SQL_Latin1_General_CI_AS` or `Latin1_General_CI_AS` receive one of the **warning** messages.

## No native support

Receiving the following warning means that you need to consider collation implications before performing the migration.

cmdline

```
The collection database's collation '{collation}' is not natively supported  
in Azure DevOps Services. Importing your collection will result in your  
collation being converted to one of the supported Azure DevOps Services  
collations. See more details at https://aka.ms/AzureDevOpsImportCollations
```

This warning **DOES NOT** mean that you can't migrate your collection.

This warning requires you to acknowledge acceptance of the warning. Accepting the warning allows the Data Migration Tool to continue migration preparations.

When you migrate an unsupported collation into Azure DevOps Services, the collation is transformed to a supported collation. While this transform generally works without issue, unexpected results post migration or migration failures could occur.

For instance, customers might notice different ordering for strings containing non-English characters. Non-English characters like 'é' might become equivalent to the English 'e' after migration. It's important that you complete and verify a test run migration when you migrate a collection with an unsupported collation.

## No native support, no internet connection

If the Data Migration Tool can't connect to the internet, it can't validate conversion of your collation. It's only a warning, so you can continue with your migration process. However, when you run the **prepare** command, an internet connection is required and collation conversion is validated at that time.

cmdline

```
The collections database's collation '{collation}' is not natively supported  
in Azure DevOps Services. It could not be validated that the collation can  
be converted during migration to a supported Azure DevOps Services  
collation, as there was no internet connection. Please run the command again  
from a machine with an internet connection. See more details at  
https://aka.ms/AzureDevOpsImportCollations
```

## Unsupported database collation

Generally you can convert a nonsupported collation to a supported collation at migration time. However, some collations can't be converted. If your collection uses one of these collations, you receive the following **error** message.

#### cmdline

```
The collection database's collation '{collation}' is not supported for  
migration to Azure DevOps Services. It will need to be changed to a  
supported collation before it can be imported. See more details at  
https://aka.ms/AzureDevOpsImportCollations
```

In order to continue, you need to [change your collection's collation](#) to one of the supported collations on Azure DevOps Services.

## Resolve identity errors

Fix identity errors before migration to prevent problems. These errors are rare and occur when old operations are invalid on a new Azure DevOps Server. For instance, some users might no longer be part of the valid users group.

The following sections provide guidance for resolving the most common identity errors.

### ISVError: 100014

This error indicates that a permission is missing from a system security group. For example, every collection that you create has Project Collection Valid Users and Project Collection Administrators groups. The system creates them by default. These groups don't support editing of their permissions.

This error indicates that one or more groups is missing a permission that it should have. To resolve this error, use the [TFSSecurity.exe](#) command to apply the expected permissions onto the flagged system groups. Your first step is to identify which [TFSSecurity](#) command you need to run.

### Project Collection Valid Users error message

Examine one or more error messages the Data Migration Tool highlighted. If the flagged group ends with "0-0-0-0-3", such as in the following example, you need to fix a missing permission for the **Project Collection Valid Users** group.

Run the following command, replace the scope with the one from the error message and specify your collection URL.

```
cmdline
```

```
TFSSecurity.exe /a+ Identity "{scope}\" Read sid:{Group SID} ALLOW  
/collection:{collectionUrl}
```

You determine the scope and group security ID (SID) from the error message.

```
cmdline
```

```
ISVError:100014 Missing permission for  
group:Microsoft.TeamFoundation.Identity;S-1-9-XXXXXXXXXX-XXXXXXX-  
XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-3 for scope:397c326b-b97c-4510-8271-  
75aac13de7a9. Expected:1 and Actual:0
```

The final command appears similar to the following entry:

```
cmdline
```

```
TFSSecurity.exe /a+ Identity "397c326b-b97c-4510-8271-75aac13de7a9\" Read  
sid:S-1-9-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-3 ALLOW  
/collection:https://localhost:8080/defaultcollection
```

## Project Collection Administrators error message

Carefully examine the error messages the Data Migration Tool highlighted. If the flagged group that ends with "0-0-0-0-1", such as in the following example, then you need to fix a missing permission for the **Project Collection Administrators** group. Run the following commands against **TFSSecurity.exe**, replace the scope with the one from the error message and specify your collection.

```
cmdline
```

```
TFSSecurity.exe /a+ Identity "{scope}\" Read sid:{Group SID} ALLOW  
/collection:{collectionUrl}
```

```
TFSSecurity.exe /a+ Identity "{scope}\" Write sid:{Group SID} ALLOW  
/collection:{collectionUrl}
```

```
TFSSecurity.exe /a+ Identity "{scope}\" Delete sid:{Group SID} ALLOW  
/collection:{collectionUrl}
```

```
TFSSecurity.exe /a+ Identity "{scope}\" ManageMembership sid:{Group SID}  
ALLOW /collection:{collectionUrl}
```

In the following example, take the scope and group **SID** from the error message and add them to the preceding command.

cmdline

```
ISVError:100014 Missing permission for  
group:Microsoft.TeamFoundation.Identity;S-1-9-XXXXXXXXXX-XXXXXXX-  
XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-1 for scope:0c7c2216-fa4b-4107-a203-  
82b324a147ef. Expected:15 and Actual:0
```

The final command appears similar to the following entry:

cmdline

```
TFSSecurity.exe /a+ Identity "0c7c2216-fa4b-4107-a203-82b324a147ef\\\" Read  
sid:S-1-9-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-1 ALLOW  
/collection:https://localhost:8080/defaultcollection

TFSSecurity.exe /a+ Identity "0c7c2216-fa4b-4107-a203-82b324a147ef\\\" Write  
sid:S-1-9-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-1 ALLOW  
/collection:https://localhost:8080/defaultcollection

TFSSecurity.exe /a+ Identity "0c7c2216-fa4b-4107-a203-82b324a147ef\\\" Delete  
sid:S-1-9-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-0-0-0-0-1 ALLOW  
/collection:https://localhost:8080/defaultcollection

TFSSecurity.exe /a+ Identity "0c7c2216-fa4b-4107-a203-82b324a147ef\\\"  
ManageMembership sid:S-1-9-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-0-0-  
0-0-1 ALLOW /collection:https://localhost:8080/defaultcollection
```

When you need to correct multiple errors, we recommend that you create a batch file to automate execution of the commands. Once you execute the commands, rerun the data migration **validate** tool to verify resolution. If some errors still persist, contact [Azure DevOps Services customer support](#).

## ISVError: 300005

ISVError: 300005 indicates that a nongroup identity is a member of an everyone group, more commonly known as the Valid Users groups. Valid Users groups are default groups defined for all projects and collections. These groups aren't editable. They're designed to only contain other Azure DevOps permission or security groups as members. This error indicates that an Active Directory (AD) group or user identity has a direct membership in a Valid Users group.

 **Important**

Ensure that you have a backup of your collection and configuration databases before running the following commands to resolve the error.

Since you can't directly edit Valid Users groups, you need to run a SQL statement against the configuration database to remove the offending identity and correct the invalid membership. Carefully examine the error messages highlighted by the Data Migration Tool. Copy the `GroupSid`, `MemberId`, and `ScopeId` as you need to place these values into the following command.

SQL

```
DECLARE @p6 dbo.typ_GroupMembershipTable

INSERT into @p6
values('{GroupSid}', 'Microsoft.TeamFoundation.Identity', '{MemberId}', 0)

EXEC prc_UpdateGroupMembership
@partitionId=1,@scopeId='{ScopeId}',@idempotent=1,@incremental=1,@insertInactiveUpdates=0,@updates=@p6,@eventAuthor='9EE20697-5343-43FC-8FC5-3D5D455D21C5',@updateGroupAudit=0
```

The following example lists an example of an ISVError: 300005 message from the Data Migration Tool.

cmdline

```
ISVError:300005 Unexpected non group identity was found to have direct membership to everyone group. GroupSid:S-1-9-1551374245-3746625149-2333054533-2458719197-2313548623-0-0-0-3, MemberId:76050ddf-4fd8-48c4-a1ff-859e44364519, ScopeId:7df650df-0f8b-4596-928d-13dd89e5f34f
```

If the error message lists a `MemberSid`, you need to get the `MemberID` from the `dbo.tbl_Identity` table in the configuration database. With the `MemberID`, you can then look up the GUID for the `MemberSid`.

cmdline

```
ISVError:300005 Unexpected non group identity was found to have direct membership to everyone group. GroupSid:S-1-9-1551374245-3746625149-2333054533-2458719197-2313548623-0-0-0-3,
MemberSid:System.Security.Principal.WindowsIdentity;S-1-5-21-124525095-708259637-1543119021-1737349, ScopeId:7df650df-0f8b-4596-928d-13dd89e5f34f
```

SQL

```
DECLARE @MemberId uniqueidentifier

SET @MemberId = (Select Id from dbo.tbl_Identity where Sid ='S-1-5-21-
124525095-708259637-1543119021-1737349');

SELECT @MemberId
```

Copy the `GroupSid`, `MemberId`, and `ScopeId` into the SQL command.

SQL

```
DECLARE @p6 dbo.typ_GroupMembershipTable

INSERT into @p6 values('S-1-9-1551374245-3746625149-2333054533-2458719197-
2313548623-0-0-0-0-3','Microsoft.TeamFoundation.Identity','76050ddf-4fd8-
48c4-a1ff-859e44364519',0)

EXEC prc_UpdateGroupMembership @partitionId=1,@scopeId='7df650df-0f8b-4596-
928d-
13dd89e5f34f',@idempotent=1,@incremental=1,@insertInactiveUpdates=0,@updates
=@p6,@eventAuthor='9EE20697-5343-43FC-8FC5-3D5D455D21C5'
```

Run the completed command against the Azure DevOps Server configuration database. Repeat this command for each ISVError: 300005 instance reported. You can batch errors with the same scope ID into a single command. Once you execute the commands, rerun the Data Migration Tool validate again to ensure that the errors are corrected. If the errors still persist, contact [Azure DevOps Services customer support](#).

### ⓘ Important

To address these errors, the collection must be attached.

If you receive a -1 result when you run the command, ensure that your collection database that produced the error is attached to your Azure DevOps Server instance and that you're running the command on the configuration database.

## Microsoft Entra timeout exception

On rare occasions, you might receive a Microsoft Entra timeout error when running the Data Migration Tool prepare command.

cmdline

Exception Message: Request failed (type AadGraphTimeoutException)

This error means that the requests to Microsoft Entra ID to find the matching Microsoft Entra identities for users in your collection timed out. Generally, you can resolve this error by waiting to run the **prepare** command at a less busy time of the day, such as after regular business hours.

To troubleshoot, test Microsoft Entra ID connection from **prepare** machine. Follow these steps to get user info from Microsoft Entra ID.

Open PowerShell in elevated mode and replace 'someone@somecompany.com' in the following command with your Microsoft Entra user identity.

PowerShell

```
# Install the Microsoft Graph PowerShell module - ensuring to select Yes to All
Install-Module Microsoft.Graph

# Import Users module
Import-Module Microsoft.Graph.Users

# Connect to Microsoft Entra and use your Microsoft Entra ID credentials (someone@somecompany.com) to login when the pop-up appears
Connect-MgGraph -Scopes 'User.Read.All'

# Try to retrieve information on a user from your Microsoft Entra
Get-MgUser -Filter "UserPrincipalName eq 'someone@somecompany.com'"
```

If the steps fail or you can't find the user, check the connection between the **prepare** machine and Microsoft Entra ID. Run a network trace with **prepare** to see if the network blocks calls. If not, contact Azure support. Check the log file for the user information.

cmdline

Number of active users is {Number of Users}.

If the number of active users is over 50,000, the volume of identities being mapped might require more time than provided by the timeout limit. Inspect your collection for inclusions of large groups such as an 'everyone' group. If possible, remove these groups and try again. If you still can't resolve this error, contact [Azure DevOps Services customer support](#).

## Resolve process errors

See the [Validate phase article, Resolve process templates](#) for details on resolving common process errors.

## Resolve field validation errors

### VS403310

The following error message can occur when an inconsistency in collection files is detected. Contact customer support if you encounter this error.

```
VS403310: An inconsistency was detected in some of the files in the collection.
```

### VS403442

Field name conflicts sometimes occur between your local collection and an Azure DevOps Services system field.

```
In order to migrate successfully, you must rename field *{TFSfieldReferenceName}*.
```

```
Given name *{TFSfieldName}* is reserved for field *{VSTSfieldReferenceName}*.
```

To resolve this error, change the name of your collection field. Use the `witadmin changefield` command from [witadmin](#).

```
cmdline
```

```
witadmin changefield  
/collection:http://AdventureWorksServer:8080/DefaultCollection  
/n:TFSfieldReferenceName /name:newFieldName
```

### VS403443

The following error indicates a field name conflict exists between your local collection and a specific Azure DevOps Services field.

```
In order to migrate successfully, you must rename field *{TFSfieldReferenceName}*  
to *{VSTSfieldName}*.  
Given name for *{TFSfieldReferenceName}* is *{TFSfieldName}*
```

To resolve this error, use the `witadmin changefield` command. For details, see [witadmin](#).

```
cmdline
```

```
witadmin changefield  
/collection:http://AdventureWorksServer:8080/DefaultCollection  
/n:TFSfieldName /name:VSTSfieldName
```

## VS403444

The following error indicates a field type conflict exists between your local collection and Azure DevOps Services.

Using [witadmin](#), you can change the data type only for HTML or PlainText fields.

```
In order to migrate successfully, you must set type of field *  
{TFSfieldName}* to *{Type}*. Given type for *{TFSfieldName}* is *  
{collectionType}*. 
```

If your field type is HTML or PlainText, then you can change its type to the required type.

cmdline

```
witadmin changefield  
/collection:http://AdventureWorksServer:8080/DefaultCollection  
/n:TFSfieldName /type:PlainText | HTML
```

### ⓘ Note

If your field type is something different than HTML or PlainText and field data isn't important or the field isn't used in any project, then we recommend you delete the field.

cmdline

```
witadmin deletefield  
/collection:http://AdventureWorksServer:8080/DefaultCollection  
/n:TFSfieldName
```

### ⓘ Important

Deleting a field results in a loss of field data across the collection.

## Resolve verification failures

Verification failures mean the migration didn't start. The Data Migration Tool attempted to queue a migration, but got an error instead. Your migration request isn't valid. Fix the error messages and then try to migrate again.

## VS403254

The region that you entered for your Azure DevOps Services migration isn't supported.

```
VS403254: Region {0} might not be used for the Import, it is not a supported  
region.
```

Open your migration specification file and update the region that you provided with the correct short name for the [region](#).

## VS403249

The organization name your team selected is already in use by an existing organization. All Azure DevOps Services migrations go into a new organization that is created at migration time.

```
VS403249: The organization {0} already exists. Please select a different name and  
try the migration again.
```

Select a different organization name and update the migration specification file before retrying the migration.

## VS403250 & VS403286

The DACPAC isn't built off a detached collection.

```
VS403250: The dacpac is not a detached Azure DevOps Server Collection database.
```

```
VS403286: The dacpac is from a Azure DevOps Server Configuration database. You must  
use a detached Azure DevOps Server Collection database.
```

[Detach](#) your collection database and generate the DACPAC again.

## VS403243

Unable to make a connection to the database using the provided SQL Connection String.

`VS403243: Unable to connect to the database using the provided SQL Connection String {0}.`

Review the parameters that were provided to ensure they're correct and try again.

## VS403260 & VS403351

The collection database isn't detached.

`VS403260: The database is not detached.`

`VS403351: The DACPAC or source database is missing an expected table. It's possible that the database was not correctly detached from Azure DevOps Server.`

[Detach](#) your collection database and retry the migration queue.

## VS403261

The connection string must be encrypted otherwise the password is sent in the clear.

`VS403261: The SQL connection string must use encryption.`

Add `Encrypt=true` to your SQL connection string.

## VS403262

The connection string must use SQL Authentication.

`VS403262: The SQL connection string must use SQL Authentication, Integrated Authentication is not supported.`

Add `Integrated Security=False` to your SQL connection string.

## VS403263

Your SQL sign in user account doesn't have the required database role.

`VS403263: The User ID {0} must be member of the database role {1}.`

Make sure the user account for sign in is assigned the '['TFSEXECROLE'](#)' role.

### Note

There is a known issue with using `sp_addrolemember` to add `TFSEXECROLE` to an existing SQL login. The role membership isn't applied until all open connections using that identity are closed. If you receive the VS403263 error and have confirmed your identity has the role, we recommend that you create a new identity for your migration.

## VS403264

The connection string doesn't point to an Azure DevOps Server collection database.

`VS403264: The database is not a Azure DevOps Server Collection database, it cannot be used for migration.`

Verify or correct the connection string points to your collection database.

## VS40325

The Azure DevOps Server Update has queued the file migration job. You can't perform migrations until this job completes. The completion time for this job is dependent on the size of the collection.

`VS403255: The collection cannot be imported due to an ongoing post upgrade job.`  
`Please wait and try again later`

You can track job progress by running the following query on the collection database:

SQL

```
SELECT COUNT (*) as remaining_files_to_migrate
FROM   tbl_FileReference
WHERE  PartitionId > 0
      AND MigrateFileDialog IS NOT NULL
```

Once the number of files remaining to migrate is zero, you can run the Data Migration Tool.

## VS403282

A new line character exists in the source location value. This character might remain after copying the SAS key from your windows console.

VS403282: The source location parameter contains a new line character. Please ensure the SAS key is defined on a single line in the migration specification file.

Remove the line break and try again.

## VS403271

Your migration files and DACPAC aren't located in the **required** Azure region to complete the migration to your target Azure DevOps Services region.

VS403271: It appears that your DACPAC was uploaded to East US. It's required that customers targeting Central US for migration put their DACPACs in Central US. Please move your DACPAC to Central US and requeue the migration.

Create a new Microsoft Azure storage account in the required region and copy your files. The following example shows how to copy your data using AzCopy.

cmdline

```
AzCopy.exe /Source:https://accountSCUS.blob.core.windows.net/mycontainer  
/SourceKey:"primary access key"  
/Dest:https://accountCUS.blob.core.windows.net/mycontainer /DestKey:"primary  
access key" /S
```

## VS403316

Inconsistencies were detected in some Team Foundation version control (TFVC) files within your collection.

VS403316: An inconsistency was detected in some TFVC files for this collection. The inconsistency needs to be corrected prior to running a migration to Azure DevOps Services. Please reach out to <https://aka.ms/AzureDevOpsImportSupport> for assistance with addressing this issue.

Work with Azure DevOps Services [customer support](#). Open a support ticket and they work with you to resolve the error.

## VS403366

The Data Migration Tool was unable to connect to the SQL Azure VM.

**VS403366:** A problem occurred while attempting to connect to your database. Please verify that your connection string is correct and that all required IP addresses for Azure DevOps Services have been provided exceptions for your machines firewall.

List of Azure DevOps Services IPs:

Verify that you entered the information correctly in your connection string and that you can connect to the VM.

The IPs that the error message lists are for Azure DevOps Services. Azure DevOps Services IPs can change temporarily during deployments. Add them to your firewall exceptions and try queuing the migration again. For a list of IP addresses, see [Migrate large collections, Restrict access to Azure DevOps Services IPs only](#).

## VS403373

The Data Migration Tool doesn't support migrating multiple copies of the **SAME** collection. However, it **DOES** support migrating **split** copies of a collection. Change the GUID for the ***DataImportCollectionID***.

From SQL Server Management Studio (SSMS), open the extended properties for the split copies that you didn't migrate yet. Add a newly generated GUID to the "TFS\_DATAIMPORT\_COLLECTIONID" property. Then rerun the **prepare** command and use the new **migration.json** file to queue the migration.

## VS403379

Data migration fails as one or more projects found in this collection are in the soft-deleted stage. Restore the soft-deleted projects or delete them permanently before running the data migration. For details, see [Delete a project](#).

**VS403379:** Data migration will fail as one or more projects found in this collection are in the soft-deleted stage. Please restore the soft-deleted project(s) or delete them permanently before running the data migration.

Verify the collection against which you're running the Data Migration Tool has projects in the soft-deleted stage. Once a project is deleted, it remains in a soft-delete state for 28 days during which the deleted project can be restored. You can read about how to restore a deleted project in [Restore a project](#). If you have projects in the soft-deleted stage, remove them completely or restore them back before running data migration.

# Resolve migration failures

Migration failures mean that the migration queued, but didn't complete. The individual who queued the migration receives a failure email notification. Most of the time this email includes a reason for the failure. If it does, use the troubleshooting steps provided in the email and this page to resolve the errors and retry your migration.

If the error is more complex, then the email you receive provides instructions on how to file a [customer support case](#). After you submit a customer support case, your team must roll back by bringing your Azure DevOps Server instance back online and reattach your collection. Your team members can then continue working. We recommended that you don't try the migration again until the failure causing the issue gets resolved.

## FAQs

### Q: What should I do if my migration was queued but failed and I didn't receive an email with next steps?

A: If your migration was queued but failed and you didn't receive an email notification, follow these steps:

- **Check migration logs:** Review the migration logs for any error messages that might indicate the cause of the failure. The logs can provide insights into what went wrong during the migration process.
- **Follow troubleshooting steps:** Refer to the troubleshooting steps outlined in this migration troubleshooting guide. These steps can help you identify and resolve common issues that perhaps caused the failure.
- **Contact Customer Support:** If the error is complex or you can't resolve the issue using the logs and troubleshooting steps, consider [filing a customer support case](#) for further assistance.
- **Rollback and retry:** If necessary, roll back your Azure DevOps Server instance and reattach the collection before attempting the migration again.

## Related articles

- [Complete post migration tasks](#)
- [Delete a project](#)

ⓘ Note: The author created this article with assistance from AI. [Learn more](#)

# Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

# Default permissions quick reference

Article • 01/09/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

To use Azure DevOps features, users must be added to a security group with the appropriate permissions and granted access to the web portal. Limitations to select features are based on the *access level* and *security group* to which a user is assigned. The **Basic** access level and higher supports full access to most Azure DevOps services, except for Azure Test Plans. **Stakeholder** access level provides partial support to Azure Boards and Azure Pipelines. To learn more about access levels, see [About access levels](#) and [Stakeholder access quick reference](#).

## Assign users to a security group

The most common built-in security groups—**Readers**, **Contributors**, and **Project Administrators**—and team administrator role grant permissions to specific features.

In general, use the following guidance when assigning users to a security group:

- Add to the **Contributors** security group full-time workers who contribute to the code base or manage projects.
- Add to the **Project Administrators** security group users tasked with managing project resources.
- Add to the **Project Collection Administrators** security group users tasked with managing organization or collection resources.

To learn more about administrative tasks see [About user, team, project, and organization-level settings](#). For a complete reference of all built-in groups and permissions, see [Permissions and groups](#). For information about access levels, see [About access levels](#).

In the tables provided in this article, a (checkmark) indicates that the corresponding access level or security group has access to a feature by default.

To assign or change an access level, see [Add users and assign licenses](#). If you need to [grant specific users select permissions](#), you can do so.

## Azure Boards

You can plan and track work from the web portal **Boards** hub, and using Visual Studio, Excel, and other clients. For an overview of work tracking features, see [About Agile tools](#). To change permissions, see [Set permissions and access for work tracking](#). In addition to the permissions set at the project level via the [built-in groups](#), you can set permissions for the following objects: [area and iteration paths](#) and individual [queries and query folders](#).

 **Note**

Team administrators can configure settings for their team's tools. Organization owners and members of the **Project Administrators** group can configure settings for all teams. To be added as an administrator, see [Add team administrators](#) or [Change project-level permissions](#).

Each user's access level or permission assignment controls access to the following tasks. Members of the Readers, Contributors, or Project Administrators group are assumed to have at least Basic access.

## General work item permissions

You can use work items to track anything you need to track. For more information, see [Understand how work items are used to track issues, tasks, and epics](#).

### Task or permission

Readers

Contributors

Project admins

---

### View work items in this node (Area Path permission)



### Edit work items in this node (Area Path permission)



**Edit work item comments in this node** (Area Path permission)



**Create tag definition**



**Change work item type** (Project-level permission)



**Move work items out of this project** (Project-level permission)



**Email work items**



**Apply a work item template**



**Delete and restore work items** (Project-level permission) (able to restore from the Recycle bin)



[Permanently delete work items](#) (Project-level permission)



[Provide feedback](#) (through the Microsoft Feedback client)



[Request feedback](#)



#### Note

Work items are subject to rules applied to them. Conditional rules based on user or group membership are cached for your web browser. If you find yourself restricted to update a work item, you may have encountered one of these rules. If you believe you've encountered an issue that doesn't apply to you, see [Work item form IndexDB caching issues](#). For more information, see [Rules and rule evaluation](#).

## Boards

You use **Boards** to implement Kanban/Agile methods. Boards present work items as cards and support quick status updates through drag-and-drop.

**Task**

**Readers**

**Contributors**

**Team admins**

**Project admins**

View boards and open work items



Add work items to a board; update status through drag-and-drop



Reorder work items or reparent child items through drag-and-drop; update a field on a card



Add child items to a checklist



Assign to a sprint (from card field)



Configure board settings



## Backlogs features access

**Backlogs** display work items as lists. A product backlog represents your project plan and a repository of all the information you need to track and share with your team. Portfolio backlogs allow you to group and organize your backlog into a hierarchy.

### Task

**Readers**

**Contributors**

**Team admins**

**Project admins**

View backlogs and open work items



Add work items to a backlog



Use bulk edit features



Add child items to a backlog item; prioritize or reorder a backlog; parent items using the Mapping pane; Assign items to a sprint using the Planning pane



Configure team settings, backlog levels, show bugs, work days off



## Sprints

You use sprint tools to implement Scrum methods. The **Sprints** set of tools provide filtered views of work items that a team has assigned to specific iteration paths or sprints.

## Task

### Readers

#### Contributors

##### Team admins Project admins

View sprint backlogs, taskboards, and open work items



Add work items to a sprint backlog or taskboard



Prioritize/reorder a sprint backlog or taskboard; add child items to a backlog item; reassign items to a sprint using the Planning pane



View team capacity and work details



Set team capacity



Use bulk edit features





Define team sprints



## Queries

[Queries](#) are filtered lists of work items based on criteria that you define by using a query editor. [Adhoc searches](#) are powered by a semantic search engine.

Task

Readers

Contributors

Project admins

---

View and run managed queries, view query charts



Create and save managed [My queries](#), query charts



Create, delete, and save [Shared queries](#), charts, folders



## Delivery plans

[Delivery plans](#) display work items as cards against a calendar view. This format can be an effective communication tool with managers, partners, and stakeholders for a team.

## Task

### Readers

### Contributors

### Team admins

### Project admins

View delivery plans



Create, edit, or delete a delivery plan, Contributors can only edit or delete plans that they create



Manage permissions for a delivery plan, Contributors can only manage permissions for plans that they create



## Azure Repos

You can manage your source code from the web portal **Repos** hub, or using Xcode, Eclipse, IntelliJ, Android Studio, Visual Studio, or Visual Studio Code.

Stakeholders for private projects have no access to **Repos**. Stakeholders for public projects have the same access to **Repos** as **Contributors**.

## Advanced Security

You can use [Advanced Security](#) to identify security vulnerabilities in your repository.

## Permission

Readers

Contributors

Build Admins

Project Admins

---

**View alerts** (ability to view all security alerts under the Advanced Security tab)



**Manage and dismiss alerts** (ability to dismiss any Advanced Security alert)



**Manage settings** (toggle on Advanced Security and/or enable push protection for a repository)

---

## Code: Source control

You can connect to your code from the web portal **Code** hub, or using Xcode, Eclipse, IntelliJ, Android Studio, Visual Studio, or Visual Studio Code. Stakeholders for private projects have no access to **Code**.

## Git

You can use [Git repositories](#) to host and collaborate on your source code. For an overview of code features and functions.

## Permission

Readers

**Contributors**

**Build Admins**

**Project Admins**

---

**Read** (clone, fetch, and explore the contents of a repository); also, can create, comment on, vote, and **Contribute to pull requests**



**Contribute, Create branches, Create tags, and Manage notes**



**Create repository, Delete repository, and Rename repository**



**Edit policies, Manage permissions, Remove others' locks**



**Bypass policies when completing pull requests, Bypass policies when pushing, Force push (rewrite history, delete branches and tags)**  
(not set for any security group)

---

## TFVC

[Team Foundation Version Control \(TFVC\)](#) provides a centralized version control system to manage your source control.

## Note

Tasks such as create, delete, or rename a TFVC repository are not supported. Once a TFVC repository is created you can't delete it. Also, you can only have one TFVC repository per project. This is different from Git repositories which allow for adding, renaming, and deleting multiple repositories.

## Permission

### Readers

### Contributors

### Build Admins

### Project Admins

**Check in, Label, Lock, Merge, Pend a change in a server workspace, Read**

Read only



**Administer labels, Manage branches, Manage permissions, Revise other users' changes, Undo other users' changes, Unlock other users' changes**



## Azure Pipelines

You can define and manage your builds and releases from the web portal **Pipelines** hub. For an overview of pipelines features and functions, see [Continuous integration on any platform](#).

 Expand table

Task	Readers	Contributors	Build Admins	Project Admins	Release Admins
View release pipelines	✓	✓	✓	✓	✓
Define builds with continuous integration	✓	✓	✓	✓	
Define releases and manage deployments	✓			✓	✓
Approve releases	✓	✓	✓	✓	✓
Azure Artifacts (5 users free)	✓			✓	✓
Queue builds, edit build quality	✓	✓	✓	✓	
Manage build queues and build qualities			✓	✓	
Manage build retention policies, delete and destroy builds	✓	✓	✓	✓	
Administer build permissions		✓		✓	
Manage release permissions				✓	✓
Create and edit task groups	✓	✓	✓	✓	✓
Manage task group permissions			✓	✓	✓
Can view library items such as variable groups	✓	✓	✓	✓	✓
Use and manage library items such as variable groups			✓	✓	✓

## Azure Test Plans

Users granted **Basic + Test Plans** or **Visual Studio Enterprise** access level can define and manage manual tests from the web portal. For an overview of manual test features and functions, see [Testing overview](#). You set several [test permissions](#) at the project level from **Project Settings>Permissions**.

### Permission

**Level**

**Readers**

**Contributors**

**Project Admins**

**View test runs**

Project-level



**Create test runs**

**Delete test runs**

Project-level



**Manage test configurations**

**Manage test environments**

Project-level



**Create tag definition**

**Delete and restore work items**

Project-level



## Permanently delete work items

Project-level



### View work items in this node

Area Path



### Edit work items in this node

Manage test plans

Manage test suites

Area Path



#### ⓘ Note

The **Change work item type** permission doesn't apply to test-specific work items.

Even if you choose this feature from the work item form, changing the work item type is disallowed.

## Azure Artifacts

You can manage feeds from the web portal, [Artifacts](#). Users with at least Stakeholder or Basic access can access Azure Artifacts features. To set permissions, see [Secure feeds using permissions](#).

Feeds have four permission roles: **Feed Reader**, **Feed and Upstream Reader (Collaborator)**, **Feed Publisher (Contributor)**, and **Feed Owner**. Feed Owners can add user accounts or security groups to any role.

[\[ \]](#) Expand table

Permission	Feed Reader	Feed and Upstream Reader (Collaborator)	Feed Publisher (Contributor)	Feed Owner
List packages in the feed	✓	✓	✓	✓
Download/install/restore packages	✓	✓	✓	✓
Save packages from upstream sources		✓	✓	✓
Publish packages			✓	✓
Promote packages to a view			✓	✓
Deprecate/unlist/yank packages			✓	✓
Delete/unpublish packages				✓
Add/remove upstream sources				✓
Allow external package versions				✓
Edit feed settings and permissions				✓

By default, the Project Collection Build Service is a Contributor and your project team is a Reader.

 **Note**

In Azure Artifacts, feeds may be scoped to a single project or to the entire organization. To access a project-scoped feed, a user must also have access to the project containing that feed.

## Notifications, alerts, and team collaboration tools

To manage notifications, see [Manage personal notifications](#) and [Manage team notifications](#).

 **Note**

There are no UI permissions associated with managing notifications. Instead, you can manage them using the [TFS Security command line tool](#).

## Task

### Readers

### Contributors

### Team admins

### Project admins Project Collection admins

---

View the project page, navigate using the project page

- ✓
- ✓
- ✓
- ✓

Edit the project page

- ✓

Set personal notifications or alerts

- ✓
- ✓
- ✓

Set team notifications or alerts

- ✓
- ✓

Set project-level notifications or alerts



View Project READMEs



View Project wikis or code wikis



Provision or create a project wiki



Publish code as a wiki



Request feedback





Provide feedback



Search across projects, organizations, collections



## Dashboards, charts, reports, and widgets

You can define and manage team and project dashboards from the web portal, [Dashboards](#). For an overview of dashboard and chart features, see [Dashboards](#). You can set [individual dashboard permissions](#) to grant or restrict the ability to edit or delete dashboards.

Users granted Stakeholder access to private projects can't view or create query charts. Stakeholder access to public projects can view and create query charts.

**Task**

**Readers**

**Contributors**

**Team admins**

**Project admins**

---

View team and project dashboards



Add and configure project dashboards



---

## Power BI Integration and Analytics views

From the web portal **Analytics views**, you can create and manage Analytics views. An Analytics view provides a simplified way to specify the filter criteria for a Power BI report based on the Analytics Service data store. The Analytics Service is the reporting platform for Azure DevOps. For more information, see [What is the Analytics Service?](#).

You set [permissions](#) for the service at the project level, and for shared Analytics views at the object level. Users with **Stakeholder** access have no access to view or edit Analytics views.

**Task**

**Readers**

**Contributors**

**Project admins**

---

**View Analytics**



View a shared Analytics view



Add a private or shared Analytics view



Edit and delete shared Analytics views



---

## Related articles

- [Add users to a project or team](#)
  - [Permissions and groups reference](#)
  - [About access levels](#)
  - [Web portal navigation](#)
  - [Troubleshoot permissions](#)
- 

## Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

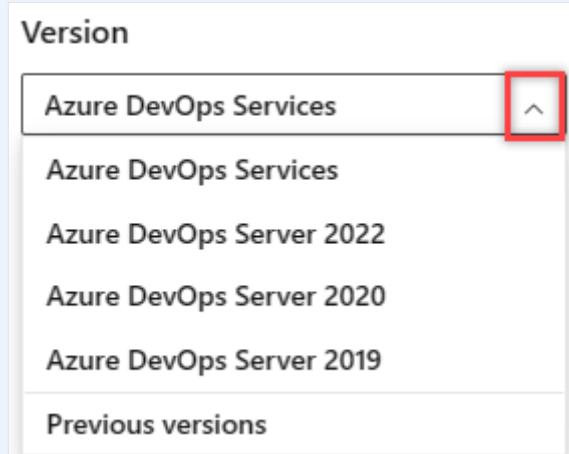
# About access levels

Article • 04/04/2025

## Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

Access levels in Azure DevOps control which web portal features are available or not. Access levels supplement security groups, which allow or deny specific tasks. Administrators ensure that their user base has access to the features they need and only pay for those specific features. It's an efficient way to manage costs while providing the necessary functionality to users. For more information, see [Stakeholder access quick reference](#) and [Manage users and access](#).

### ⓘ Important



Select the version of this article that corresponds to your platform and version. The version selector is above the table of contents. [Look up your Azure DevOps platform and version.](#)

When you add a user or group to a team or project, they automatically gain access to the features associated with the default access level and security group. For most users, assigning them to the **Basic** access level and the **Contributors** security group provides access to most features. For a simplified overview of the permissions assigned to the most common groups **Readers**, **Contributors**, and **Project Administrators**, see [Default permissions](#).

## Supported access levels

Assign users or groups of users to one of the following access levels:

- **Basic:** Provides access to most features. Assign to users with a Visual Studio Professional subscription, an Azure DevOps Server CAL, and to users for whom you're paying for Basic

access in an organization.

- **Basic + Test Plans:** Provides access to all features included in **Basic** and Azure Test Plans. Assign to users with a Visual Studio Test Professional or MSDN Platforms subscription, and to users for whom you're paying for Basic + Test Plans access in an organization.
- **Stakeholder:** Provides limited access to private projects and nearly full access to public projects. Assign to an unlimited number of users without requiring a license or subscription, ideal for those needing access to a restricted set of features. Stakeholders can perform various, including viewing work items, participating in discussion, and accessing dashboards.
- **Visual Studio subscriber:** Assign to users who already have a Visual Studio subscription. The system automatically recognizes the user's subscription—Visual Studio Enterprise, Visual Studio Professional, Visual Studio Test Professional, or MSDN Platform—and enables any other features included in their subscription level. If you assign **Basic** or **Stakeholder**, they also receive their Visual Studio subscription benefits upon sign-in.

### Tip

As a best practice when adding new users, we recommend assigning the **Visual Studio Subscriber** level when appropriate (as opposed to Basic) to prevent being charged the **Basic** rate before the user signs in for the first time.

- **GitHub Enterprise:** The system automatically recognizes users with a GitHub Enterprise license the next time they sign in to Azure DevOps. Regardless of a user's assigned access level (for example, they could be assigned **Stakeholder** access), they receive **Basic** access when they're associated with a GitHub Enterprise license.

The following table indicates those features available for each supported access level. Visual Studio Test Professional and MSDN Platform subscriptions grant access to the same features as Visual Studio Enterprise.

#### Feature

#### Stakeholder

**Basic, GitHub Enterprise, &  
Visual Studio Professional**

**Basic + Test Plans &  
Visual Studio Enterprise**

## **Administer organization**

Can configure resources when also added to a security group or role: team administrator, Project Administrator, or Project Collection Administrator.



---

## **Advanced backlog and sprint planning tools**

Includes full access to all [backlog](#) and [sprint planning](#) tools.



---

## **Advanced home page**

Includes [access](#) to projects, work items, and pull requests defined across projects you work in.



---

## **Advanced portfolio management**

Includes full access to define features and epics from a [portfolio backlog](#) or [board](#).



---

## **Agile boards**

Stakeholders get limited access to [boards](#) and [Taskboards](#). Stakeholders use drag-and-drop to create and change work items, but only change the State field on cards. They only view [the sprint capacity settings](#).





---

## Agile Portfolio Management

Includes limited access to [portfolio backlogs](#) and [boards](#). Stakeholders can't change the backlog priority order, can't assign items to an iteration, use the mapping pane, or exercise forecasting.



## Artifacts

Includes full access to all Azure Artifacts features, up to 2-GiB free storage.



---

## Author Release Pipelines and Manage Releases

Includes defining [release pipelines](#), [multi-stage continuous deployment \(CD\) pipelines](#), and [using approvals and gates to control deployments](#).



## Basic backlog and sprint planning tools

Includes limited access to add and modify items on [backlogs](#) and [sprint backlogs](#) and [Taskboards](#). Stakeholders can't assign items to an iteration, use the mapping pane, or forecasting.



## Build

Includes full access to all features to [manage continuous integration and continuous delivery of software](#).



## Chart Authoring

Can create work tracking [query charts](#).



---

## Chart Viewing

Can only view work tracking query charts. Stakeholders can't view query charts from the Queries page. They can view them when added to a dashboard.



---

## Code

Includes full access to all features to manage code using [Git repositories](#) or using [Team Foundation Version Control \(TFVC\)](#) Team Foundation Version Control (TFVC).



---

## Delivery Plans

Includes full access to add and view Delivery plans.



---

**Request and Manage Feedback** Includes full access to request and manage feedback on working software.



---

### Standard Features

Includes [working across projects](#), [View dashboards](#), [View wikis](#), and [Manage personal notifications](#). Stakeholders can't view Markdown README files defined for repositories and can only view wiki pages. Access might be restricted based on specific project or organization permissions. For full functionality, including the ability to view all wiki features, a **Basic** license is recommended.



---

### Test services in build and release

Includes [running unit tests with your builds](#), [reviewing](#), and [analyzing](#) test results.



---

### Test Case Management

Includes [adding test plans and test suites](#), [creating manual test cases](#), [deleting test artifacts](#), and [testing different configurations](#).



---

### Test Execution and Test Analysis

Includes running [manual](#), [tracking test status](#), and [automated tests](#).





---

### Test summary access to Stakeholder license

Includes [requesting Stakeholder feedback using the Test & Feedback extension](#).



---

### View My Work Items

Access to [add and modify work items](#), [follow work items](#), [view and create queries](#), and [submit, view, and change feedback responses](#). Stakeholders can only assign existing tags to work items (can't add new tags) and can only save queries under My Queries (can't save under Shared Queries).



---

### View Releases and Manage Approvals

Includes [viewing releases](#) and [approving releases](#).



---

## Visual Studio subscription access

Visual Studio subscribers get **Visual Studio subscription** features as a subscriber benefit. When you add those users, be sure to assign them the **Visual Studio subscription** access level.

The system automatically recognizes their subscription and enables any other features included, based on their subscription level.

## Programmatic mapping of access levels

You can manage access levels programmatically using the [az devops user add \(Azure DevOps Services only\)](#) or the [User Entitlement - Add REST API](#). The following table provides a mapping of the access level selected through the user interface and the `accountLicenseType`, `licensingSource`, and `msdnLicenseType` parameters.

[ ] Expand table

Access level (user interface) licenseDisplayName	accountLicenseType	licensingSource	msdnLicenseType
Basic	express	account	none
Basic + Test Plans	advanced	account	none
Visual Studio Subscriber	none	msdn	eligible
Stakeholder	stakeholder	account	none
Visual Studio Enterprise subscription	none	msdn	enterprise
GitHub Enterprise	express	account	enterprise

! Note

The `earlyAdopter` accountLicenseType is an internal value used solely by Microsoft.

## Related articles

- [Stakeholder access quick reference](#)
- [Get started as a Stakeholder](#)
- [Export a list of users and their access levels](#)
- [Default permissions and access](#)

# Azure DevOps Services status

Article • 07/24/2024

## Azure DevOps Services

Our team of engineers around the world work 24/7 to ensure that our customers are always productive and successful with our service. We respond quickly during performance slowdowns and stability issues. Our top priority is to communicate the incident status and our next steps to mitigate the issue. Check the status of our services through the [Azure DevOps Services status portal](#).

Our Customer Impact Assessment (CIA) is modeled after our availability model, which measures real customer experiences representing both reliability and performance. Many of the events we post are based on the CIA.

## Services health matrix

Azure DevOps is a product suite of service offerings. The geography indicates where an organization is hosted in the cloud. The data residency, sovereignty, compliance, and resilience requirements are honored within the geographical boundaries. To help clarify which specific aspects of the service are affected, we communicate impact of each of these services by geography in the service matrix.

The [status portal](#) provides a two-dimensional matrix view of active events mapped to a given service and geography. In addition to the suite of Azure DevOps Services, it displays the following items:

- **Core services:** Encompass the set of features that are fundamental to all five services, such as authentication or the web portal
- **Other services:** Correspond to features that complement the suite, such as extensions

## Service health indicators

The Azure DevOps Services status portal displays indicators that reflect the severity of a service health event, based on the number of customers affected by the issue. The highest severity events affect a large percentage of our customers and render some parts of the product unusable.



The Azure DevOps Services status portal displays four indicators that reflect the severity of a service health event: Healthy, Degraded, Unhealthy, and Advisory. The highest severity events affect a large percentage of our customers and render some parts of the product unusable.

## Service status and event logs

Access detailed information on active and past events from the [Status history page](#). Each event log contains associated information such as the impacted service, geography, and event duration. You can filter the logs to adjust the scope of your search into past events. Additionally, you can use the REST API to build automated alerting solutions to stay on top of events.

## When and how to report availability issues

If you see an issue reported on the Azure DevOps Services health page, we're already working to restore normal operations. If your issue isn't reported, you can ask a question through the [Azure DevOps Services virtual support agent](#). For issues not related to availability, refer to our [Developer Community portal](#).

## RSS feed

Subscribe to [the RSS feed](#) to receive updates in your feed reader.

## Use REST APIs to build automated solutions

The [Azure Resource health REST API](#) can retrieve the current health status of each of the Azure DevOps Services. You can use it to build an automated solution to monitor the infrastructure incidents.

 **Note**

Looking for Azure DevOps REST APIs? See the latest [Azure DevOps REST API reference](#).

For information about .NET client libraries, see [.NET client libraries for Azure DevOps](#).

## Related articles

- [Azure Service Health overview](#)
  - [Blog post: How do you measure quality of a service?](#)
- 

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

# Data protection overview

Article • 02/17/2025

## Azure DevOps Services

Azure DevOps Services is a cloud-hosted application for your development projects, from planning through deployment. Based on the on-premises capabilities, with more cloud services, we manage your source code, work items, builds, and tests. Azure DevOps uses platform as a service (PaaS) infrastructure and many Azure services, including Azure SQL, to deliver a reliable, globally available service for your development projects.

This article discusses the steps that Microsoft takes to help keep your projects safe, available, secure, and private. It describes the role that you play in keeping your projects safe and secure.

This article is for organization administrators and IT professionals who manage their project assets daily. It's most useful to individuals who are already familiar with Azure DevOps and want to know more about how Microsoft protects stored assets in Azure DevOps.

## Our commitment

Microsoft helps to ensure that your projects remain safe and secure, without exception. When you store your projects in Azure DevOps, they benefit from multiple layers of security and governance technologies, operational practices, and compliance policies. We enforce data privacy and integrity both at rest and in transit.

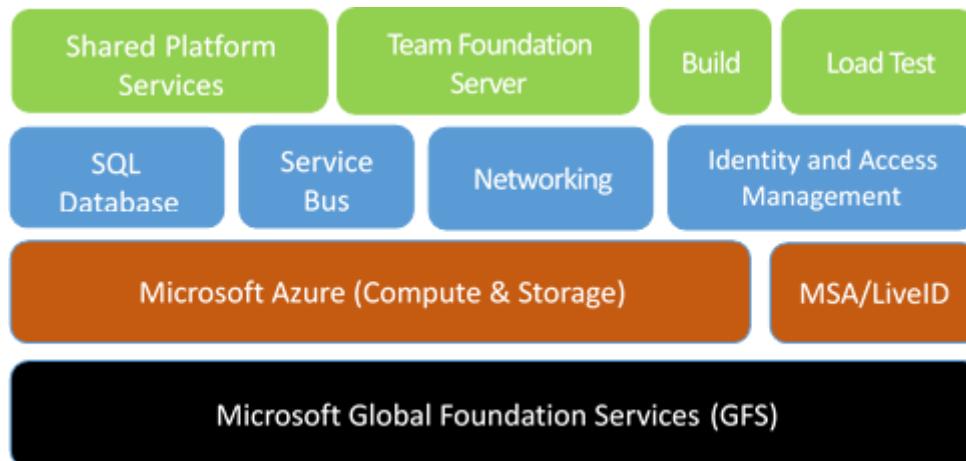
The threats that you face are in four basic categories: data availability, service availability, service security, and data privacy. This article explores specific threats within each category and explains what Azure DevOps does to address them. The article begins by describing how data is stored and how Azure DevOps manages access to your data.

Data protection requires the active engagement of administrators and users who know what steps to take to protect your assets from unauthorized disclosure and tampering. Be explicit when you grant permissions to user access points, so only the right people access data within Azure DevOps.

You should consider all data to be potentially at risk, no matter where it's located or how it's being used. This statement is true for both data stored in the cloud and data stored in a private datacenter. It's important to classify your data, its sensitivity and risk, and the

damage that it might do if it becomes compromised. Also, categorize your data relative to an overall policy for managing information security.

## Built on Azure



We host Azure DevOps entirely in Azure datacenters. Azure DevOps uses many core Azure services, including compute, storage, networking, Azure SQL, identity and access management, and Azure Service Bus.

Azure DevOps uses Azure Storage as the primary repository for service metadata and customer data. Depending on the type of data and the storage and retrieval requirements, Azure DevOps uses Azure Blob Storage and Azure SQL Database storage.

To help you understand the Azure DevOps Services approach to data protection, here's some background on the storage services:

- [Azure Blob Storage](#) stores large chunks of unstructured data. All projects use this service. Data includes potentially sensitive or private information, like the contents of source files and attachments for work items. For most projects, most storage in use is this type of unstructured blob storage.
- [Azure SQL Database](#) stores the structured and transactional aspects of your organization, including project metadata, the versioned source-control history, and details of work items. Database storage gives you fast access to the important elements of your project. It provides indexes into the blob storage to look up files and attachments.

Administrators can manage access to resources by [granting or restricting permissions](#) on user identities or groups. Azure DevOps uses federated authentication of user identities via [Microsoft Entra ID](#) and Microsoft accounts.

During authentication, the user is routed to the authentication provider, where they provide their credentials. After the authentication provider verifies the user's credentials, Azure DevOps issues an authentication cookie to the user. This cookie allows the user to remain authenticated against Azure DevOps.

In this way, the user's credential information is never shared directly with Azure DevOps. For each Azure DevOps resource that the user tries to access, validation of permissions is based on the user's explicit permissions and on permissions that the user inherited through group membership.

Administrators can use access controls to help protect [access to the organization](#), project collections, team projects, and team-scoped data and functionality. Administrators can also use access controls for specific assets like folders for version control and area paths for work items.

## Data availability

Azure DevOps uses many Azure Storage features to help ensure data availability if there's a hardware failure, service disruption, or regional disaster. Also, the Azure DevOps team follows procedures to help protect data from accidental or malicious deletion.

## Data redundancy

To help protect data during hardware or service failures, Azure Storage geo-replicates customer data between two regions in the same geographical location. For example, Azure Storage can geo-replicate data between North and West Europe or between North and South United States.

For Azure Blob Storage, customer data is replicated three times within a single region. Customer data is replicated asynchronously to a second region in the same geographical location. As such, Azure always maintains the equivalent of six copies of your data.

Having multiple copies enables you to fail over to a separate region if there's a major outage or disaster, while also having local redundancy for hardware failures within a region. For Azure SQL Database storage, daily backups are maintained offsite if there's a regional disaster.

Regarding data redundancy and failover:

- There's an inherent delta, measured in minutes, when Microsoft replicates your data between the primary and secondary region.
- Failover to the secondary region is a decision that Microsoft must make centrally, because it affects all customers on a particular scale unit. Except in extreme circumstances, Microsoft opts to avoid failing over so that customer data isn't lost.
- Azure DevOps offers a service-level agreement (SLA) of 99.9 percent uptime. Azure DevOps refunds a portion of the monthly charges if it misses that SLA in a specific month.
- Because there's only one region in Brazil, customer data in Brazil is replicated to the South Central US region for disaster recovery purposes.

## Mistakes happen

To safeguard against accidental data loss, Microsoft employs point-in-time backups for both blobs stored in Azure Blob Storage and databases within Azure SQL Database. Each storage account maintains a separate copy of all blobs, with changes being appended to the existing data. These backups are immutable, eliminating the need to rewrite any existing storage during backup procedures.

Azure SQL Database includes standard backup features utilized by Azure DevOps. Your data is retained for 28 days, with these backups also being replicated in a paired region to facilitate recovery during a regional outage.

You can recover deleted organizations or projects within the 28-day window following deletion. But, once this time period elapses, these entities are permanently deleted and can't be restored. While these backups serve as a crucial component for disaster recovery, it's essential for customers to practice appropriate data management and backup strategies to ensure comprehensive protection of their data.

### Important

- *Accidental deletion* here refers to scenarios that arise as a result of an incident on our services. It doesn't include customers' accidental deletion of assets (for example, repositories, work items, attachments, or artifacts).
- We don't support restoring assets that customers accidentally delete. These backups are meant only for business continuity and to aid recovery from outage or disaster scenarios.
- In rare cases, our deletion process might take up to 70 days due to backend retries and the need to delete data from multiple sources.

## Practice is critical

Having multiple backups of your data is good, but without practice, restoring can be unpredictable. People say that "backups never fail; the restores do." Though the statement is technically incorrect, the sentiment is right.

Microsoft regularly practices restoring datasets from backup. We regularly test geo-redundant storage from Azure. There are many combinations of disaster and data corruption scenarios. We continue to plan and run new tests for these scenarios regularly.

## Service availability

Azure DevOps offers distributed denial-of-service (DDoS) protections and live site response to help ensure that you have access to your organization and associated assets.

### DDoS protections

In some cases, a malicious DDoS attack can affect service availability. Azure has a DDoS defense system that helps prevent attacks against our service. It uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits. The system is designed to withstand attacks not only from the outside but also from within Azure.

For application-specific attacks that can penetrate the Azure defense systems, Azure DevOps establishes application-level and organization-level quotas and throttling. This practice helps prevent any overuse of key service resources during an attack or accidental misuse of resources.

### Live site response

In rare circumstances, you might require a live site response to a problem with service availability. We have an operations team that's constantly available to rapidly identify the problem and to engage the necessary development team resources.

The development team resources then address the problem. They also aim to update the service status page within minutes of detecting a problem that affects the service. After development team resources address a problem, they identify the root cause and track the necessary changes to prevent similar problems in the future.

Azure DevOps processes for live site management focus on your experience and the health of the service. These processes minimize the time to detect, respond to, and mitigate problems. All engineering disciplines are involved and responsible, so continual improvements evolve out of direct experience. Monitoring, diagnostics, resiliency, and quality assurance processes then improve over time.

Live site management in Azure DevOps has three distinct tracks: telemetry, incident management, and live site review. Here's what these tracks entail:

Telemetry	Incident management	Live-site review
<ul style="list-style-type: none"><li><b>Alerts</b> – define health alerts for failure modes</li><li><b>Diagnostics</b> – deliver instrumentation data and operational reports</li><li><b>Troubleshooting guides</b> – guidance for investigating an alert is defined by the feature, and then refined by the Service Engineer</li><li><b>Failure mode testing</b> – the Service Delivery (SD) team performs failure testing to ensure alerts fire as expected</li><li><b>Onboarding</b> – the feature team works with their Service Engineer (SE) to onboard new alerts to the 24 x 7 team</li></ul>	<ul style="list-style-type: none"><li><b>Detection</b> – product alerts detect health issues and start the Live Site Incident (LSI) process</li><li><b>Triage</b> – The 24 x 7 team receives all critical alerts and confirms impact using Azure DevOps guidance</li><li><b>Escalation</b> – both Dev and Ops have individuals in an on-call rotation. SE is the initial escalation path. The SE calls Dev, as needed</li><li><b>Incident management</b> – a bridge is managed by the SE who engages Dev, and Partners to troubleshoot</li><li><b>Resolution</b> – communication and service restoration are actively driven until customer impact is eliminated</li></ul>	<ul style="list-style-type: none"><li><b>Goal</b> – weekly review of LSI ensure that leadership has visibility into live site health and repeat issues</li><li><b>Cadence</b> – Incidents from prior week have root cause documented, then reviewed on weekly basis</li><li><b>Audience</b> – VS Leadership, Partner team when they drive impact. Developer attends to provide details on Service incident</li><li><b>Ownership</b> – Dev. Owns reviews for App and Deploy issues. SD owns for Platform issues.</li><li><b>Driving improvements</b> – Bugs and problem work items are logged for gaps (e.g. – missing alerts) and repeat root cause</li></ul>

The operations team also monitors the availability metrics for individual organizations. These metrics provide insights into specific conditions that might affect only some of our customers. Investigations into this data can often result in targeted improvements to address customer-specific issues. In some cases, Microsoft might even contact you directly to understand your experience and work with you to improve the service.

Microsoft publishes an SLA and provides a financial guarantee to ensure that we meet this agreement each month. For more information, see [SLA for Azure DevOps](#).

Sometimes, partner teams or dependencies have incidents that affect Azure DevOps. All partner teams follow similar approaches to identifying, resolving, and learning from these service outages.

# Service security

Service security requires constant vigilance, from proper design and coding techniques to operational factors. Microsoft actively invests in the prevention of security holes and in breach detection. If there's a breach, Microsoft uses security response plans to minimize data leakage, loss, or corruption. For more information, see [About security, authentication, and authorization](#).

## Security by design

Azure DevOps is designed to be secure. Azure DevOps uses the Microsoft Security Development Lifecycle at the core of its development process. The Microsoft Operational Security Assurance program guides cloud operation procedures in Azure DevOps.

The Azure DevOps team has annual training requirements for all engineers and operations personnel. The team also sponsors informal meetings hosted by Microsoft engineers. After the team solves a problem that surfaces in a meeting, it shares the lessons learned with other teams.

The following methodologies specify the training requirements:

- Threat modeling during service design
- Following best practices for design and code
- Verifying security with standard tooling and testing
- Limiting access to operational and customer data
- Gating rollout of new features through a rigid approval process

A cloud service is only as secure as the host platform. Azure DevOps uses PaaS for much of its infrastructure. PaaS automatically provides regular updates for known security vulnerabilities.

Virtual machines hosted in Azure use infrastructure as a service (IaaS), such as for a [hosted build service](#). Such images receive regular updates to include the latest security patches available from Windows Update. The same update rigor applies for on-premises machines, including those machines used for deployment, monitoring, and reporting.

The Azure DevOps team conducts regular, security-focused penetration testing of Azure DevOps. Penetration testing tries to exploit the live production services and infrastructure of Azure DevOps by using the same techniques and mechanisms that malicious attackers use. The goal is to identify real-world vulnerabilities, configurations, errors, or other security gaps in a controlled process.

The team reviews the results of these tests to identify other areas of improvement and to increase the quality of the preventative systems and training. You can review the results of recent Azure DevOps penetration tests on the [Microsoft Service Trust Portal](#).

## Credential security

Microsoft is committed to ensuring that your projects remain safe and secure, without exception. In Azure DevOps, your projects benefit from multiple layers of security and governance technologies, operational practices, and compliance policies. We enforce data privacy and integrity both at rest and in transit. In addition, we adhere to the following practices with respect to the credentials or secrets that Azure DevOps stores. To learn more about how to choose the right authentication mechanism, see [Guidance for authentication](#).

### Important

[Azure DevOps doesn't support Alternate Credentials authentication](#). If you're still using Alternate Credentials, we strongly encourage you to switch to a more secure authentication method.

## Personal access tokens (PATs)

- We store a hash of the PAT.
- Raw PATs generate in-memory on the server side. 32 bytes randomly generated through the RNGCryptoServiceProvider and get shared with the caller as a base-32-encoded string. This value is NOT stored.
- PAT hash generates in-memory on the server side as an *HMACSHA256Hash* of the raw PAT using a 64-byte symmetric signing key stored in our key vault.
- Hash gets stored in our database.

## Secure shell (SSH) keys

- We store a hash of the enclosing organization ID and the SSH public key.
- Raw public keys get provided directly by the caller over SSL.
- SSH hash generates in-memory on the server side as an *HMACSHA256Hash* of the organization ID and raw public key using a 64-byte symmetric signing key stored in our key vault.
- Hash gets stored in our database.

## OAuth credentials (JWTs)

- OAuth credentials issue as fully self-describing JSON web tokens (JWTs) and aren't stored in our service.
- The claims in JWTs issued and presented to our service get validated using a certificate stored in our key vault.

## Reporting security flaws

If you believe that your penetration testing revealed a potential security flaw related to the Azure DevOps service, report it to Microsoft within 24 hours. For more information, see the [Microsoft webpage for reporting a computer security vulnerability](#).

### Important

Although you don't need to notify Microsoft about penetration testing activities, you must comply with the [Microsoft Penetration Testing Rules of Engagement](#).

## Bounty program

Azure DevOps participates in the Microsoft Bug Bounty program. This program rewards security researchers who report problems to us, and it encourages more people to help keep Azure DevOps secure. For more information, see [Microsoft Azure DevOps Bounty Program](#).

## Restricting access

Microsoft maintains strict control over who gets access to our production environment and customer data. We grant access at the level of least privilege required, and only after verification of a user's justifications. If a team member needs access to resolve an urgent problem or deploy a configuration change, they must apply for just-in-time access to the production service. Access is revoked as soon as the situation is resolved.

We track and monitor access requests and approvals in a separate system. All access to the system correlates against these approvals. If we detect unapproved access, we alert the operations team to investigate.

We use two-factor authentication for all remote system access. If the username and password for one of our developers or operations staff are stolen, the data remains protected. More authentication checks via smart card or a phone call to a preapproved number must occur before we permit any remote access to the service.

To manage and maintain the service, Microsoft uses secrets such as RDP passwords, SSL certificates, and encryption keys. These secrets are all managed, stored, and transmitted securely through the Azure portal. Any access to these secrets requires specific permission, which is logged and recorded securely. All secrets are rotated on a regular cadence, and we can rotate them on demand if there's a security event.

The Azure DevOps operations team uses hardened administrator workstations to manage the service. These machines run a minimal number of applications and operate in a logically segmented environment.

Operations team members must provide specific credentials with two-factor authentication to access the workstations. All access is monitored and securely logged. To isolate the service from outside tampering, we don't permit applications such as Outlook and Office, because they're often targets of spear phishing and other types of attacks.

## Intrusion protection and response

We encrypt data via HTTPS and SSL to help ensure that it isn't intercepted or modified while in transit between you and Azure DevOps. Data that we store on your behalf in Azure DevOps is encrypted as follows:

- Data stored in Azure SQL databases is encrypted via [transparent data encryption](#). This feature helps protect against malicious activity by doing real-time encryption of the database, associated backups, and transaction log files at rest.
- Azure Blob Storage connections are encrypted to help protect your data in transit. For data at rest stored in Azure Blob Storage, Azure DevOps uses [service-side encryption](#).

The Azure DevOps team uses the Azure infrastructure to log and monitor key aspects of the service. Logging and monitoring help ensure that activities within the service are legitimate, and they help detect breaches or attempted breaches.

All deployment and administrator activities are securely logged, as is operator access to production storage. The log information is automatically analyzed, and any potentially malicious or unauthorized behavior raises real-time alerts.

When the Azure DevOps team identifies a possible intrusion or high-priority security vulnerability, it has a clear response plan. This plan outlines responsible parties, required steps for securing customer data, and instructions on how to engage with security experts at Microsoft. The team also notifies any organization owners if data was disclosed or corrupted, so that they can take appropriate steps to remedy the situation.

To help combat emerging threats, Azure DevOps employs an *assume breach* strategy. A highly specialized team of security experts within Microsoft assumes the role of sophisticated adversaries. This team tests breach detection and response, to accurately measure readiness and the impacts of real-world attacks. This strategy strengthens threat detection, response, and defense of the service. It also allows the team to validate and improve the effectiveness of the entire security program.

## Ransomware attack protection

Azure DevOps uses Azure controls to help prevent, detect, and respond to a ransomware attack. For more information about how Azure helps protect customers from ransomware attacks, see [Ransomware protection in Azure](#).

## Data privacy

You should have confidence that we're handling your data appropriately and for legitimate uses. Part of that assurance involves carefully restricting usage.

## General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the biggest change in data protection laws in Europe since the 1995 introduction of the European Union (EU) Data Protection Directive 95/46/EC. For more information about GDPR, see the [overview page in the Microsoft Trust Center](#).

## Data residency and sovereignty

Azure DevOps is available in the following eight geographical locations across the world: United States, Canada, Europe, United Kingdom, India, Australia, Asia Pacific, and Brazil. By default, your organization is assigned to your closest location. However, you can choose a different location when you create your organization. If you change your mind later, you can migrate the organization to a different location with the assistance of Microsoft support.

Azure DevOps doesn't move or replicate customer data outside the chosen location. Instead, your data is geo-replicated to a second region within the same location. The only exception is Brazil, which replicates data to the South Central US region for disaster recovery purposes.

 Note

For builds and releases that run on Microsoft-provided macOS agents, your data is transferred to a GitHub datacenter in the United States.

For more information, see [Data locations for Azure DevOps](#).

## Law enforcement access

In some cases, third parties such as law enforcement entities might approach Microsoft to obtain access to customer data stored in Azure DevOps. We try to redirect the requests to the organization owner for resolution. When a court order compels Microsoft to disclose customer data to a third party, Microsoft makes a reasonable effort to notify the organization owner in advance, unless we're legally prohibited from doing so.

Some customers require their data storage in a particular geographical location to ensure a specific legal jurisdiction for any law enforcement activities. All customer data, such as source code, work items, test results, and geo-redundant mirrors and offsite backups, is maintained within one of the previously mentioned locations.

## Microsoft access

From time to time, Microsoft employees need to obtain access to customer data stored in Azure DevOps. As a precaution, all employees who have (or might ever have) access to customer data must pass a background check that includes previous employment and criminal convictions. We permit access to the production systems only when there's a live site incident or other approved maintenance activity, which is logged and monitored.

Because not all data within our system is treated the same way, we classify data into these types:

- **Customer data:** What you upload to Azure DevOps.
- **Organization data:** Information that you submit when you sign up for or administer your organization.
- **Microsoft data:** Information required for or collected through the operation of the service.

Based on the classification, we control usage scenarios, geo-location requirements, access restrictions, and retention requirements.

## Microsoft promotional use

Microsoft occasionally wants to contact customers to let them know about more features and services that might be useful. Because not all customers want to be contacted about these offers, you can opt in and opt out of marketing email communications.

Microsoft never uses customer data to target specific offers for specific users or organizations. Instead, we use organization data and aggregate usage statistics at the organization level to determine groups that should receive specific offers.

## Managing privacy policies for admins to control user feedback collection

The feedback toggle feature allows Azure DevOps organization owners to control whether users are prompted to provide feedback and submit it. This feature is essential for ensuring that feedback practices align with your organization's privacy and governance policies.

## Building confidence

You can be confident in other efforts that Microsoft makes on behalf of Azure DevOps. These efforts include internal adoption policies at Microsoft, the level of transparency into the state of our service, and progress toward receiving certification of our systems for managing information security.

## Internal adoption

Microsoft teams are adopting Azure DevOps internally. The Azure DevOps team moved into an organization in 2014 and uses it extensively. We established guidelines to enable the adoption plans for other teams.

Large teams move more gradually than smaller ones, because of their investments in existing DevOps systems. For teams that move quickly, we established a project classification approach. It assesses risk tolerance, based on project characteristics, to determine if the project is appropriate for Azure DevOps. For larger teams, the adoption typically occurs in phases, with more planning.

More requirements for internal projects include associating the organization with Microsoft Entra ID to ensure the proper user-identity lifecycle and password complexity. Projects that are more sensitive also require two-factor authentication.

## Compliance certifications

You might be interested in understanding third-party evaluation of our procedures for data security. Azure DevOps achieved the following certifications:

- ISO 27001:2013
- ISO 27018:2019
- ISO 26262:2023
- Health Insurance Portability and Accountability Act (HIPAA)
- Business Associate Agreement (BAA)
- EU Model Clauses
- System and Organization Controls (SOC) 1 Type 2
- SOC 2 Type 2
- Germany C5
- Australia IRAP
- ENS-Spain

The SOC audit for Azure DevOps covers controls for data security, availability, processing integrity, and confidentiality. The SOC reports for Azure DevOps are available through the [Microsoft Service Trust Portal](#).

The Consensus Assessment Initiative Questionnaire (CAIQ) helps organizations assess and evaluate the security practices and capabilities of cloud service providers. In alignment with our commitment to security and transparency, we recently completed the CAIQ assessment for Azure DevOps. We invite you to review the full report on the [Microsoft Service Trust Portal](#).

## Steps you can take

Proper data protection requires active engagement from you, your administrators, and your users. Your project data stored in Azure DevOps is only as secure as the user access points. Match the level of permission strictness and granularity for those organizations with your project's sensitivity level.

## Classify your data

The first step is to classify your data. Classify data based on sensitivity and risk horizon, along with the damage that might occur if compromised. Many enterprises have existing classification methods that they can reuse when projects move to Azure DevOps. For more information, you can download [Data classification for cloud readiness](#) from Microsoft Trustworthy Computing.

## Adopt Microsoft Entra ID

Use Microsoft Entra ID to manage your organization's access to Azure DevOps.

Microsoft Entra ID provides another way to improve the security of your users' credentials.

Microsoft Entra ID allows your IT department to manage its user access policy, password complexity, password refreshes, and expiration when users leave your organization. Through Active Directory federation, you can directly link Microsoft Entra ID to your organization's central directory, so you have only one location to manage these details for your enterprise.

The following table compares Microsoft account and Microsoft Entra characteristics relative to Azure DevOps access:

[\[+\] Expand table](#)

Property	Microsoft account	Microsoft Entra ID
Identity creator	User	Organization
Single username and password for all work assets	No	Yes
Password lifetime and complexity control	User	Organization
Azure DevOps membership limits	Any Microsoft account	Organization's directory
Traceable identity	No	Yes
Organization and IP ownership	Unclear	Organization
Two-factor authentication enrollment	User	Organization
Device-based conditional access	No	Organization

[Learn more about configuring this support for your organization.](#)

## Require two-factor authentication

You might want to restrict access to your organization by requiring more than one factor to sign in. You can require multiple factors by using Microsoft Entra ID. For example, you can require phone authentication, in addition to a username and password, for all authentication requests.

## Use BitLocker

For sensitive projects, you can use BitLocker on your Windows laptop or desktop computer. BitLocker encrypts the entire drive on which Windows and your data reside. When BitLocker is enabled, it automatically encrypts any file you save on that drive. If your computer falls into the wrong hands, BitLocker prevents unauthorized access of local copies of data from your projects.

## Limit use of alternate authentication credentials

The default authentication mechanism for Git-related tooling is alternate authentication (sometimes called *basic authentication*). This mechanism allows a user to set up an alternate username and password for use during Git command-line operations. The user can use this username/password combination to access any other data for which that user has permissions. By its nature, alternate authentication credentials are less secure than the default federated authentication.

You can still make choices for increased security. All communication is sent over HTTPS, and there are password complexity requirements. Your organization should continue to evaluate whether it needs more policies to meet your projects' security requirements.

You can disable alternate authentication credentials if you decide that it doesn't meet your organization's security requirements. For more information, see [Change application connection & security policies for your organization](#).

## Secure access to your organization

Administrators can use Microsoft Entra ID to control access to Azure resources and applications, such as Azure DevOps. With conditional access control in place, Microsoft Entra ID checks for the specific conditions that you set for a user to access an application. After the user meets access requirements, the user is authenticated and can access the application.

Azure DevOps supports enforcing certain types of conditional access policies (for example, IP fencing) for custom Azure DevOps authentication mechanisms. These mechanisms include personal access tokens, alternate authentication, OAuth, and Secure Shell (SSH) keys. If your users access Azure DevOps through a third-party client, only IPv4-based policies are honored.

## More resources

- [Azure DevOps home page ↗](#)
- [Data locations for Azure DevOps](#)

- Microsoft privacy statement [↗](#)
  - Azure DevOps Support [↗](#)
  - Features and services included with Azure DevOps
  - Azure Trust Center [↗](#)
  - Microsoft Security Development Lifecycle [↗](#)
- 

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback [↗](#)

# Data locations for Azure DevOps

Article • 12/15/2023

## Azure DevOps Services

You can choose the location for your data during initial sign-up and creation of your organization.

## Data locations

Azure DevOps data is available in the following geographical locations:

- Australia
- Brazil
- Canada
- Asia Pacific
- Europe (EU)
- India
- United Kingdom (UK)
- United States (US)

By default, your organization uses the closest location. However, you can choose a different location when you create your organization. If you change your mind later, you can [migrate your organization to a different location](#).

## Customer data

Except [as noted later in this article](#), Azure DevOps maintains all customer data within your selected geographical location. Customer data includes the following data types:

- Source code
- Work items
- Test results
- Geo-redundant mirrors and offsite backups

Azure DevOps works with and uses many Microsoft Azure services. For more information on customer data retention by location, see [Data residency in Azure](#).

## Profile data

Azure DevOps stores information that's global in nature, such as user identities and profile data, as follows:

- For US-based users: in the US datacenter
- For EU-based users: in the EU datacenter
- For UK-based users: in the UK datacenter
- For users from all other countries and regions: in the US datacenter

## Token data

Azure DevOps stores token data, such as personal access tokens and Secure Shell (SSH) keys, in a US datacenter.

## Allowlist data for tenant policies

We recommend using groups with your tenant policy allowlists. If you use a named user, be aware that a reference to the named user's identity resides in the US, EU, and Southeast Asia (Singapore).

## Transferring your data

We don't transfer customer data outside your selected location. However, we transfer your data if we need to take any of the following actions:

- Provide customer support
- Troubleshoot the service
- Comply with legal requirements

If necessary, you can transfer your data by using preview, beta, or other prerelease services. These services typically store your data in the United States, but they might store it globally.

### Note

For builds and releases that run on Microsoft-provided macOS agents, your data is transferred to a GitHub datacenter in the United States. GitHub owns and manages this datacenter location with compliance certifications, such as [SOC 1 Type 2](#) and [SOC 2 Type 2](#).

Microsoft doesn't control or limit the locations from which you or your users can access your data.

 **Note**

Because there's only one region in Brazil, customer data in Brazil is replicated to the South Central US region for disaster recovery and load balancing. For more information, see [Data residency in Azure](#).

## Related articles

- [Get started with Azure DevOps](#)
- [Data protection overview](#)

# Launch Visual Studio via Azure DevOps Services

Article • 10/25/2024

## Azure DevOps Services

When you first open [Visual Studio 2022](#), you can sign in and connect to [Azure DevOps Services](#).

If you're already signed in to Visual Studio 2019, see [connect to Azure DevOps Services](#).

Once connected, you can store and share code in free, unlimited, private, cloud-based Git repositories or Team Foundation Version Control (TFVC). Use Agile tools for DevOps, continuous integration, and continuous delivery to organize and manage your work, which helps your team build frequently, test early, and ship faster.

To set up Visual Studio without Azure DevOps Services, see [Install Visual Studio](#). To host your own server, [install and set up Azure DevOps Server](#).

You can also use Azure DevOps Services with any IDE or code editor, like the following examples:

- [Eclipse, Android Studio, or IntelliJ](#)
- Xcode (see [Git](#) or [TFVC](#))
- [Visual Studio Code](#)

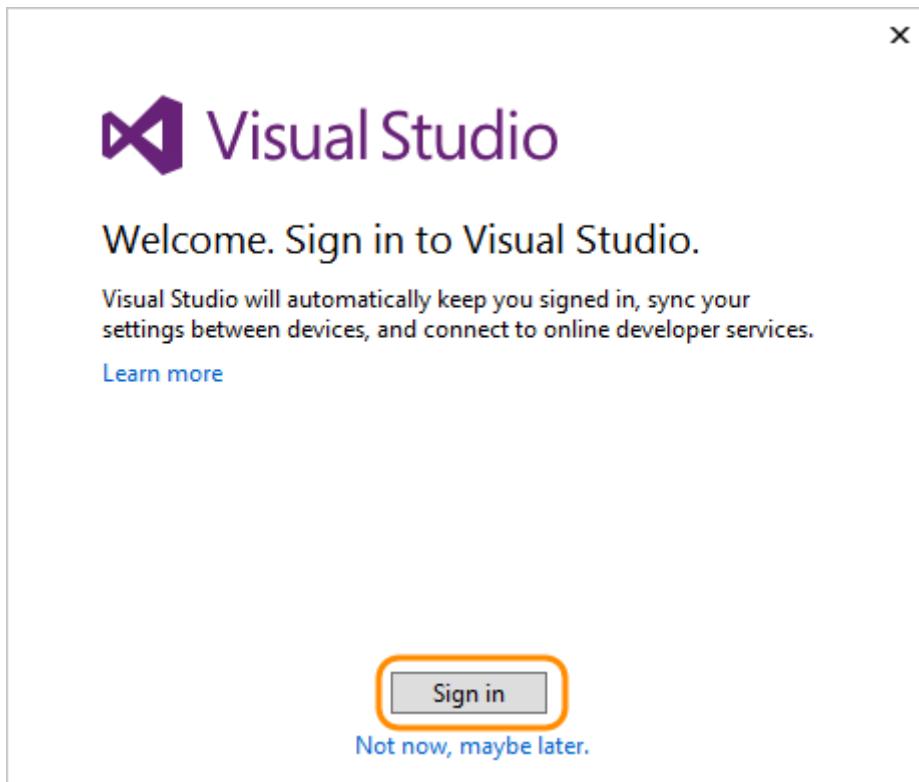
## Prerequisites

Tools: [Download and install Visual Studio](#). If you have a Visual Studio subscription that includes the Visual Studio IDE, get the version that's available with your subscription.

## Set up Visual Studio 2022 for Azure DevOps Services

1. Start Visual Studio, and then sign in to create your profile.

This profile saves your settings and roams with you when you sign in to Visual Studio on any computer. [Why else should I sign in?](#) If you're a Visual Studio subscriber, use the sign in address for your subscription.



[Can't sign in?](#)

2. Enter your credentials.
3. Add your Visual Studio profile details. You only need to do this action once.

A screenshot of the Visual Studio profile details window. It shows fields for "Full name" (Jamal Hartnett), "Contact e-mail" (jamalhartnett@outlook.com), "Phone number" (empty), and "Country/Region" (United States). The "Full name" field has a red asterisk and a question mark icon, indicating it is required.

4. Name your organization and confirm its location.

Create a Visual Studio Team Services site (optional)

<https://fabrikam>

.visualstudio.com

Your account will be hosted in the **South Central US** region.

[Change options](#)

Microsoft may use your contact information to provide updates and special offers about Visual Studio. You can unsubscribe at any time.

By clicking **Continue**, you agree to the [Terms of Service](#) and [Privacy Statement](#).

[Continue](#)

[How can I create an organization later or change its location?](#)

5. Create your first project to store your code, work items, backlog, builds, tests, and other assets. Name your project, select a process to organize your work, and choose a version control to manage your code.

 **Visual Studio**

## Create your first team project

Welcome. Your account, <https://fabrikam.visualstudio.com/>, is created and ready to go. Now create your first team project where you'll host your code and backlog. [Learn more](#)

Project name: \*

Process template: \*

Version control: \*

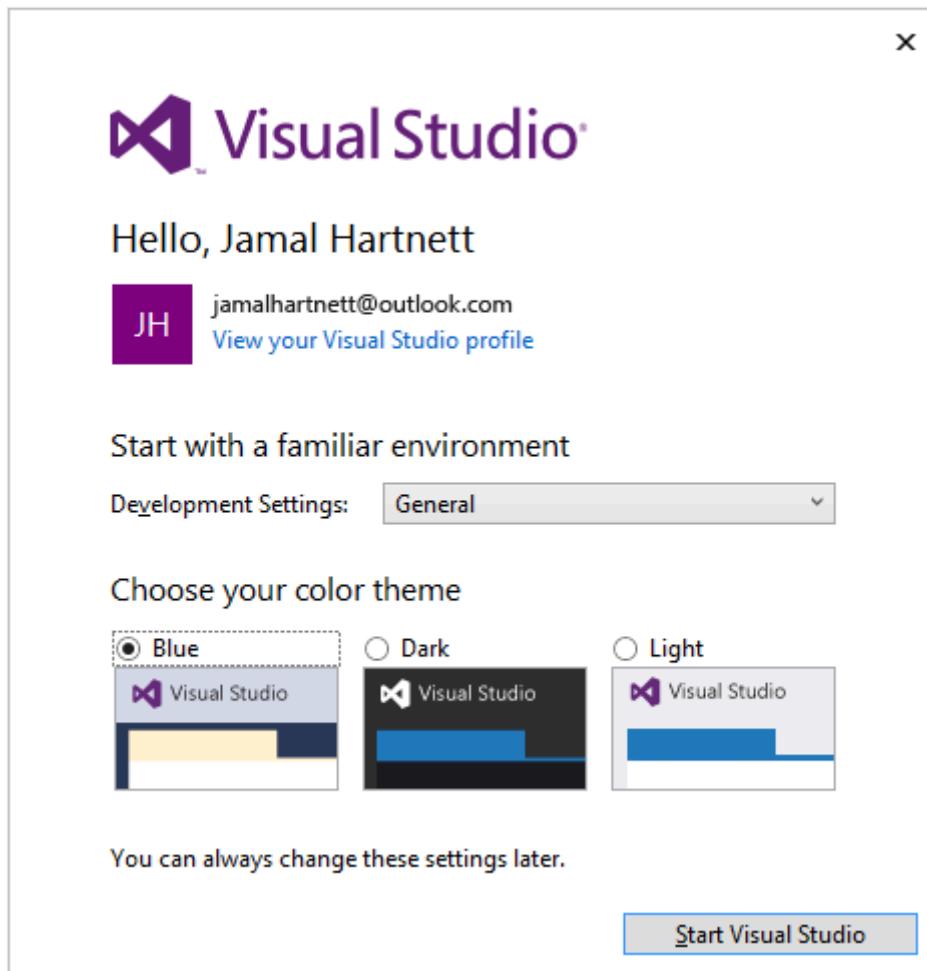
 Git (i)     Team Foundation Version Control (i)

Create a README.md file to describe this project

[Not now, maybe later](#) [Create project](#)

Not sure which to choose? Learn which [process](#) and version control, [Git](#) or [TFVC](#), work best for you.

6. If you're a new Visual Studio user, you can change your settings anytime in Visual Studio options.



These changes get saved with your profile and your settings roam with you wherever you sign in.

7. To view your new organization, sign in to

[https://dev.azure.com/{Your\\_Organization}](https://dev.azure.com/{Your_Organization}).

## Next steps

[Add users to your organization](#)

## Related articles

- [Add code to Git](#)
- [Add code to TFVC](#)
- [Create your backlog](#)
- [Manage your process](#)
- [Customize your process](#)

---

# Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# Settings & Usage documentation

Configure resources and manage settings for an organization, project, team, or user.

## Get started



### OVERVIEW

[About settings](#)

[Get started as an administrator](#)



### QUICKSTART

[Set user preferences](#)



### HOW-TO GUIDE

[Enable preview features](#)

## Manage your organization (cloud)



### OVERVIEW

[About managing your organization](#)

[Plan your organizational structure](#)



### QUICKSTART

[Create an organization](#)



### CONCEPT

[Manage access with Microsoft Entra ID](#)



### HOW-TO GUIDE

[Add users to your organization](#)

[Connect your organization to Microsoft Entra ID](#)

## Add & manage projects

---

### CONCEPT

[About projects & scaling up](#)

[Customize your project](#)

---

### OVERVIEW

[Manage your project](#)

---

### HOW-TO GUIDE

[Create a project](#)

[Connect to GitHub](#)

## Add & manage teams

---

### CONCEPT

[About teams & Agile tools](#)

---

### HOW-TO GUIDE

[Add a team](#)

[Configure team tools](#)

[Define team area paths](#)

[Configure team iterations](#)

[Add a team administrator](#)

## Set alerts or notifications

---

### CONCEPT

[About notifications](#)

## HOW-TO GUIDE

[Set personal notifications](#)

[Set team notifications](#)

## Audit & usage (cloud)

### CONCEPT

[Rate limits & usage](#)

### QUICKSTART

[Access, export, and filter audit logs](#)

## Configure Pipelines resources

### HOW-TO GUIDE

[Create & manage agent pools](#)

[Create & manage deployment groups](#)

[Set build & release retention policies](#)

[Create & manage service connections](#)

## Configure Repos resources

### OVERVIEW

[About branches and branch policies](#)

### HOW-TO GUIDE

[Create & manage Git repositories](#)

[Set Git repository settings and policies](#)

[Manage Git branch policies](#)

[Add TFVC check-in policies](#)

## Configure Test resources



HOW-TO GUIDE

[Set test retention policies](#)

# About projects and scaling your organization

Article • 03/12/2025

Azure DevOps Services | Azure DevOps Server 2022 - Azure DevOps Server 2019

A project in Azure DevOps provides a space for users to plan, track progress, and collaborate on building software solutions. It serves as a fundamental container for storing data and source code.

When you create a project, Azure DevOps automatically creates a team with the same name, which is sufficient for small organizations. For enterprise-level organizations, you might need to scale up by creating more teams and projects. Azure DevOps supports up to 1,000 projects within an organization.

An organization with multiple projects allows teams to configure tools to suit their needs and complete administrative tasks at the appropriate levels. As your organization grows, your tools can scale to support a [culture of team autonomy and organizational alignment](#).

For more information, see [Work tracking, process, and project limits](#) and [Plan your organizational structure](#).

## Manage work across your organization

When you connect to Azure DevOps, you connect to an organization. Within this organization, you can define one or more projects. At least one project must be created to use the system.

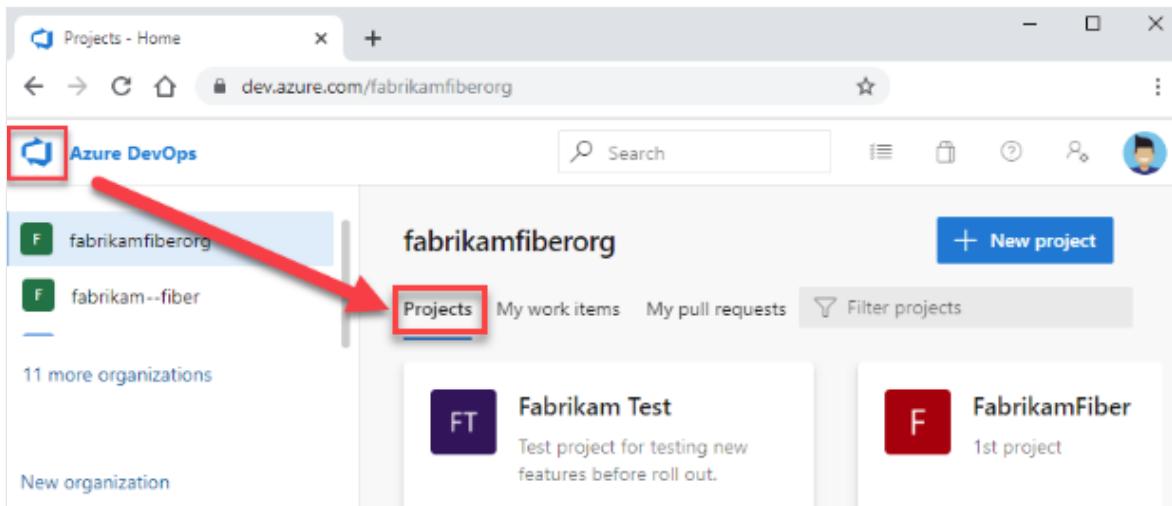
You can scale your organization in the following ways:

- **Add projects:** Support different business units.
- **Add teams:** Create teams within a project.
- **Add repositories and branches:** Manage your source code.
- **Add agents, agent pools, and deployment pools:** Support continuous integration and deployment.
- **Manage access:** Use Microsoft Entra ID to handle a large number of users.

## View projects in your organization

View the projects defined for your organization by opening the **Projects** page.

1. Select  **Azure DevOps** to open **Projects**.



2. Choose a project from the list of projects.

For more information, see [Create a project](#).

## Limit project visibility

By default, users added to an organization can view all organization and project information and settings. For more information, see [Limit user visibility for projects and more](#) and [Change project visibility to public or private](#).

## View historical data

All project members can view identities added to comments, discussions, or assignments. For example, everyone in the project (even users with new restrictions) can still see a user's name assigned to a work item when the user is no longer part of the project. The same applies to @mentions in PRs, comments, discussions, and more.

## Use a single project

One recommended approach is to use a single project to support your organization or enterprise. A single project can help minimize the maintenance of administrative tasks and provides the most optimized and flexible [cross-link object](#) experience.

Even if you have many teams working on hundreds of different applications and software projects, you can easily manage them within a single project. A project isolates

the data stored within it, and moving data from one project to another results in the loss of associated history.

For more information, see [How many projects do you need?](#).

## Add another project

Another feasible approach is to have multiple projects. This approach is recommended if your organization needs to:

- Prohibit or manage access to the information contained within a project for select groups
- Support custom work tracking processes for specific business units within your organization
- Support entirely separate business units that have their own administrative policies and administrators
- Test customization activities or add extensions before rolling out changes to the working project
- Support an open-source software (OSS) project

## Use private and public projects

You can have both private and public projects. You can also [change the visibility of a project from either one to the other](#).

### Private projects:

- Require adding and managing user access.
- Require users to sign in to gain access even for read-only access.
- Provide all project members access to the project and organization information.

For more information, see [Resources granted to project members](#).

### Public projects:

- Don't require users to sign in for read-only access to many services.
- Support sharing code with others.
- Support continuous integration/continuous deployment (CI/CD) of open-source software.

For more information, see [Change visibility of a project](#).

# Version control support

Git repositories can be browsed and cloned only via HTTPS. SSH and GVFS endpoints are unavailable. Clients like Visual Studio and IntelliJ work with the HTTPS clone URL but don't offer the connected experience linking to work items and other collateral.

# Dashboard widget support

The following dashboard widgets don't display any useful information for nonmembers.

- Assigned to me
- Code tile
- New work item
- Pull request
- Query results
- Requirements quality
- Sprint burndown
- Sprint capacity
- Sprint overview
- Team members
- Welcome
- Work links
- Other links

For more information, see [Add widgets to a dashboard](#) and [FAQs about dashboards, charts, and reports](#).

# Structure your project

Use the following elements to structure your project to support your business needs:

- [Create a Git repository](#) for each subproject or application, or [create root folders within a TFVC repository](#) for each subproject. If you're using TFVC and heading toward a combined project model, create root folders for different teams and projects, just as you would create separate repos in Git. Secure folders as needed and control which segments of the repo you're actively using with workplace mappings.
- [Define area paths](#) to support different subprojects, products, features, or teams.
- [Define iteration paths \(also known as sprints\)](#) that can be shared across teams.
- [Add a team](#) for each product team that develops a set of features for a product. Each team you create automatically creates a security group for that team, which

you can use to manage permissions for a team. For more information, see [Portfolio management](#).

- [Manage access to specific features and functions](#) using custom security groups.
- [Create query folders](#) to organize queries for teams or product areas into folders.
- [Define or modify notifications](#) set at the project level.

## Customize and configure your project

You can configure and customize most services and applications to support your business needs or the way your teams work. Within each project, you can do the following tasks. For a comprehensive view of which resources can be configured, see [About team, project, and organizational-level settings](#).

- **Dashboards:** Each team can [configure their set of dashboards](#) to share information and monitor progress.
- **Source control:** For each [Git repository](#), you can apply branch policies and define branch permissions. For TFVC repositories, you can [set check-in policies](#).
- **Work tracking:** You can add fields, change the workflow, add custom rules, and add custom pages to the work item form of most work item types. You can also add custom work item types. For more information, see [Customize an inheritance process](#).
- **Azure Pipelines:** You can fully customize your build and release pipelines, and define build steps, release environments, and deployment schedule. For more information, see [Build and release](#).
- **Azure Test Plans:** You can define and configure test plans, test suites, test cases, and test environments. You can also add test steps within your build pipelines. For more information, see [Exploratory and manual testing](#) and [continuous testing for your builds](#).

## Add a team

As your organization grows, you can add teams equipped with configurable Agile tools to meet each team's workflow. For more information, see the following articles.

- [Scale Agile to large teams](#)
- [About teams and Agile tools](#)
- [Manage a portfolio of backlogs](#) and see progress.
- [Use delivery plans](#) to scheduled work items by sprint (iteration path) of selected teams against a calendar view.
- [Incrementally adopt practices that scale](#) to create greater rhythm and flow within your organization, engage customers, improve project visibility, and develop a

productive workforce.

- Structure projects to gain visibility across teams or to support epics, release trains, and multiple backlogs to support the Scaled Agile Framework.

## Connect to a project with other clients

Aside from connecting via a web browser, you can connect to a project from the following clients:

- [Visual Studio \(Professional, Enterprise, Test Professional\)](#) ↗
- [Visual Studio Code](#) ↗
- [Visual Studio Community](#) ↗
- [Office Excel](#)
- [Test & Feedback extension](#)
- [Microsoft Feedback Client](#)

For more information, see [Compatibility with Azure DevOps Server versions](#).

## Key concepts

Use the following index to quickly access concepts and tasks related to managing projects and teams.

- [About projects](#)
- [About teams](#)
- [Access levels](#)
- [Area paths](#)
- [Dashboards](#)
- [Notifications and subscriptions](#)
- [GitHub connections](#)
- [Iteration paths](#)
- [Permissions](#)
- [Process \(Inherited\)](#)
- [Project resources viewable by members](#)
- [Project Wiki](#)
- [Project-level permissions](#)
- [Project-level security groups](#)
- [Project and process object limits](#)
- [Projects page](#)
- [Public vs private projects](#)
- [Security groups](#)

- Service hooks
- Service visibility
- Summary page

## User and administrative tasks

Several of the following tasks require permissions granted to a member of the Project Administrators group or a team administrator.

- Add Git repository
- Add project administrators
- Add project dashboard
- Add project members
- Add security groups
- Add team administrators
- Add team members
- Add/manage service hooks
- Connect to a project
- Connect to GitHub
- Create project
- Delete project
- Edit project Summary
- Enable/disable project services
- Export list of projects
- Export list of teams
- Manage notifications
- Manage your project
- Navigate the Web portal
- Remove team
- Rename project
- Rename team
- Restore project
- Change user access levels
- Search across projects
- Set area paths
- Set favorites
- Set iteration paths
- Set project-level permissions
- Set project visibility
- Switch project, repository, team

# Frequently asked questions (FAQs)

**Q: Can I move or transfer a project to another organization or collection?**

A: Yes, but not without losing data. You can manually copy resources and leave some behind, or use a non-Microsoft tool.

**Q: What programmatic tools support projects?**

A. See [Projects REST API](#).

You can also use the [az devops project CLI](#).

## Related articles

- [Get started as an administrator](#)
- [Navigate the web portal](#)
- [Understand what you get with a project](#)
- [Understand differences between Azure DevOps](#)

ⓘ Note: The author created this article with assistance from AI. [Learn more](#)

---

## Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

# Marketplace & Extensibility documentation

Discover, manage, develop extensions, and widgets for integration with Azure DevOps.

## Discover & manage Marketplace extensions

### CONCEPT

[Learn about Azure DevOps Marketplace](#)

### HOW-TO GUIDE

[Request extensions](#)

[Install extensions](#)

[Manage extension permissions](#)

## Develop extensions

### QUICKSTART

[Develop a web extension](#)

[Extension samples](#)

[Extensibility points](#)

### TUTORIAL

[Create a custom pipelines task](#)

## Integrate with Slack or Microsoft Teams

### HOW-TO GUIDE

[Use Azure Boards with Slack](#)

[Use Azure Pipelines with Slack](#)

## Integrate with Service hooks

### OVERVIEW

[Integrate with service hooks](#)

### TUTORIAL

[Create a service hook with Microsoft Teams](#)

[Create a service hook with WebHooks](#)

## Building applications on Azure DevOps

### OVERVIEW

[Learn about building applications](#)

# What is DevOps?

Article • 01/25/2023

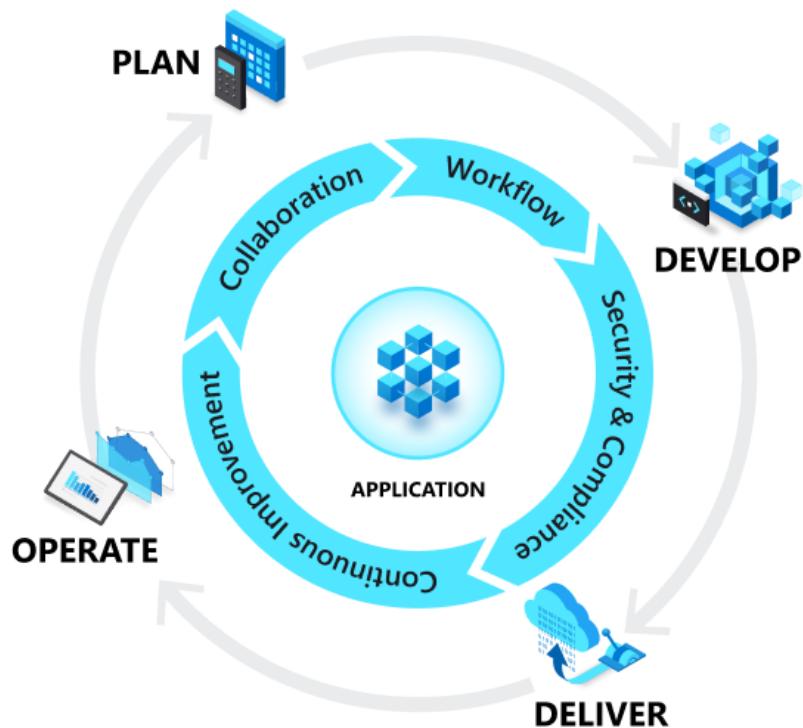
DevOps combines development (Dev) and operations (Ops) to unite people, process, and technology in application planning, development, delivery, and operations. DevOps enables coordination and collaboration between formerly siloed roles like development, IT operations, quality engineering, and security.

Teams adopt DevOps culture, practices, and tools to increase confidence in the applications they build, respond better to customer needs, and achieve business goals faster. DevOps helps teams continually provide value to customers by producing better, more reliable products.

## DevOps and the application lifecycle

DevOps influences the [application lifecycle](#) throughout its **planning**, **development**, **delivery**, and **operations** phases. Each phase relies on the other phases, and the phases aren't role-specific. A DevOps culture involves all roles in each phase to some extent.

The following diagram illustrates the phases of the DevOps application lifestyle:



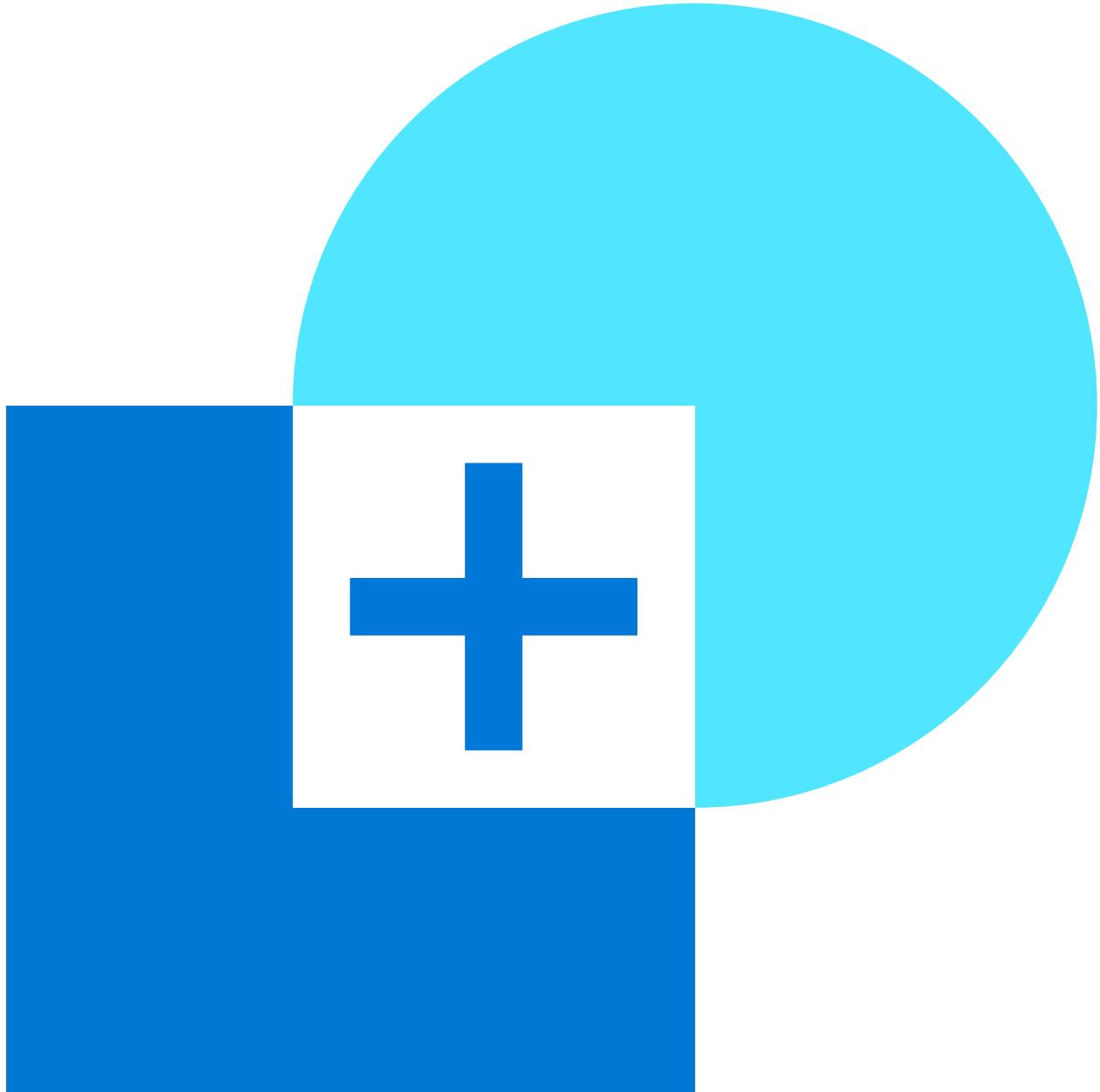
## DevOps goals and benefits

When a team adopts DevOps culture, practices, and tools, they can achieve amazing things:



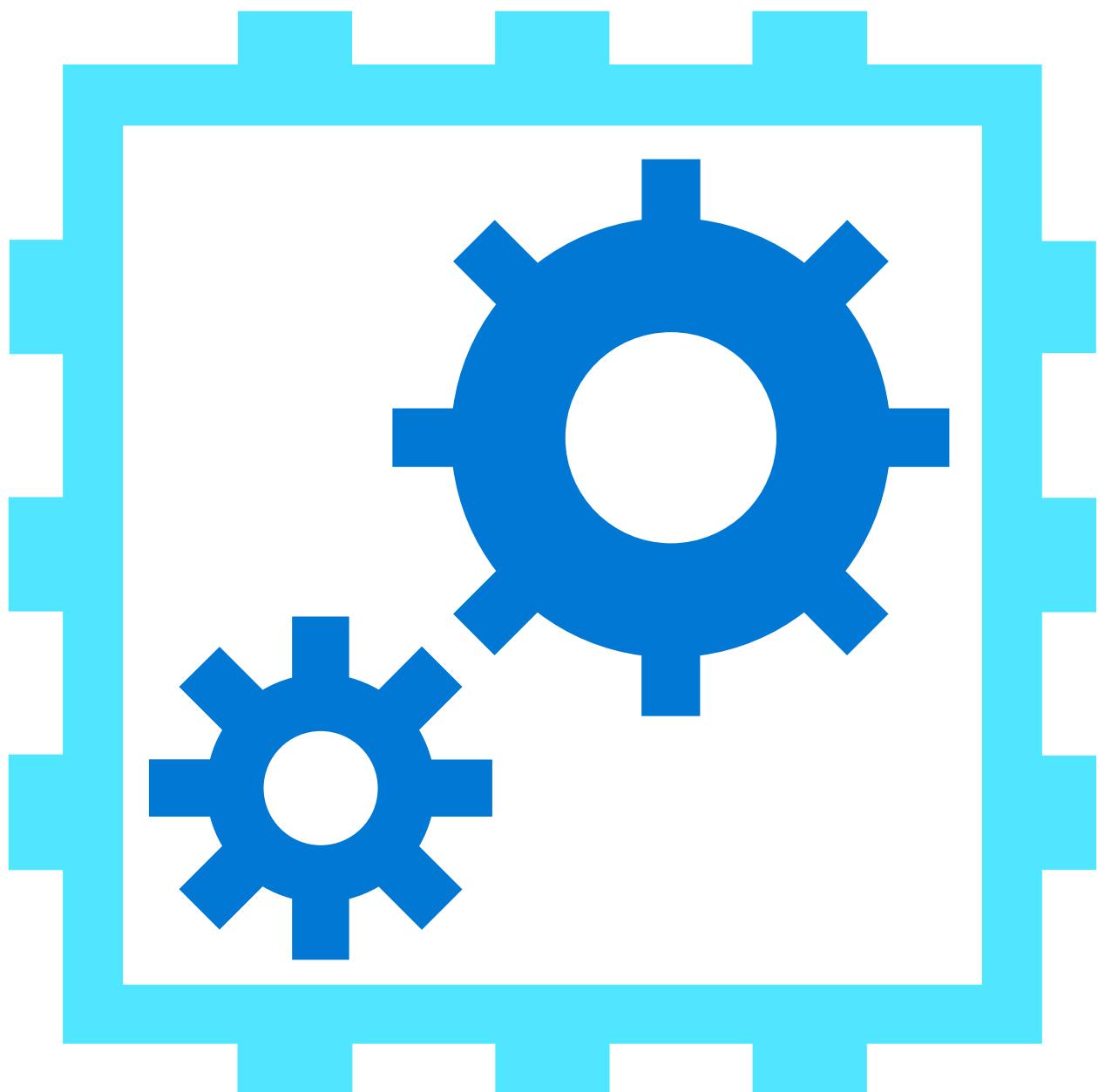
## Accelerate time to market

Through increased efficiencies, improved team collaboration, automation tools, and continuous deployment--teams are able to rapidly reduce the time from product inception to market launch.



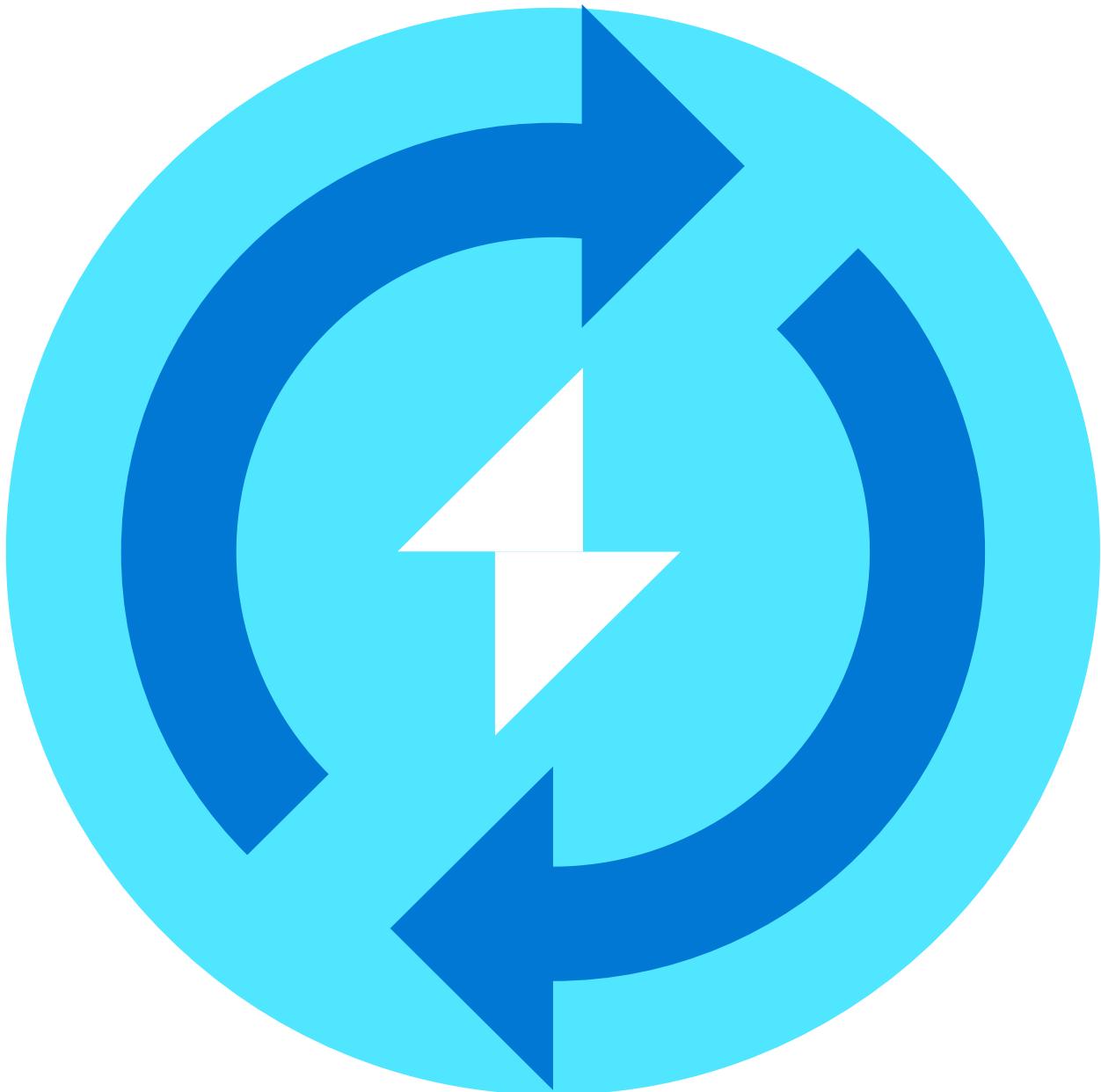
## Adapt to the market and competition

A DevOps culture demands teams have a customer-first focus. By marrying agility, team collaboration, and focus on the customer experience, teams can continuously deliver value to their customers and increase their competitiveness in the marketplace.



## Maintain system stability and reliability

By adopting continuous improvement practices, teams are able to build in increased stability and reliability of the products and services they deploy. These practices help reduce failures and risk.



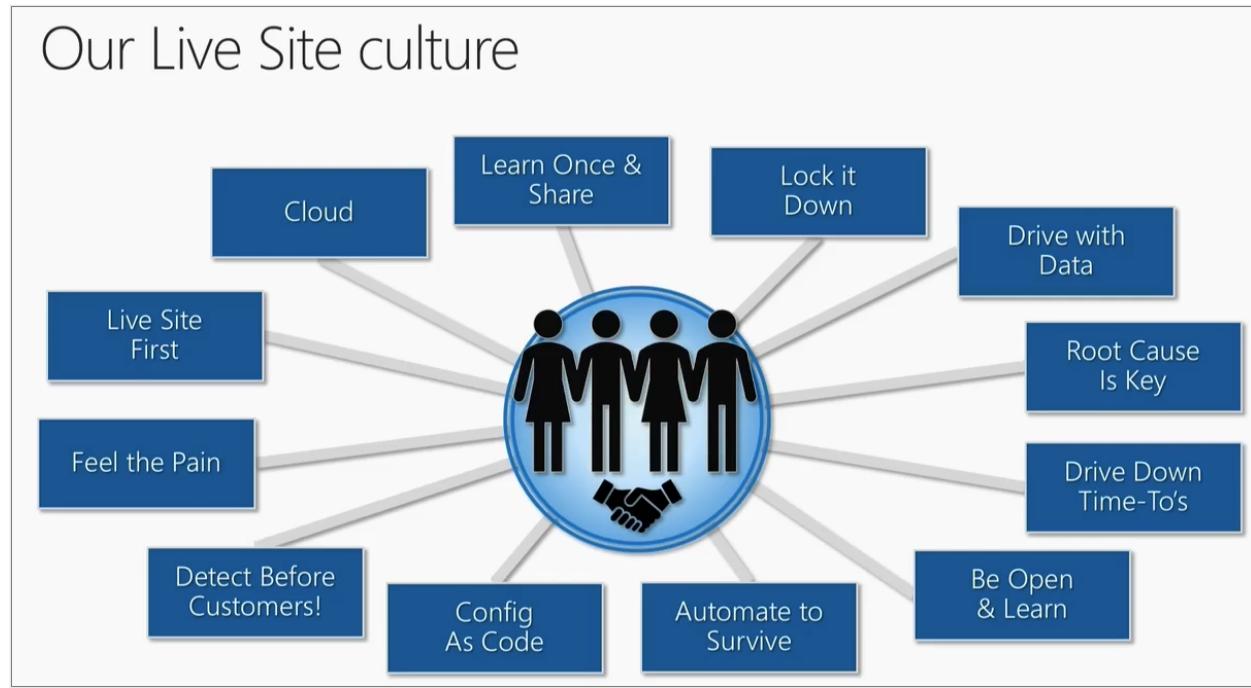
## Improve the mean time to recovery

The *mean time to recovery* metric indicates how long it takes to recover from a failure or breach. To manage software failures, security breaches, and continuous improvement plans, teams should measure and work to improve this metric.

## Adopt a DevOps culture

To fully implement DevOps, you must adopt a DevOps culture. Cultivating a DevOps culture requires deep changes in the way people work and collaborate. When organizations commit to a DevOps culture, they create an environment for high-performing teams to evolve. While adopting DevOps practices automates and optimizes processes through technology, without a shift to a DevOps culture within the organization and its people, you won't gain the full benefits of DevOps.

The following image captures key aspects of Microsoft's live site culture.



The following practices are key components of a DevOps culture:

- **Collaboration, visibility, and alignment:** A hallmark of a healthy DevOps culture is collaboration between teams. Collaboration starts with visibility. Development, IT, and other teams should share their DevOps processes, priorities, and concerns with each other. By planning their work together, they are better positioned to align on goals and measures of success as they relate to the business.
- **Shifts in scope and accountability:** As teams align, they take ownership and become involved in other lifecycle phases—not just the ones central to their roles. For example, developers become accountable not only to the innovation and quality established in the develop phase, but also to the performance and stability their changes bring in the operate phase. At the same time, IT operators are sure to include governance, security, and compliance in the plan and develop phase.
- **Shorter release cycles:** DevOps teams remain agile by releasing software in short cycles. Shorter release cycles make planning and risk management easier since progress is incremental, which also reduces the impact on system stability. Shortening the release cycle also allows organizations to adapt and react to evolving customer needs and competitive pressure.
- **Continuous learning:** High-performing DevOps teams establish a growth mindset. They fail fast and incorporate learnings into their processes. They strive to continually improve, increase customer satisfaction, and accelerate innovation and market adaptability.

## Implement DevOps practices

You implement DevOps by following DevOps practices (described in the sections that follow) throughout the application lifecycle. Some of these practices help accelerate, automate, and improve a specific phase. Others span several phases, helping teams create seamless processes that help improve productivity.

## Continuous integration and continuous delivery (CI/CD)

Continuous Integration (CI) is the practice used by development teams to automate, merge, and test code. CI helps to catch bugs early in the development cycle, which makes them less expensive to fix. Automated tests execute as part of the CI process to ensure quality. CI systems produce artifacts and feed them to release processes to drive frequent deployments.

Continuous Delivery (CD) is a process by which code is built, tested, and deployed to one or more test and production environments. Deploying and testing in multiple environments increases quality. CD systems produce deployable artifacts, including infrastructure and apps. Automated release processes consume these artifacts to release new versions and fixes to existing systems. Systems that monitor and send alerts run continually to drive visibility into the entire CD process.

## Version Control

Version control is the practice of managing code in versions—tracking revisions and change history to make code easy to review and recover. This practice is usually implemented using version control systems such as Git, which allow multiple developers to collaborate in authoring code. These systems provide a clear process to merge code changes that happen in the same files, handle conflicts, and roll back changes to earlier states.

The use of version control is a fundamental DevOps practice, helping development teams work together, divide coding tasks between team members, and store all code for easy recovery if needed. Version control is also a necessary element in other practices such as continuous integration and infrastructure as code.

## Agile software development

Agile is a software development approach that emphasizes team collaboration, customer and user feedback, and high adaptability to change through short release cycles. Teams that practice Agile provide continual changes and improvements to customers, collect their feedback, then learn and adjust based on customer wants and needs. Agile is substantially different from other more traditional frameworks such as

waterfall, which includes long release cycles defined by sequential phases. Kanban and Scrum are two popular frameworks associated with Agile.

## Infrastructure as code

Infrastructure as code defines system resources and topologies in a descriptive manner that allows teams to manage those resources as they would code. Those definitions can also be stored and versioned in version control systems, where they can be reviewed and reverted—again like code.

Practicing infrastructure as code helps teams deploy system resources in a reliable, repeatable, and controlled way. Infrastructure as code also helps automate deployment and reduces the risk of human error, especially for complex large environments. This repeatable, reliable solution for environment deployment lets teams maintain development and testing environments that are identical to production. Duplicating environments to different data centers and cloud platforms likewise becomes simpler and more efficient.

## Configuration management

Configuration management refers to managing the state of resources in a system including servers, virtual machines, and databases. Using configuration management tools, teams can roll out changes in a controlled, systematic way, reducing the risks of modifying system configuration. Teams use configuration management tools to track system state and help avoid configuration drift, which is how a system resource's configuration deviates over time from the desired state defined for it.

Along with infrastructure as code, it's easy to template and automate system definition and configuration, which help teams operate complex environments at scale.

## Continuous monitoring

Continuous monitoring means having full, real-time visibility into the performance and health of the entire application stack. This visibility ranges from the underlying infrastructure running the application to higher-level software components. Visibility is accomplished through the collection of telemetry and metadata and setting of alerts for predefined conditions that warrant attention from an operator. Telemetry comprises event data and logs collected from various parts of the system, which are stored where they can be analyzed and queried.

High-performing DevOps teams ensure they set actionable, meaningful alerts and collect rich telemetry so they can draw insights from vast amounts of data. These insights help the team mitigate issues in real time and see how to improve the application in future development cycles.

## Planning

In the planning phase, DevOps teams ideate, define, and describe the features and capabilities of the applications and systems they plan to build. Teams track task progress at low and high levels of granularity, from single products to multiple product portfolios. Teams use the following DevOps practices to plan with [agility](#) and visibility:

- Create backlogs.
- Track bugs.
- Manage [Agile software development](#) with [Scrum](#).
- Use [Kanban boards](#).
- Visualize progress with dashboards.

For an overview of the several lessons learned and practices Microsoft adopted to support DevOps planning across the company's software teams, see [How Microsoft plans with DevOps](#).

## Development

The development phase includes all aspects of developing software code. In this phase, DevOps teams do the following tasks:

- [Select a development environment](#).
- Write, test, review, and integrate the code.
- Build the code into artifacts to deploy into various environments.
- Use [version control](#), usually [Git](#), to collaborate on code and work in parallel.

To innovate rapidly without sacrificing quality, stability, and productivity, DevOps teams:

- Use highly productive tools.
- Automate mundane and manual steps.
- Iterate in small increments through [automated testing](#) and [continuous integration \(CI\)](#).

For an overview of the development practices Microsoft adopted to support their shift to DevOps, see [How Microsoft develops with DevOps](#).

# Deliver

Delivery is the process of consistently and reliably deploying applications into production environments, ideally via [continuous delivery \(CD\)](#).

In the delivery phase, DevOps teams:

- Define a release management process with clear manual approval stages.
- Set automated gates to move applications between stages until final release to customers.
- Automate delivery processes to make them scalable, repeatable, controlled, and [well-tested](#).

Delivery also includes deploying and configuring the delivery environment's foundational infrastructure. DevOps teams use technologies like [infrastructure as code \(IaC\)](#), [containers](#), and [microservices](#) to deliver fully governed infrastructure environments.

[Safe deployment practices](#) can identify issues before they affect the customer experience. These practices help DevOps teams deliver frequently with ease, confidence, and peace of mind.

Core DevOps principles and processes Microsoft evolved to provide efficient delivery systems are described in [How Microsoft delivers software with DevOps](#).

# Operations

The operations phase involves maintaining, [monitoring](#), and troubleshooting applications in production environments, including hybrid or public clouds like [Azure](#). DevOps teams aim for [system reliability](#), high availability, [strong security](#), and [zero downtime](#).

Automated delivery and safe deployment practices help teams identify and mitigate issues quickly when they occur. Maintaining vigilance requires rich telemetry, actionable alerting, and full visibility into applications and underlying systems.

Practices Microsoft uses to operate complex online platforms are described in [How Microsoft operates reliable systems with DevOps](#).

# Next steps

- [Plan efficient workloads with DevOps](#)

- Develop modern software with DevOps
- Deliver quality services with DevOps
- Operate reliable systems with DevOps

## Other resources

- [DevOps solutions on Azure ↗](#)
- [The DevOps journey at Microsoft ↗](#)
- [Start doing DevOps with Azure ↗](#)
- [Security in DevOps \(DevSecOps\)](#)
- [What is platform engineering?](#)

## Training and Certifications

- [Get started with Azure DevOps](#)
- [Introduce DevOps Dojo: Create efficiencies that support your business](#)
- [AZ-400: Get started on a DevOps transformation journey](#)
- [Facilitate communication and collaboration](#)
- [Exam AZ-400: Designing and Implementing Microsoft DevOps Solutions](#)
- [AZ-400: Implement security and validate code bases for compliance](#)

# What is Agile?

Article • 11/28/2022



Agile is a term that describes approaches to software development that emphasize incremental delivery, team collaboration, continual planning, and continual learning. The term *Agile* was coined in 2001 in the [Agile Manifesto](#). The manifesto set out to establish principles to guide a better approach to software development. At its core, the manifesto declares four value statements that represent the foundation of the Agile movement. As written, the manifesto states:

We have come to value:

- Individuals and interactions over processes and tools.
- Working software over comprehensive documentation.
- Customer collaboration over contract negotiation.
- Responding to change over following a plan.

The manifesto doesn't imply that the items on the right side of these statements aren't important or needed. Rather, items on the left are simply more valued.

## Agile methods and practices

It's important to understand that Agile isn't a *thing*. You don't *do Agile*. Rather, Agile is a mindset that drives an approach to software development. Because there's no single approach that works for all situations, the term *Agile* has come to represent various methods and practices that align with the value statements in the manifesto.

Agile methods, which are often called frameworks, are comprehensive approaches to phases of the DevOps lifecycle: planning, development, delivery, and operations. They prescribe a method for accomplishing work, with clear guidance and principles.

[Scrum](#) is the most common Agile framework, and the one that most people start with. Agile practices, on the other hand, are techniques that are applied during phases of the software development lifecycle.

- [Planning Poker](#) is a collaborative estimation practice that's designed to encourage team members to share their understanding of what *done* means. Many people find the process fun, and it has proven to help foster teamwork and better estimates.
- [Continuous integration](#) (CI) is a common Agile engineering practice that involves integrating code changes into the main branch frequently. An automated build verifies changes. As a result, there's a reduction in integration debt and a continually shippable main branch.

These practices, like all Agile practices, carry the *Agile* label, because they're consistent with the principles in the Agile manifesto.

## What Agile isn't

As Agile has gained popularity, many stereotypes and misinterpretations have cast a negative shadow on its effectiveness. It's easy to say "Yes, we're doing Agile," without any accountability. Keeping this point in mind, consider a few things that Agile isn't.

- Agile isn't [cowboy coding](#). Agile shouldn't be confused with a "we'll figure it out as we go" approach to software development. Such an idea couldn't be further from the truth. Agile requires both a [definition of done](#) and explicit value that's delivered to customers in every sprint. While Agile values autonomy for individuals and teams, it emphasizes aligned autonomy to ensure that the increased autonomy produces increased value.
- Agile isn't without rigor and planning. On the contrary, Agile methodologies and practices typically emphasize discipline in planning. The key is continual planning throughout the project, not just planning up front. Continual planning ensures that the team can learn from the work that they execute. Through this approach, they maximize the return on investment (ROI) of planning.

"Plans are worthless, but planning is everything." — Dwight D. Eisenhower

- Agile isn't an excuse for the lack of a roadmap. This misconception has probably done the most harm to the Agile movement overall. Organizations and teams that

follow an Agile approach absolutely know where they're going and the results that they want to achieve. Recognizing change as part of the process is different from pivoting in a new direction every week, sprint, or month.

- Agile isn't development without specifications. It's necessary in any project to keep your team aligned on *why* and *how* work happens. An Agile approach to specs includes ensuring that specs are *right-sized*, and that they reflect appropriately how the team sequences and delivers work.
- Agile isn't incapable of accommodating unplanned work and other interruptions. It's important to complete sprints on schedule. But just because an issue comes up that sidetracks development doesn't mean that a sprint has to fail. Teams can plan for interruptions by designating resources ahead of time for problems and unexpected issues. Then they can address those issues but stay on track with development.
- Agile isn't inappropriate for large organizations. A common complaint is that collaboration, a key component of Agile methodologies, is difficult in large teams. Another gripe is that scalable approaches to Agile introduce structure and methods that compromise flexibility. In spite of these misconceptions, it's possible to scale Agile principles successfully. For information about overcoming these difficulties, see [Scaling Agile to large teams](#).
- Agile isn't inefficient. To adapt to customers' changing needs, developers invest time each iteration to demonstrate a working product and collect feedback. It's true that these efforts reduce the time that they spend on development. But incorporating customer requests early on saves significant time later. When features stay aligned with the customer's vision, developers avoid major overhauls down the line.
- Agile isn't a poor fit for today's applications, which often center on data streaming. Such projects typically involve more data modeling and extract-transform-load (ETL) workloads than user interfaces. This fact makes it hard to demonstrate usable software on a consistent, tight schedule. But by adjusting goals, developers can still use an Agile approach. Instead of working to accomplish tasks each iteration, developers can focus on running data experiments. Instead of presenting a working product every few weeks, they can aim to better understand the data.

## Why Agile?

So why would anyone consider an Agile approach? It's clear that the rules of engagement around building software have fundamentally changed in the last 10-15 years. Many of the activities look similar, but the landscape and environments where we apply them are noticeably different.

- Compare what it's like to purchase software today with the early 2000s. How often do people drive to the store to buy business software?
- Consider how feedback is collected from customers about products. How did a team understand what people thought about their software before social media?
- Consider how often a team desires to update and improve the software that they deliver. Annual updates are no longer feasible against modern competition.

Forrester's Diego Lo Guidice says it best in his blog, *Transforming Application Delivery* (October, 2020).

"Everything has dramatically changed. Sustainability, besides green and clean, means that what we build today has to be easily and quickly changed tomorrow. Strategic plans are short-term, and planning and change are continuous." — Diego Lo Guidice, Forrester

The rules have changed, and organizations around the world now adapt their approach to software development accordingly. Agile methods and practices don't promise to solve every problem. But they do promise to establish a culture and environment where solutions emerge through collaboration, continual planning and learning, and a desire to ship high-quality software more often.

## Next steps

Deciding to take the Agile route to software development can introduce some interesting opportunities for enhancing your DevOps process. One key set of considerations focuses on how [Agile development](#) compares and contrasts with an organization's current approach.

# What is Git?

Article • 11/28/2022

Git has become the worldwide standard for version control. So what exactly is it?

Git is a distributed version control system, which means that a local clone of the project is a complete version control repository. These fully functional local repositories make it easy to work offline or remotely. Developers commit their work locally, and then sync their copy of the repository with the copy on the server. This paradigm differs from centralized version control where clients must synchronize code with a server before creating new versions of code.

Git's flexibility and popularity make it a great choice for any team. Many developers and college graduates already know how to use Git. Git's user community has created resources to train developers and Git's popularity make it easy to get help when needed. Nearly every development environment has Git support and Git command line tools implemented on every major operating system.

## Git basics

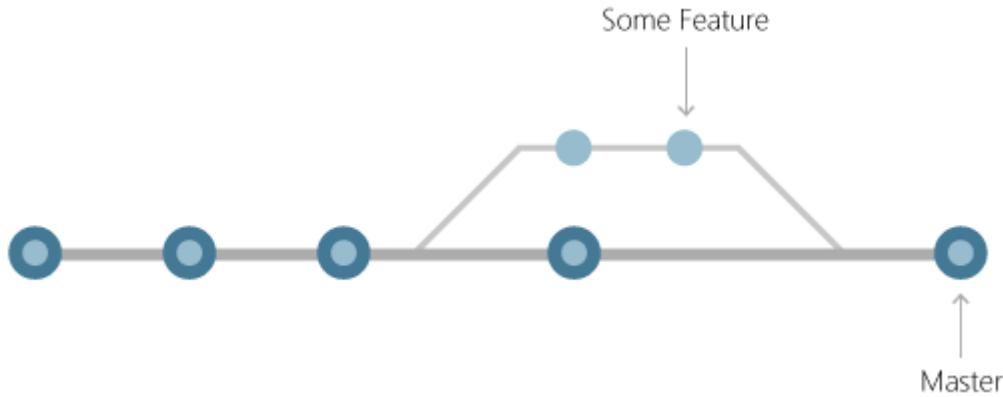
Every time work is saved, Git creates a commit. A commit is a snapshot of all files at a point in time. If a file hasn't changed from one commit to the next, Git uses the previously stored file. This design differs from other systems that store an initial version of a file and keep a record of deltas over time.



Commits create links to other commits, forming a graph of the development history. It's possible to revert code to a previous commit, inspect how files changed from one commit to the next, and review information such as where and when changes were made. Commits are identified in Git by a unique cryptographic hash of the contents of the commit. Because everything is hashed, it's impossible to make changes, lose information, or corrupt files without Git detecting it.

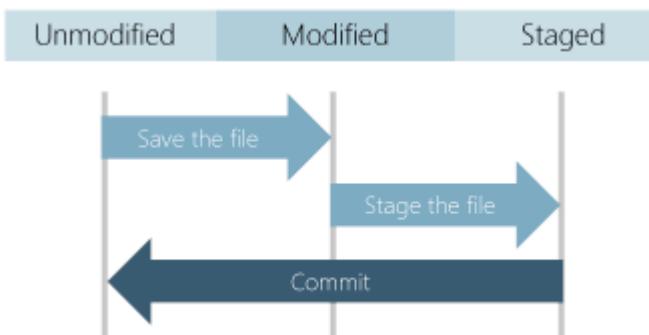
## Branches

Each developer saves changes to their own local code repository. As a result, there can be many different changes based off the same commit. Git provides tools for isolating changes and later merging them back together. Branches, which are lightweight pointers to work in progress, manage this separation. Once work created in a branch is finished, it can be merged back into the team's main (or trunk) branch.



## Files and commits

Files in Git are in one of three states: modified, staged, or committed. When a file is first modified, the changes exist only in the working directory. They aren't yet part of a commit or the development history. The developer must *stage* the changed files to be included in the commit. The staging area contains all changes to include in the next commit. Once the developer is happy with the staged files, the files are packaged as a *commit* with a message describing what changed. This commit becomes part of the development history.



Staging lets developers pick which file changes to save in a commit in order to break down large changes into a series of smaller commits. By reducing the scope of commits, it's easier to review the commit history to find specific file changes.

## Benefits of Git

The benefits of Git are many.

## Simultaneous development

Everyone has their own local copy of code and can work simultaneously on their own branches. Git works offline since almost every operation is local.

## Faster releases

Branches allow for flexible and simultaneous development. The main branch contains stable, high-quality code from which you release. Feature branches contain work in progress, which are merged into the main branch upon completion. By separating the release branch from development in progress, it's easier to manage stable code and ship updates more quickly.

## Built-in integration

Due to its popularity, Git integrates into most tools and products. Every major IDE has built-in Git support, and many tools support continuous integration, continuous deployment, automated testing, work item tracking, metrics, and reporting feature integration with Git. This integration simplifies the day-to-day workflow.

## Strong community support

Git is open-source and has become the de facto standard for version control. There is no shortage of tools and resources available for teams to leverage. The volume of community support for Git compared to other version control systems makes it easy to get help when needed.

## Git works with any team

Using Git with a source code management tool increases a team's productivity by encouraging collaboration, enforcing policies, automating processes, and improving visibility and traceability of work. The team can settle on individual tools for version control, work item tracking, and continuous integration and deployment. Or, they can choose a solution like [GitHub](#) or [Azure DevOps](#) that supports all of these tasks in one place.

## Pull requests

Use [pull requests](#) to discuss code changes with the team before merging them into the main branch. The discussions in pull requests are invaluable to ensuring code quality.

and increase knowledge across your team. Platforms like GitHub and Azure DevOps offer a rich pull request experience where developers can browse file changes, leave comments, inspect commits, view builds, and vote to approve the code.

## Branch policies

Teams can configure GitHub and Azure DevOps to enforce consistent workflows and process across the team. They can set up [branch policies](#) to ensure that pull requests meet requirements before completion. Branch policies protect important branches by preventing direct pushes, requiring reviewers, and ensuring clean builds.

## Next steps

[Install and set up Git](#)