

Contents

[Azure DevOps manage & configure resources documentation](#)

[About settings](#)

[Get started as an administrator](#)

[User preferences](#)

[Set user preferences](#)

[Enable preview features](#)

[Set personal favorites](#)

[Configure personal notifications](#)

[Authentication](#)

[Authenticate access with personal access tokens](#)

[Authorize access to REST APIs with OAuth 2.0](#)

[Use SSH key authentication](#)

[Revoke users' PATs - for admins](#)

[Teams](#)

[Manage teams](#)

[When to add a team or project](#)

[About teams & Agile tools](#)

[Quickstarts](#)

[Define area paths & assign to a team](#)

[Define iteration paths \(sprints\) & configure team iterations](#)

[Add a team](#)

[Add a team administrator](#)

[Add users to a project or team](#)

[Tutorials](#)

[Portfolio management](#)

[Configure a hierarchy of teams](#)

[Concepts](#)

[Area & iteration paths](#)

[How-to Guides](#)

- [Configure team tools](#)
- [Select backlog levels](#)
- [Show bugs on backlogs & boards](#)
- [Set working days](#)
- [Set team favorites](#)
- [Projects](#)
 - [Manage projects](#)
 - [About projects](#)
 - [What do I get with a project?](#)
- [Quickstarts](#)
 - [Share your project vision](#)
 - [Connect a project to GitHub](#)
- [Concepts](#)
 - [Resources granted to members](#)
- [How-to guides](#)
 - [Create a project](#)
 - [Rename a project](#)
 - [Delete a project](#)
 - [Restore a project](#)
 - [Change service visibility](#)
 - [Set project visibility](#)
 - [Save project data](#)
 - [Connect a project](#)
- [Troubleshooting](#)
 - [Create a project](#)
 - [Rename a project](#)
 - [Add administrators](#)
 - [Set up Visual Studio](#)
 - [Troubleshoot connection](#)
 - [TF31002: Unable to connect](#)
- [Organizations](#)
 - [Manage organizations](#)

[About managing organizations](#)

[Access with Azure AD](#)

[Create your organization or project collection](#)

[Concepts](#)

[Plan your org structure](#)

[Project member resources](#)

[How-to guides](#)

[Manage your organization](#)

[Change organization owner](#)

[Rename organization](#)

[Delete organization](#)

[Recover organization](#)

[Change organization location](#)

[Add privacy policy URL](#)

[Manage access](#)

[Add users to your organization](#)

[Manage users](#)

[Manage conditional access](#)

[Authenticate with PATs](#)

[Revoke user PATs - for admins](#)

[Change app access policies](#)

[Delete users from organization](#)

[Add external users](#)

[Access with Azure AD](#)

[Connect organization to Azure AD](#)

[Change Azure AD connection](#)

[Disconnect from Azure AD](#)

[Manage groups](#)

[Add users to Azure AD](#)

[Delete users connected to Azure AD](#)

[FAQ](#)

[Manage group-based licensing](#)

[Assign access levels and extensions](#)
[Remove direct assignments](#)

Troubleshooting

[Create organization](#)
[Add and delete organization users](#)
[Add team members](#)
[Access with Azure AD](#)
[Change app access](#)
[Add administrators](#)
[Change organization ownership](#)
[Delete and restore organization](#)
[Set up Visual Studio](#)
[Manage group-based licensing](#)
[Access with Azure AD](#)

Billing

[Billing](#)
[Billing overview](#)
[Quickstarts](#)
[Set up billing](#)
[Buy Basic for users](#)
[Buy Basic + Test Plans for users](#)
[Buy CI/CD](#)
[Buy Azure Artifacts](#)
[Try Azure Test Plans for free](#)
[Buy cloud-based load testing](#)

How-to guides

[Add user to make purchases](#)
[Change Azure subscription](#)
[Buy Azure DevOps Server CALs or Test](#)
[Billing FAQ](#)
[Guidance for Cloud Solution Providers](#)
[CSPs: Buy Azure DevOps](#)

[CSPs: Buy and manage Visual Studio subscriptions](#)

[CSPs: Buy App Center resources](#)

Security & identity

[Security & identity](#)

[About security and identity](#)

[Quickstart](#)

[View permissions](#)

[Look up the organization owner or a project administrator](#)

[Add users to a project or team](#)

[Set Git or TFVC repository permissions](#)

[Add administrators or set permissions at the project or collection level](#)

Tutorials

[Set up Active Directory or Azure AD](#)

[Add AD/Azure AD security groups to built-in security groups](#)

[Change individual permissions](#)

[Grant or restrict permissions to select tasks](#)

[Remove user accounts](#)

[Get started as a Stakeholder](#)

Concepts

[About permissions and groups](#)

[About security roles](#)

[About access levels](#)

[Azure Active Directory groups](#)

[Active Directory groups](#)

How-to guides

[Add users to Azure DevOps Services](#)

[Change access levels](#)

[Export user list](#)

[Set permissions for an object or role](#)

[Set dashboard permissions](#)

[Set Git branch permissions](#)

[Set pipeline permissions](#)

[Provide Stakeholders access to edit pipelines](#)

[Set package feed permissions](#)

[Set Wiki permissions](#)

[Set work tracking and plan permissions](#)

[Set feedback permissions](#)

[Set permissions to manage extensions](#)

[Set SQL Server report permissions](#)

[Set SharePoint project portal permissions](#)

[Sign-in to the web or a client](#)

[Authenticate access with personal access tokens](#)

[Revoke user PATs - for admins](#)

Troubleshooting

[Add and delete users](#)

[Add team members](#)

[Access with Azure AD](#)

[Change app access](#)

[Add administrators](#)

[Manage group-based licensing](#)

[Resolve connection issues](#)

[TF31002: Unable to connect](#)

[Network connections](#)

[Trace permissions](#)

Reference

[Default permissions & access](#)

[Permission lookup guide](#)

[Permissions & groups](#)

[Git permissions prior to TFS 2017 Update 1](#)

[Web site settings and security](#)

[Azure DevOps Services](#)

[Data protection overview](#)

[Data location](#)

[Credential storage](#)

- [Add IP addresses and URLs to allow list](#)
 - [TFSSecurity command](#)
 - [Security glossary](#)
- [Notifications](#)
 - [Notifications](#)
 - [About notifications](#)
 - [Navigating the UI](#)
- [Concepts](#)
 - [Events and notifications](#)
 - [How email recipients are determined](#)
- [Tutorials](#)
 - [Follow work & pull requests](#)
 - [Manage personal notifications](#)
 - [Manage team and group notifications](#)
- [How-to guides](#)
 - [Manage organization notifications](#)
 - [Manage organization default delivery settings](#)
 - [View notification statistics for your organization](#)
 - [Change your preferred email address](#)
 - [Use subscription logging for troubleshooting](#)
 - [Exclude yourself from notification of events initiated by you](#)
 - [Use @mentions to further discussion](#)
 - [Use #ID to link to work items](#)
 - [Send notifications to third-party services \(Slack, Teams, etc\)](#)
- [Troubleshooting](#)
 - [Why am I not getting an email](#)
 - [Why am I getting this email](#)
 - [Why are my emails delayed](#)
 - [Contacting support](#)
- [Reference](#)
 - [Default notifications](#)
 - [Events](#)

[Default permissions \(Security\)](#)

[FAQs](#)

[Additional settings](#)

[DevOps settings](#)

[Build and release](#)

[Agent pools & queues](#)

[Service endpoints](#)

[Retention & limits](#)

[Deployment pools & groups](#)

[Code](#)

[Create & manage Git repositories](#)

[Manage Git branch policies](#)

[Manage repository permissions](#)

[Add TFVC Check-In Policies](#)

[Test](#)

[Set test retention policies](#)

[Audit](#)

[Access auditing](#)

[Reference](#)

[Features index](#)

[REST API reference](#)

[Area and iteration paths](#)

[Authentication guidance](#)

[Teams](#)

[Projects](#)

[Teams](#)

[Organizations](#)

[Security](#)

[Permissions](#)

[Processes](#)

[Notifications](#)

[Resources](#)

[Add an alternate account to your Visual Studio subscription](#)

[Marketplace & extensibility](#)

[Git](#)

[Work items](#)

[Public projects](#)

[Process customization](#)

[Service hooks](#)

[Web portal navigation](#)

Azure DevOps Manage & Configure Resources Documentation

Configure resources and manage settings for an organization, project, team, or user. For information on customizing Azure Boards and Agile tools—such as backlogs, boards, and work tracking artifacts—see, [Process Customization](#).

User preferences

[Set user preferences](#)

[Enable preview features](#)

[Set personal favorites](#)

[Configure personal notifications](#)

Teams

[Teams and Agile tools](#)

[Configure team tools](#)

[Define team area paths](#)

[Configure team iterations](#)

[Add a team](#)

[Add a team administrator](#)

[Add users to a team](#)

Projects

[About projects and scaling your organization](#)

[Create a project](#)

[Manage your project](#)

[Define area paths](#)

[Define iterations](#)

[Add project administrators or set project-level permissions](#)

[Add users to a project](#)

[Connect to a project](#)

Organizations

[About organizations](#)

[Create an organization](#)

[Connect your organization to Azure Active Directory](#)

Billing

[Billing overview](#)

[Set up billing](#)

Permissions, Security, & Identity

[About security & identity](#)

[Default permissions & access](#)

[View permissions](#)

[Change individual or group permissions](#)

Notifications

[About notifications](#)

[Events, subscriptions, and notifications](#)

[Manage personal notifications](#)

[Manage notifications for a team](#)

DevOps Settings

[About settings](#)

[Manage your project](#)

[Change service visibility](#)

User preferences

[Set user preferences](#)

[Set personal favorites](#)

[Configure personal notifications](#)

Teams

[Teams and Agile tools](#)

[Configure team tools](#)

[Define team area paths](#)

[Configure team iterations](#)

[Add a team](#)

[Add a team administrator](#)

[Add users to a team](#)

Projects

- [About projects and scaling your deployment](#)
- [Create a project](#)
- [Manage your project](#)
- [Define area paths](#)
- [Define iterations](#)
- [Add project administrators or set project-level permissions](#)
- [Add users to a project](#)
- [Connect to a project](#)

Permissions, Security, & Identity

- [About security & identity](#)
- [Default permissions & access](#)
- [View permissions](#)
- [Change individual or group permissions](#)

Billing

- [Billing overview](#)
- [Set up billing](#)

Notifications

- [About notifications](#)
- [Events, subscriptions, and notifications](#)
- [Manage personal notifications](#)
- [Manage notifications for a team](#)

DevOps Settings

- [About settings](#)
- [Change service visibility](#)

User preferences

- [Set user preferences](#)
- [Set personal favorites](#)
- [Configure personal notifications](#)

Teams

[Teams and Agile tools](#)

[Configure team tools](#)

[Define team area paths](#)

[Configure team iterations](#)

[Add a team](#)

[Add a team administrator](#)

[Add users to a team](#)

Projects

[About projects and scaling your deployment](#)

[Create a project](#)

[Manage your project](#)

[Define area paths](#)

[Define iterations](#)

[Add project administrators or set project-level permissions](#)

[Add users to a project](#)

[Connect to a project](#)

Permissions, Security, & Identity

[About security & identity](#)

[Default permissions & access](#)

[View permissions](#)

[Change individual or group permissions](#)

Billing

[Billing overview](#)

[Set up billing](#)

Notifications

[About notifications](#)

[Events, subscriptions, and notifications](#)

[Manage personal notifications](#)

[Manage notifications for a team](#)

DevOps Settings

[About settings](#)

[Manage your project](#)

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

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You configure resources either for yourself, your team, a project, or your organization from an administrative **Settings** page. The settings you can configure depend on the security group or administrative role you belong to.

If you're just getting started as a project administrator, see [Get started as an administrator](#).

NOTE

You can delegate several tasks to a user with Stakeholder or Basic access by adding them to the Project Collection Administrators group. To learn more about Stakeholder access, see [About access levels, Stakeholder access](#).

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

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You configure resources either for yourself, your team, a project, or your project collection from a **Settings** page. The settings you can configure depend on the security group or administrative role you belong to.

User settings

Individual contributors can set their user preferences, enable features that are in preview, and manage their favorites and notifications.

Area	Supported Tasks	Notes
General	<ul style="list-style-type: none">Set your preferencesEnable preview features	For an overview of default permission assignments by role, see Default permissions and access .
Security	<ul style="list-style-type: none">View permissionsAdd an alternate account to your Visual Studio subscription	For an overview of default permission assignments by role, see Default permissions and access .
Authentication	<ul style="list-style-type: none">Authenticate access with personal access tokensAuthorize access to REST APIs with OAuth 2.0Use SSH key authentication	For an overview of supported authentication methods, see Authentication overview .
Favorites	<ul style="list-style-type: none">Set personal or team favorites	Favorites provide a quick way to navigate to backlogs, boards, dashboards, and more artifacts. Any member of the Contributors group or team member can set their own favorites. Team members can set team favorites.

Notifications	<ul style="list-style-type: none"> View your subscriptions, opt-out as needed Change your preferred email address Manage personal notifications 	Notifications alert you through email messages when changes occur to work items, code reviews, pull requests, source control files, builds, and more. When a project is created, a number of notifications are defined. If you want to opt out of these, you can.
----------------------	--	---

Team Administrator role and managing teams

Team administrators are tasked with configuring team resources which mostly correspond to Agile tools and dashboards. To configure team resources, you must be added as a [team administrator for the specific team](#), or be a member of the Project Administrators or Project Collection Administrators groups.

For a complete overview of all Agile tools that you can configure, see [Manage teams and configure team tools](#).

AREA	SUPPORTED TASKS	NOTES
Team profile	<ul style="list-style-type: none"> Add users to a project or specific team Add team admins 	Members of a team are included within the team group which can be used in queries and @mentions in pull requests and work item discussions.
Boards, Team configuration	<ul style="list-style-type: none"> Backlog levels Show bugs on backlogs & boards Set working days Configure area paths Select active iteration paths (sprints) Define work item templates 	For an overview of team resources, see About teams and Agile tools . You configure Kanban boards from the board view: Columns , Swimlanes , Cards , WIP limits .
Dashboards	<ul style="list-style-type: none"> Create team dashboards Set default team dashboard permissions, manage dashboard permissions 	New dashboards added to a project are associated with a team. The default permissions allow team members to create and edit dashboards for their team.
Notifications	<ul style="list-style-type: none"> Manage team notifications 	A number of team notifications are automatically defined when a team is added. To learn more about how notifications are managed, see About notifications .

Project Administrator role and managing projects

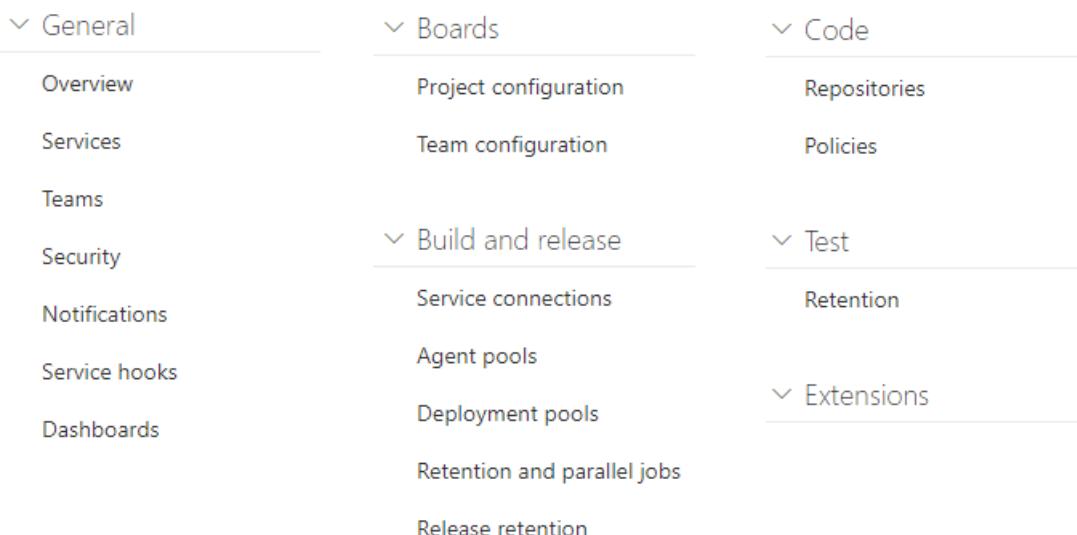
Members of the [Project Administrators group](#) are tasked with configuring resources for a project and managing permissions at the project-level. Note that members of the [Project Collection Administrators group](#) can configure team settings as well.

See also [Get started as an administrator](#).

Project settings

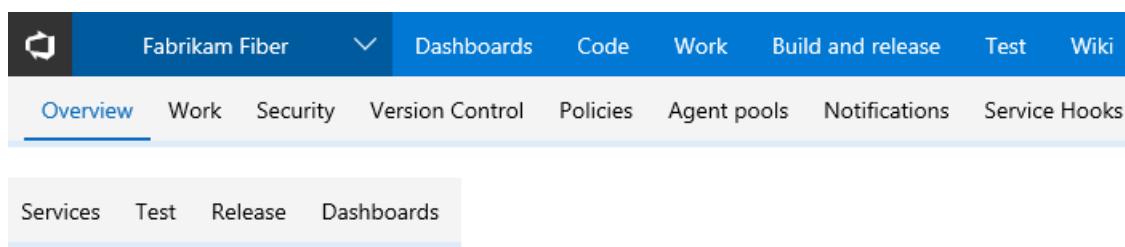
From the administrative **Project settings** pages, you can configure settings available from the tabs shown in the following image.

Project Settings > Overview



Project-level settings

From the administrative **Project settings** pages, you can configure settings available from the tabs shown in the following image.



NOTE

Project settings differ depending on your on-premises TFS version. Some settings aren't available for earlier versions of TFS.

AREA	SUPPORTED TASKS	NOTES
General	<ul style="list-style-type: none">Set project descriptionChange the project visibility, public or private (Azure DevOps Services only)	Update the project description or change its visibility.
Services	<ul style="list-style-type: none">Turn a service on or off	Services that aren't used by project members can be disabled so that they don't appear in the web portal. Turning a service off removes the service from the user interface for all project users. However, data defined for the service is preserved and available if you later decide to turn the service on.

Teams	<ul style="list-style-type: none"> • Add another team and team members • Add a team administrator 	<p>A default team is created when you create a project. You add a team when you want to provide a group of users in your organization a set of Agile tools which they have full ownership to configure and manage. Teams have access to a product backlog, portfolio backlogs, sprint backlogs, dashboards, team-scoped widgets, and more.</p> <p>For an overview of all tools that support a team, see About teams and Agile tools.</p>
Security	<ul style="list-style-type: none"> • Add users to a project • Change individual permissions, grant select access to specific functions • Grant or restrict access to select features • Add administrators • Manage project-level permissions • Set build and release permissions 	<p>Project Administrators can add users to a project or a team. When you add a user to a team, you automatically add them to the project. Users added to a project can only view and contribute to that specific project.</p> <p>For an overview of security concepts, see About permissions and groups and About access levels. For a list of project-level permissions, see Permissions and groups reference, Project-level permissions.</p>
Notifications	<ul style="list-style-type: none"> • Manage project-level notifications 	<p>A number of project-level notifications are automatically defined when a project is added. Notifications at the project-level are managed in much the same way as they are at the team level.</p>
Service Hooks	<ul style="list-style-type: none"> • Configure service hooks 	<p>With service hooks, you can automate a task on other services, such as Campfire, Flowdock, HipChat, and more. You can use service hooks in custom apps and services to drive activities as events happen.</p>
Dashboards	<ul style="list-style-type: none"> • Set default dashboard permissions 	<p>New dashboards added to a project inherit the default dashboard permissions. The default permissions allow team members to create and edit dashboards for their team.</p>
Boards, Project configuration	<ul style="list-style-type: none"> • Define area paths • Define iteration paths or sprints 	<p>Area and iteration paths set at the project level are then used to set team defaults. To configure additional product backlogs, Kanban boards, and dashboards, you first add a team.</p>
Build and release (Agent Pools, Release)	<ul style="list-style-type: none"> • Manage Agent queues and agent pools • Manage service connections • Manage deployment pools and groups • Set retention policies 	<p>To build your code or deploy your software you need at least one agent. Agent and deployment pools are build and release resources that you manage across projects.</p>
Repos, Code, version control	<ul style="list-style-type: none"> • Create additional Git repos • Manage repository permissions • Manage branch policies • Add TFVC Check-In Policies 	<p>You can manage code using Git repositories or one Team Foundation Version Control (TFVC) repository.</p>
Test	<ul style="list-style-type: none"> • Set test retention policies • Manage test-related permissions at project level • Set area path-level test permissions 	<p>Manual testing relies on work item types to create and manage test plans, test suites, test cases, shared steps, and shared parameters. Of these, you can customize the test plans, test suites, and test cases using an inherited process. See Customize a process.</p>

Wiki	<ul style="list-style-type: none"> • Create a wiki for your project • Publish a Git repository to a wiki • Manage README and Wiki permissions 	To share information with your team, you can use Markdown format within a project Wiki, within your project README file, or other repository README file. To learn more, see About READMEs and Wikis .
Extensions	<ul style="list-style-type: none"> • Request a Marketplace extension 	Individual contributors and project administrators can request a Marketplace extension be installed. Only members of the Project Collection Administrators group can respond to these requests and actually install extensions.

Project Collection Administrator (PCA) role and managing collections of projects

Members of the [Project Collection Administrators](#) group are tasked with configuring resources for all projects defined for an organization or collection. They also can perform all tasks to add projects, manage projects, and manage permissions for the collection, a project, or an object.

Organization settings

From the administrative **Organization settings** pages, you can configure settings available from the tabs shown in the following image.

Organization Settings > Overview

- General
 - Overview (highlighted)
 - Projects
 - Policy
 - Users
 - Security
 - Notifications
 - Extensions
 - Usage
- Boards
 - Process
- Build and release
 - Agent pools
 - Deployment pools
 - Retention and parallel jobs
 - OAuth configurations

Project collection-level settings

From the administrative pages for a collection, you can configure the settings shown in the following image.

NOTE

Project collection settings differ depending on your on-premises TFS version. Some settings aren't available for earlier versions of TFS.

fabrikam

- Projects (selected)
- My favorites
- My work items
- My pull requests
- Users

- Notifications
- Extensions
- Usage

For an overview of managing your organization, see [About organization management](#).

Area	Supported Tasks	Notes
Preview features	<ul style="list-style-type: none"> Enable preview features 	Organization administrators can enable or disable account-level features that are in preview.
Overview (Settings)	<ul style="list-style-type: none"> Add and manage organization information: change organization owner, Rename, Delete, Recover Find or change your organization location Set up billing 	From the Settings page, you can manage the time zone, owner, region, and other settings that apply to all projects defined under your account.
Billing	<ul style="list-style-type: none"> Set up billing Try Azure Test Plans for free Pay for users (Basic) Buy CI/CD Add a user to make purchases 	All billing is managed through Azure. To learn more, see Billing overview .
Projects	<ul style="list-style-type: none"> Add and manage projects: Create, Rename, Delete Add users to projects Save project data 	A project provides the fundamental resource for storing your code, managing your CI/CD operations, and planning and tracking work for your project. In general, you'll want to minimize the number of projects you create, to keep things simple. Learn more About projects and scaling your organization .
Policy	<ul style="list-style-type: none"> Change application access policies 	Set policies to allow or disallow access by other applications or services to the organization.
Users	<ul style="list-style-type: none"> Add users Add external users Manage user access levels Remove users Assign paid extension access to users 	For large organizations with a sizable number of users, we recommend that you manage user access through Azure Active Directory . For a small number of users, you can manage user access by adding their Microsoft Service Account (MSA) email. From the account-level Users page, you can also export the set of users and their access levels .
Security	<ul style="list-style-type: none"> Change individual permissions Grant or restrict access to select features Add administrators Add Azure Active Directory groups Connect to Azure Active Directory Manage conditional access 	For an overview of security concepts, see About permissions and groups and About access levels . For a list of collection-level permissions, see Permissions and groups reference , Collection-level permissions .
Notifications	<ul style="list-style-type: none"> Manage collection-level notifications 	A number of notifications are automatically defined when an organization is added. Notifications at the organization-level are managed in much the same way as they are at the team level .

Extensions	<ul style="list-style-type: none"> • Install and manage Marketplace extensions • Approve extensions • Assign paid extension access to users • Change the number of paid users • Grant permissions to manage extensions • Uninstall or disable extensions 	An extension is an installable unit that contributes new capabilities to your projects. You can find extensions from within the Visual Studio Marketplace in the Azure DevOps tab to support planning and tracking of work items, sprints, scrums, etc.; build and release flows; code testing and tracking; and collaboration among team members.
Usage	<ul style="list-style-type: none"> • Monitor usage 	Certain rate limits are in place to ensure performance across the cloud service platform.
Boards, Process	<ul style="list-style-type: none"> • Customize a project • Add and manage processes 	Process customization applies to Azure Boards only. To customize the Agile tools and work tracking artifacts, you create and customize an inherited process and then update the project to use that process. To learn more, see About process customization and inherited processes .
Build and release	<ul style="list-style-type: none"> • Set retention policies • Set resource limits for pipelines • Add and manage agent pools • Add and manage deployment pools 	You manage resources that support CI/CD operations for all projects through the Agent pools , Deployment pools , and Retention and limits pages.

For an overview of managing collections, see [Configure and manage Azure DevOps Server resources](#).

AREA	SUPPORTED TASKS	NOTES
Settings	<ul style="list-style-type: none"> • Change access levels 	From the Settings page, you can manage the time zone, owner, region, and other settings that apply to all projects defined under your account.
Projects	<ul style="list-style-type: none"> • Add and manage projects: Create, Rename, Delete • Add users to projects • Save project data 	A project provides the fundamental resource for storing your code, managing your CI/CD operations, and planning and tracking work for your project. In general, you'll want to minimize the number of projects you create, to keep things simple. Learn more About projects and scaling your organization .
Security	<ul style="list-style-type: none"> • Change individual permissions • Grant or restrict access to select features • Add collection-level administrators • Set up groups for use in Azure DevOps Server deployments • Add administrators to Azure DevOps Server 	For an overview of security concepts, see About permissions and groups and About access levels . For a list of collection-level permissions, see Permissions and groups reference , Collection-level permissions .
Notifications	<ul style="list-style-type: none"> • Manage collection-level notifications 	A number of notifications are automatically defined when a project collection is added. Notifications at the collection-level are managed in much the same way as they are at the team level .

Boards, Process	<ul style="list-style-type: none"> Customize a project Add and manage processes 	Process customization applies to Azure Boards only. To customize the Agile tools and work tracking artifacts, you create and customize an inherited process and then update the project to use that process. To learn more, see About process customization and inherited processes .
Build and release, Agent pools, Deployment pools	<ul style="list-style-type: none"> Set retention policies Set resource limits for pipelines Add and manage agent pools Add and manage deployment pools 	You manage resources that support CI/CD operations for all projects through the Agent pools , Deployment pools , and Retention and limits pages.
Extensions	<ul style="list-style-type: none"> Install and manage Marketplace extensions Approve extensions Assign paid extension access to users Change the number of paid users Grant permissions to manage extensions Uninstall or disable extensions 	An extension is an installable unit that contributes new capabilities to your projects. You can find extensions from within the Visual Studio Marketplace in the Azure DevOps tab to support planning and tracking of work items, sprints, scrums, etc.; build and release flows; code testing and tracking; and collaboration among team members.

For an overview of managing collections, see [Configure and manage TFS resources](#).

AREA	SUPPORTED TASKS	NOTES
Settings	<ul style="list-style-type: none"> Change access levels 	From the Settings page, you can manage the time zone, owner, region, and other settings that apply to all projects defined under your account.
Projects	<ul style="list-style-type: none"> Add and manage projects: Create, Rename, Delete Add users to projects Save project data 	A project provides the fundamental resource for storing your code, managing your CI/CD operations, and planning and tracking work for your project. In general, you'll want to minimize the number of projects you create, to keep things simple. Learn more About projects and scaling your organization .
Security	<ul style="list-style-type: none"> Change individual permissions Grant or restrict access to select features Add collection-level administrators Set up groups for use in TFS deployments Add administrators to TFS 	For an overview of security concepts, see About permissions and groups and About access levels . For a list of collection-level permissions, see Permissions and groups reference , Collection-level permissions .
Notifications	<ul style="list-style-type: none"> Manage collection-level notifications 	A number of notifications are automatically defined when a project collection is added. Notifications at the collection-level are managed in much the same way as they are at the team level .
Build and release, Agent pools, Deployment pools	<ul style="list-style-type: none"> Set retention policies Set resource limits for pipelines Add and manage agent pools Add and manage deployment pools 	You manage resources that support CI/CD operations for all projects through the Agent pools , Deployment pools , and Retention and limits pages.

Extensions	<ul style="list-style-type: none">• Install and manage Marketplace extensions• Approve extensions• Assign paid extension access to users• Change the number of paid users• Grant permissions to manage extensions• Uninstall or disable extensions	An extension is an installable unit that contributes new capabilities to your projects. You can find extensions from within the Visual Studio Marketplace in the Azure DevOps tab to support planning and tracking of work items, sprints, scrums, etc.; build and release flows; code testing and tracking; and collaboration among team members.
-------------------	---	--

Server Administrator role

Members of the [Team Foundation Server Administrators group](#) are tasked with configuring resources for all project collections. They also can perform all tasks to administer projects, collections, and server instances.

The main task they perform from the web portal is to set access levels for a user or security group. See [Change access levels](#).

For additional information, see [Team Foundation Server Administration Documentation](#).

Related articles

- [Resources granted to project members](#)
- [Permissions and groups reference](#)
- [Rate limits](#)

Manage your project

6/18/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

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.

That said, as an organization owner or a project administrator, there are a few tasks you might want to do once you created your project to ensure a smooth operational experience. If you own a large organization, you'll want to consider additional tasks to structure your projects to support multiple teams or software development apps.

Add users to your project

The first task is to ensure that all members of your organization or group are added to your organization and projects. For small groups, using [Microsoft Accounts](#) to add users to your organization and projects works fine.

Larger enterprises may want to consider using Azure Active Directory to manage permissions and user access. To learn more, see the following articles:

- [Add organization users for Azure DevOps Services](#)
- [Manage user access through Azure Active Directory](#)

The first task is to ensure that all members of your organization or group are added to your organization and project. Larger organizations may want to consider using Azure Active Directory to keep the maintenance of managing permissions and user access. Typically, you should install Azure Active Directory prior to installing TFS. To learn more, see these articles:

- [Install Azure Active Directory Domain Services \(Level 100\)](#)
- [Step-By-Step: Setting up Azure Active Directory in Windows Server 2016](#)

You can delegate the task to add users to an organization by adding a user with Stakeholder or higher access to the [Project Collection Administrators group](#).

Grant or restrict permissions

Access to features and functions is controlled by access-level assignments, permissions, and security groups. To quickly understand the defaults configured for your project, see [Default permissions and access](#).

If you decide that you want to delegate specific tasks to others, then you'll want to add them to a built-in or custom security group or add them to a specific role. To learn more, see these articles:

- [Grant or restrict access to select features and functions](#)
- [Set permissions at the project level or project collection level](#)

To learn more about permissions and security, review the following articles:

- [About security and identity](#)
- [About permissions and groups](#)
- [About security roles](#)
- [About access levels](#)

Share your project vision and support collaboration

Each project has a summary page where you can share information through **README** files or by pointing to a project Wiki. To orient users who are new to your project and share established processes and procedures, we recommend that you [set up your project summary page](#) or [provision a Wiki](#).

Each project has a summary page where you can share information through **README files**. To orient users who are new to your project and share established processes and procedures, we recommend that you [set up your project summary page](#).

Remove unused services from the user interface

To simplify the web portal user interface, you can disable select services. For example, if you use a project only to log bugs, then you can remove all services except for **Boards**.

This example shows that **Test Plans** has been disabled:

The screenshot shows the 'Project Settings > Overview' page. On the left, there's a sidebar with 'General' and 'Boards' sections. Under 'General', 'Overview' is selected. In the main area, titled 'Azure DevOps services', there are six service toggles:

Service	Description	Status
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

Set code, test, and other policies

There are several policies you can set to support collaboration across your teams, secure your projects, and automatically remove files that are no longer needed. To set policies, review the following articles:

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

Define area and iteration paths for work tracking

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

ITERATIONS	AREAS																																													
<p>Iterations Areas</p> <p>Create and manage the iterations for this project. These are used for iteration planning (sprint planning). click here</p> <p>To access the default team's iteration settings, click here.</p> <p>New New child + Add Edit</p> <table><thead><tr><th>Iterations</th><th>Start Date</th><th>End Date</th></tr></thead><tbody><tr><td>◀ Fabrikam Fiber</td><td></td><td></td></tr><tr><td> ◀ Release 1</td><td></td><td></td></tr><tr><td> Sprint 1</td><td>6/11/2018</td><td>6/29/2018</td></tr><tr><td> Sprint 2</td><td>7/2/2018</td><td>7/20/2018</td></tr><tr><td> Sprint 3</td><td>7/16/2018</td><td>8/3/2018</td></tr><tr><td> Sprint 4</td><td>7/23/2018</td><td>8/10/2018</td></tr><tr><td> Sprint 5</td><td>9/17/2018</td><td>10/5/2018</td></tr><tr><td> Sprint 6</td><td>10/29/2018</td><td>11/16/2018</td></tr><tr><td> Release 2</td><td></td><td></td></tr><tr><td> Release 3</td><td></td><td></td></tr></tbody></table>	Iterations	Start Date	End Date	◀ Fabrikam Fiber			◀ Release 1			Sprint 1	6/11/2018	6/29/2018	Sprint 2	7/2/2018	7/20/2018	Sprint 3	7/16/2018	8/3/2018	Sprint 4	7/23/2018	8/10/2018	Sprint 5	9/17/2018	10/5/2018	Sprint 6	10/29/2018	11/16/2018	Release 2			Release 3			<p>Iterations Areas</p> <p>Create and manage the areas for this project. These are used for the team's backlog and what work items the team is responsible for. click here</p> <p>To access the default team's area settings, click here.</p> <p>New New child + Add Edit</p> <table><thead><tr><th>Areas</th><th>Teams</th></tr></thead><tbody><tr><td>◀ Fabrikam Fiber</td><td>Fabrikam Fiber Team</td></tr><tr><td> Customer Service</td><td>Customer Service Team</td></tr><tr><td> Phone</td><td>Fabrikam Fiber Team, Phone</td></tr><tr><td> Voice</td><td>Voice</td></tr><tr><td> Web</td><td>Fabrikam Fiber Team, Web</td></tr></tbody></table>	Areas	Teams	◀ Fabrikam Fiber	Fabrikam Fiber Team	Customer Service	Customer Service Team	Phone	Fabrikam Fiber Team, Phone	Voice	Voice	Web	Fabrikam Fiber Team, Web
Iterations	Start Date	End Date																																												
◀ Fabrikam Fiber																																														
◀ Release 1																																														
Sprint 1	6/11/2018	6/29/2018																																												
Sprint 2	7/2/2018	7/20/2018																																												
Sprint 3	7/16/2018	8/3/2018																																												
Sprint 4	7/23/2018	8/10/2018																																												
Sprint 5	9/17/2018	10/5/2018																																												
Sprint 6	10/29/2018	11/16/2018																																												
Release 2																																														
Release 3																																														
Areas	Teams																																													
◀ Fabrikam Fiber	Fabrikam Fiber Team																																													
Customer Service	Customer Service Team																																													
Phone	Fabrikam Fiber Team, Phone																																													
Voice	Voice																																													
Web	Fabrikam Fiber Team, Web																																													

Customize work-tracking processes

You and your teams can start using all work-tracking tools immediately after you create a project. But often, one or more users want to customize the experience to meet one or more business needs. Although you can customize the process easily through the user interface, you can establish a methodology for who manages the updates and evaluates requests.

NOTE

By default, users granted Stakeholder and higher access are granted permission to create, edit, and manage processes used to customize the work-tracking experience. If you want to lock down who can perform these tasks, set permissions at the organization level to **Deny**.

To learn more, see the following articles:

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

Customize work-tracking processes

You and your teams can start using all work-tracking tools immediately after you create a project. But often, one or more users want to customize the experience to meet one or more business needs. You can establish a

methodology for who manages the updates and evaluates requests.

To learn more, see [On-premises XML process model](#).

Review and update notifications

A number of 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 notifications](#), managed by a team administrator.
- Project notifications, managed by a member of the Project Administrators group.
- [Organization and collection level notifications](#), managed by a member of the Project Collection Administrators group.

If users believe they're getting too many notifications, they can [opt out of a subscription](#).

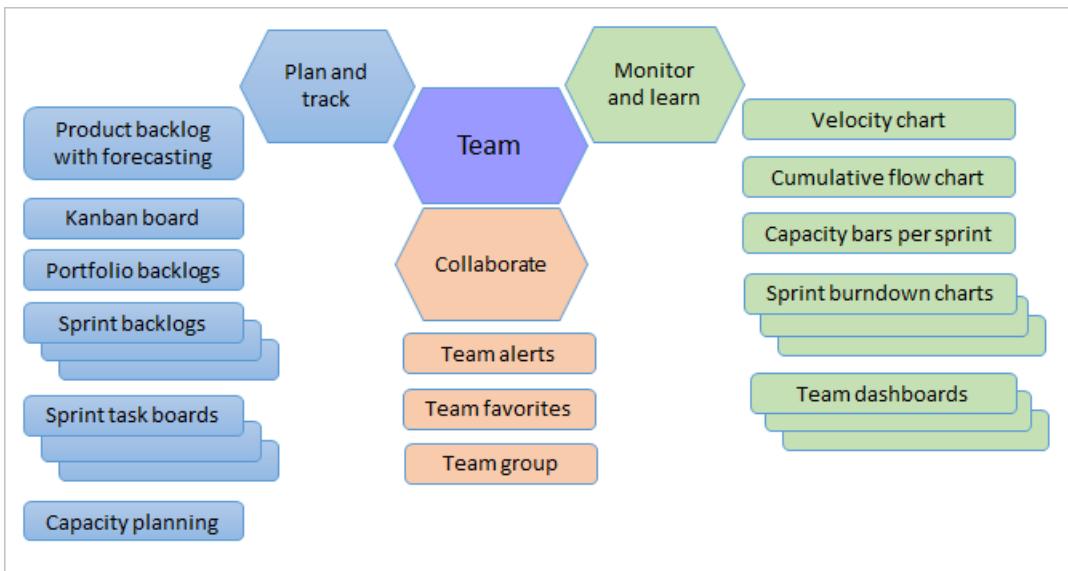
Description	Type	Notifies	State
Build			
 Build completes Notifies you when a build you queued or that was queued for you compl...	Build completed (any project)	 You	 On
Code (Git)			
 Pull request reviewers added or removed Notifies you when you are added to a pull request or when a user is add...	Pull request (any project)	 You	 On
 Pull request completion failures Notifies you when a pull request you created fails to complete	Pull request (any project)	 You	 On
 Pull request changes Notifies you when changes are made to a pull request you created or are...	Pull request (any project)	 You	 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	 On

Configure an SMTP server

In order for team members to receive notifications, [you must configure an SMTP server](#).

Add teams to scale your organization

We recommend that you add teams as your organization grows. Each team gets [access to their own set of Agile tools](#) that they can customize.



To learn more, 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](#)

Install and manage extensions

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

- Planning and tracking of work items, sprints, scrums, etc.
- 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, you must be an organization owner, a member of the Project Collection Administrators group, or added to the [Manager role for extensions](#).

Set up billing

All organizations can add up to five users with Basic access and unlimited users with Stakeholder access. If you need to add more users or pay for additional services or extensions, [set up billing](#).

Next steps

[Manage projects](#)

Related articles

- [Security & identity](#)
- [Organization management](#)
- [About user, team, project, and organization-level settings](#)
- [Manage projects](#)
- [Security & identity](#)

- [Organization management](#)
- [About user, team, project, and organization-level settings](#)
- [TFS administration](#)

Set user preferences

7/2/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

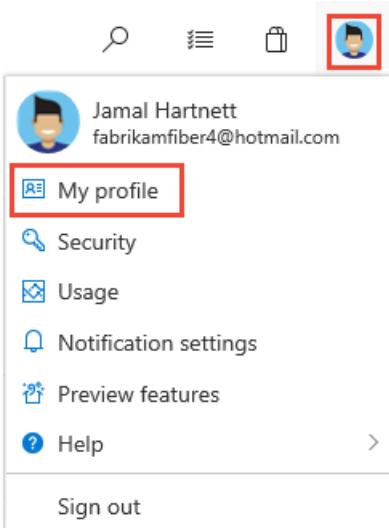
From your profile page, you can change your picture or other account preferences. Specifically, you can set the following:

AREA	TASK
Profile	<ul style="list-style-type: none">Change your pictureChange your display nameChange your preferred emailChange your locale settings
Security	<ul style="list-style-type: none">Personal access tokensAlternate authentication credentialsOAuth authorizationsSSH public keys
Other	<ul style="list-style-type: none">Manage personal notificationsUsageEnable preview features

Locale settings include language, date and time pattern, time zone, and user interface theme.

Change profile settings

1. To change your user preferences, open your profile menu.



2. Choose **Edit profile**.



Jamal Hartnett

fabrikamfiber4@hotmail.com

[Edit profile](#)

Microsoft account



United States

fabrikamfiber4@hotmail.com

Visual Studio Dev Essentials

Get everything you need to build and deploy your app on any platform.

[Use your benefits](#)

Authorizations

You have authorized 12 applications

[Manage authorizations](#)

Visual Studio Team Services Accounts

fabrikamfabulous.visualstudio.com (Owner)

Projects

[New project](#)

fabrikam-fiber.visualstudio.com (Owner)

com-and-business.visualstudio.com (Member)

fabrikamfib.visualstudio.com (Member)

fabrikamfiber.visualstudio.com (Member)

fabrikaminthecloud.visualstudio.com (Member)

- From the **About** page, you can change your profile picture, change your display name, contact information, and country.

Edit Profile

About**Preferences ***

Profile Image



Select an image file on your computer (4MB max)

Choose image**Reset profile picture**

Full name

Jamal Hartnett

Contact e-mail

fabrikamfiber4@hotmail.com

Country/Region

United States

 Microsoft may use your contact information to provide updates and special offers about Visual Studio.

You can unsubscribe at any time.

By clicking Save changes, you agree to the [Terms of Service](#), [Privacy Statement](#), and [Code of Conduct](#) and certify that you have the right to distribute the uploaded file.

Save changes**Cancel**

4. From the **Preferences** page, you can change your preferred language, date and time pattern, time zone, UI theme, and whether or not borders appear on work item forms for fields.

Edit Profile

About

Preferences *

Locale

Preferred Language

Browser: English (United States)

Date Pattern

7/18/2018 (M/d/yyyy)

Time Pattern

9:10 PM (h:mm tt)

Time Zone

(UTC) Coordinated Universal Time

User Interface

UI Theme

Default

Work item form

Hide field borders

By clicking Save changes, you agree to the [Terms of Service](#), [Privacy Statement](#), and [Code of Conduct](#) and certify that you have the right to distribute the uploaded file.

Save changes

Cancel

Change profile settings

1. To change your user preferences, open your profile menu.

The screenshot shows the Fabrikam Fiber application interface. At the top, there is a navigation bar with icons for notifications, user profile, and search. The user profile section displays the name "Jamal" and the email "fabrikamfiber5@hotmail.com". Below the profile picture, there is a red box highlighting the "My profile" link. Other options in the profile menu include "Notification settings", "Security", "Usage", and "Preview features". On the left side of the screen, there are cards for "Visual Studio" (with links to "Open in Visual Studio" and "Get Visual Studio"), "Dashboards", "Code", and a three-dot menu. The "Overview" card is currently selected.

2. Choose **Edit profile**.



Jamal Hartnett

fabrikamfiber4@hotmail.com

[Edit profile](#)

Microsoft account



United States

fabrikamfiber4@hotmail.com

Visual Studio Dev Essentials

Get everything you need to build and deploy your app on any platform.

[Use your benefits](#)

Authorizations

You have authorized 12 applications

[Manage authorizations](#)

Visual Studio Team Services Accounts

fabrikamfabulous.visualstudio.com (Owner)

Projects

MyFirstProject

[New project](#)

fabrikam-fiber.visualstudio.com (Owner)

com-and-business.visualstudio.com (Member)

fabrikamfib.visualstudio.com (Member)

fabrikamfiber.visualstudio.com (Member)

fabrikaminthecloud.visualstudio.com (Member)

- From the **About** page, you can change your profile picture, change your display name, contact information, and country.

Edit Profile

About**Preferences ***

Profile Image



Select an image file on your computer (4MB max)

Choose image**Reset profile picture**

Full name

Jamal Hartnett

Contact e-mail

fabrikamfiber4@hotmail.com

Country/Region

United States



Microsoft may use your contact information to provide updates and special offers about Visual Studio.
You can unsubscribe at any time.

By clicking Save changes, you agree to the [Terms of Service](#), [Privacy Statement](#), and [Code of Conduct](#) and certify that you have the right to distribute the uploaded file.

Save changes**Cancel**

4. From the **Preferences** page, you can change your preferred language, date and time pattern, time zone, UI theme, and whether or not borders appear on work item forms for fields.

Edit Profile

About

Preferences *

Locale

Preferred Language

Browser: English (United States)

Date Pattern

7/18/2018 (M/d/yyyy)

Time Pattern

9:10 PM (h:mm tt)

Time Zone

(UTC) Coordinated Universal Time

User Interface

UI Theme

Default

Work item form

Hide field borders

By clicking Save changes, you agree to the [Terms of Service](#), [Privacy Statement](#), and [Code of Conduct](#) and certify that you have the right to distribute the uploaded file.

Save changes

Cancel

Related articles

- [Set favorites](#)

Enable preview features

6/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

As new features are introduced, you can turn them on or off. That way, you can try them out, provide feedback, and work with those features that meet your requirements.

Some features provide a new user interface and functionality, which can be managed per user or team member. Others support a default experience for the account and are managed by an account administrator.

NOTE

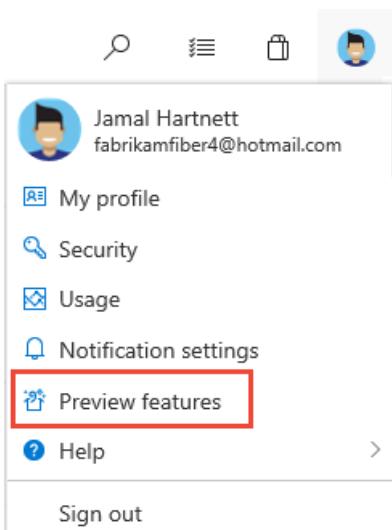
You can turn on or off select features for Azure DevOps Services. Preview features become available first on Azure DevOps Services and then become standard features with an update to Azure DevOps Server. At some point, the preview feature moves out of preview status and becomes a regular feature of the web portal.

PREVIEW FEATURES PER USER	PREVIEW FEATURES PER ORGANIZATION
<ul style="list-style-type: none">- Analytics Views- Experimental themes- Git commit menu extension points- Multi-stage pipelines- New PAT experience- Test analytics in new web platform- Test tab in new web platform	<ul style="list-style-type: none">- Analytics Views- Experimental themes- Full Access to Azure Pipelines for Stakeholders- Git Forks- Multi-stage pipelines- New PAT experience- New Releases Hub- Test analytics in new web platform- Test tab in new web platform

Enable features for your use

From time to time, a new feature is introduced in Preview mode, which allows you to turn it on or off.

1. To access the Preview features options, open your profile menu, and select **Preview features**.



2. To enable or disable a feature, choose the slider.

X

Preview features

The following preview features are available for your evaluation. Help us make them better!

for me [Jamal Hartnett]



Experimental Themes

On

Adds an early preview of various themes to the Theme management panel.

Git commit menu extension points

On

Opens up Git commit context menu to contributed actions.

New build result page

On

Lights up new build results page.

New log reader for Pipelines

On

Lights up new logs reader for Pipelines.

New PAT Experience

On

Enable new Personal access token page on security hub.

New release progress views

On

Turn on the new release views to visualize the progress of your deployment pipelines. [Learn more](#)

Enable features at the organization level (for all users)

When you enable a feature at the organization level, you essentially turn it on for all users of your account. Each user can then disable the feature if they so choose.

TIP

If you don't see the **for this account** menu option, then you aren't an account administrator. To get added as one, see [Add administrators, set permissions at the team project or collection level](#).

Preview features

The following preview features are available for your evaluation. Help us make them better!

for this account [fabrikam] ▾

Experimental Themes <input checked="" type="checkbox"/> On	Adds an early preview of various themes to the Theme management panel.
Full access to Azure Pipelines for Stakeholders <input checked="" type="checkbox"/> On	Gives users with the Stakeholder license full access to Azure Pipelines for private projects. Limit what they can do by using security groups and permissions. Turning on this feature doesn't affect public projects, where Stakeholders always have full access. Learn more
Git Forks <input checked="" type="checkbox"/> On	Enable git repositories to be forked. Learn more
New build result page <input type="checkbox"/> On	Lights up new build results page.
New log reader for Pipelines <input type="checkbox"/> Off	Lights up new logs reader for Pipelines.
New PAT Experience <input checked="" type="checkbox"/> On	Enable new Personal access token page on security hub.
New release progress views <input type="checkbox"/> On	Turn on the new release views to visualize the progress of your deployment pipelines. Learn more
New Releases Hub <input checked="" type="checkbox"/> On	Turns on the experience to create folders and manage release pipelines.
New YAML pipeline creation experience <input type="checkbox"/> Off	Enables the new YAML pipeline creation experience.
Test analytics in new web platform <input checked="" type="checkbox"/> On	Lights up test analytics features in new web platform.
Test tab in new web platform <input checked="" type="checkbox"/> On	Lights up a new test tab under build in new web platform.

Features now enabled for all Azure DevOps Services

General

- [New Navigation](#)

Azure Pipelines

- [New builds hub](#)
- [Build with multiple queues](#)
- [New Releases Hub](#)
- [Approval gates in releases - New Release Definition Editor](#)
- [Symbol server](#)
- [Task tool installers](#)

Azure Boards

- [New Rich Text Editor- New Queries Experience](#)
- [New Work Items](#)

Azure Repos

- [Pull Request Status Policy](#)

Azure Artifacts

- [NuGet.org upstream sources](#)
- [Updated package experience](#)

Azure Test Plans

- [New Test Plan Experience](#)

Dashboards and Analytics

- [New Dashboards Experience](#)

Social tools

- [Wiki](#)
- [Combine email recipients](#)
- [New experience in Code, Work Item, & Wiki search](#)
- [Out of the box notifications](#)
- [Team expansion for notifications](#)

Organization, project, and billing management

- [Streamlined User Management](#)

Tutorial: Set personal or team favorites

6/13/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

Favorite  those views that you frequently access. You can favorite all sorts of Azure DevOps features and tools—such as a project, repository, build pipeline, dashboard, backlog, board, or query. You can set favorites for yourself or your team.

As your code base, work tracking efforts, developer operations, and organization grows, you'll want to be able to quickly navigate to those view of interest to you and your team. Setting favorites allows you to do just that.

Team favorites are a quick way for members of your team to quickly access shared resources of interest. You favorite an item for yourself by choosing the  star icon. The favorited item will then show up easily from one or more directory lists. You set favorites for a team through the context menu for the definition, view, or artifact.

In this tutorial you'll learn how to view your personal favorites and to favorite or unfavorite the following views:

- Project or team
- Dashboard
- Team backlog, board, shared query, or other Azure Boards view
- Repository
- Build and release definition
- Test plans

- Project
- Shared query
- Repository
- Build and release definition
- Test plans

Prerequisites

- You must connect to a project through the web portal. If you don't have a project yet, [create one](#). To connect to the web portal, see [Connect to a project](#).
- You must be a member of the **Contributors** or an administrators security group of the project. To get added, [Add users to a project or team](#).
- To favorite projects, backlogs, boards, queries, dashboards, or pipeline views, you must have **Stakeholder** access or higher.
- To favorite repositories, or delivery plans, you must have **Basic** access or higher.
- To favorite test plans, you must have **Basic + Test Plans** access level or equivalent.

- You must connect to a project through the web portal. If you don't have a project yet, [create one](#). To connect to the web portal, see [Connect to a project](#).
- You must be a member of the **Contributors** or an administrators security group of the project. To get added, [Add users to a project or team](#).
- To favorite projects, backlogs, boards, queries, dashboards, or pipeline views, you must have **Stakeholder** access or higher.
- To favorite repositories, or delivery plans, you must have **Basic** access or higher.

- To favorite test plans, you must have **Basic + Test Plans** access level or equivalent.

For details about the different access levels, see [About access levels](#).

View personal favorites

Access views that you have favorited by choosing the inbox icon, and then choosing **Favorites**.

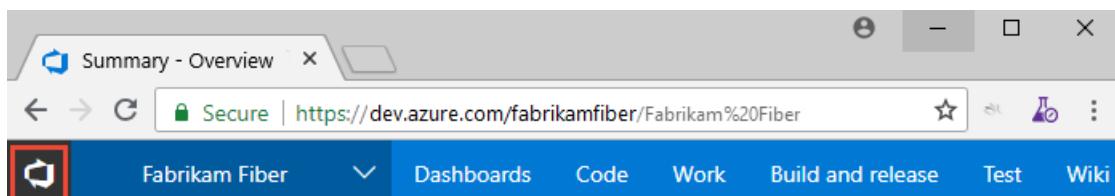
The screenshot shows the 'Favorites' section of the Azure DevOps interface. At the top, there's a navigation bar with icons for search, inbox (highlighted with a red box), library, and profile. Below the navigation bar, there are tabs for 'Work Items', 'Pull requests', and 'Favorites' (also highlighted with a red box). The main content area is divided into sections: 'Projects', 'Teams', 'Dashboards', 'Plans', and 'Queries'. Each section lists items with a star icon indicating they are favorited. For example, under 'Teams', there are three items: 'Phone', 'Voice', and 'Web', each with a yellow star. Under 'Plans', there are two items: 'Backlog team plans' and 'Fabrikam Fiber Feature plans', each with a yellow star. Under 'Queries', there are three items: 'All items', 'All items on all projects', and 'Assigned to me', each with a yellow star.

Category	Item	Status
Projects	Fabrikam Fiber	★
Teams	Phone	★
	Voice	★
	Web	★
Dashboards	Fabrikam Fiber Team Analytics	★
Plans	Backlog team plans	★
	Fabrikam Fiber Feature plans	★
Queries	All items	★
	All items on all projects	★
	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](#).

1. Access views that you have favorited by choosing the Azure DevOps logo to open **Projects**.



2. Choose **My Favorites** to quickly access any view or item that you've marked as a favorite.

Favorites

Filter favorites



Queries

Bug Triage	Fabrikam Fiber	.../Shared Queries/Current Iteration	
My Bugs	Contoso	Shared Queries	
Open User Stories	Contoso	.../Shared Queries/Current Iteration	
Product Planning	Fabrikam Fiber	Shared Queries	
Product Planning	Contoso	Shared Queries	

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. The top navigation bar includes the Azure DevOps logo, the organization name 'fabrikam', and the project name 'Fabrikam Fiber'. The main content area displays the project's logo ('FF'), name ('Fabrikam Fiber'), and a yellow star icon indicating it is favorited. Below this, there is a section for 'Web, voice, and phone apps'. A 'README.md' file is listed with the following content:

```
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
```

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 > Backlog items backlog' page. At the top, there is a team selector showing 'Phone' with a yellow star icon next to it, indicating it is favorited. Below the team selector, the backlog items list is shown with various cards. At the bottom, there are filter and search options.

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 'Phone' project settings page. At the top, there's a purple circular icon with three stylized human figures. Below it, the project name 'Phone' and the team name 'Fabrikam Fiber' are displayed, along with a 'Team Settings' link. A navigation bar at the bottom has 'Items' (underlined) and 'Members (1)' options. A dropdown menu shows 'All Items'. Below this, three items are listed: 'Phone Boards' (with a board icon), 'Phone Backlogs' (with a document icon), and 'Phone Sprints' (with a checkmark icon). Each item has a yellow star icon to its right.

Favorite a project

To favorite a project, open the project **Summary** page and choose the star icon.

The screenshot shows the 'FabrikamFiber' project summary page. At the top, there's a blue header bar with the project name 'FabrikamFiber', 'Dashboards', 'Code', and a '...' button. To the right is a search bar. Below the header, the project name 'FabrikamFiber' is displayed with a yellow star icon to its right, which is highlighted with a red box. A brief description follows: 'Customer-focused apps under development based on Agile process.' On the right side, there are sections for 'Members' (with a 'K' icon and a '+' button), 'Activity' (empty), 'Code' (empty), and 'Build & Rel' (empty). A modal window titled 'Continuous integration' is open, featuring a large circular icon with a download arrow, the text 'Use continuous integration', the subtext 'Improve code quality by detecting breaking changes as soon as they happen.', a 'Setup Build' button, and a link 'Learn more about continuous integration'.

Or, you can favorite a project from the **Projects** page by choosing the star icon next to the project.

Favorite a dashboard

1. From **Overview>Dashboards**, open the selector and choose the **Browse all dashboards** option.

The screenshot shows the Microsoft Power BI interface with the title 'Fabrikam Team Overview'. The left sidebar contains a search bar and sections for 'Favorites', 'Account Management', 'Customer Profile', and 'Fabrikam Team'. A red box highlights the 'Browse all dashboards' button at the bottom. On the right, there are several cards: one green card showing '6 items', another purple card showing '0 Commits in last 7 d...', and a third card partially visible at the bottom labeled 'All items by State'.

2. The **Mine** page shows your favorited dashboards, and all dashboards of teams that you belong to. The **All** page (shown below) lists all dashboards defined for the project in alphabetical order. You can filter the list by team or by keyword.

Dashboards

Mine **All** | + New dashboard 

Filter dashboards Filter by team ▾

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

Search

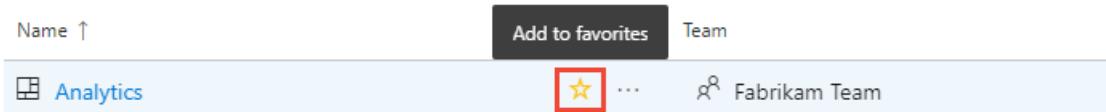
- Account Management
- Customer Profile
- Email
- Fabrikam Team
- Internet
- Phone
- Service Delivery
- Service Status

 Clear

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.



Favoriting a dashboard will cause it to appear on your **Favorites** page and towards the top in the **Dashboards** selection menu.

Favorite a team's backlog, Kanban 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**.

A screenshot of the Boards page in Azure DevOps. On the left, there's a sidebar with 'Fabrikam Fiber' and a list of sections: Overview, Boards, Work Items, Boards, Backlogs (which is highlighted with a red box), Sprints, and Queries. The main area shows 'Fabrikam Fiber Team' with a star icon. There are buttons for 'New Work Item', 'Backlog items Board', and 'Backlog items'. A table lists backlog items with columns: Order, Assigned To, State, and Title. The first item is 'Hello World Web Site' assigned to Jamal Hartnett, state Committed. The second item is 'Slow response on informa...' assigned to Jamal Hartnett, state Committed. The third item is 'Add an information form' assigned to Raisa Pokrovskaya, state New. The fourth item is 'Change initial view' assigned to Raisa Pokrovskaya, state New. The fifth item is 'Secure sign-in' assigned to Christie Church, state Committed. The sixth item is 'Welcome back page' assigned to Johnnie McLeod, state Approved. The seventh item is 'Cancel order form' assigned to Christie Church, state Committed.

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.

Fabrikam Fiber Team

Search team backlogs

My Team Backlogs

- Account Management
- Customer Profile
- Fabrikam Team
- Phone
- Service Delivery
- Service Status
- Shopping Cart

Browse all backlogs

- Choose the star icon to favorite a team backlog. Favorited artifacts (favorited 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.

Queries

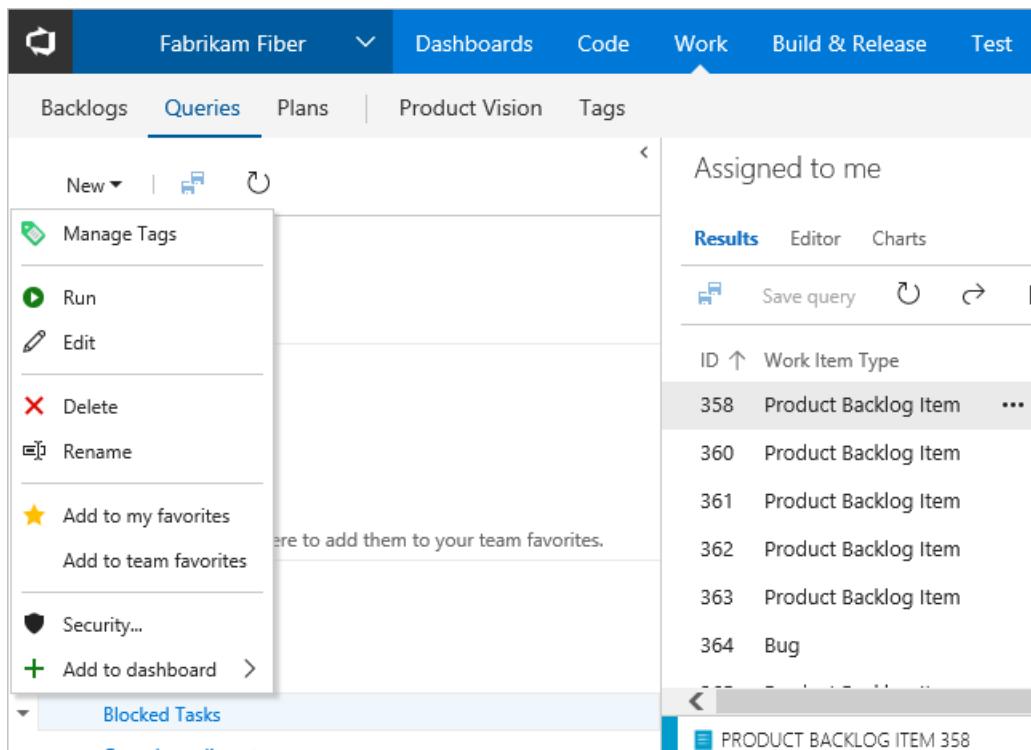
Favorites All + New query Filter by keywords

Title

- > My Queries
- ▽ Shared Queries
 - ▽ Current Sprint
 - ▀ Blocked Tasks
 - ▀ Open Impediments
 - ▀ Test Cases
 - ▀ Unfinished Work
 - ▀ Work in Progress
 - > Triage folder
 - ▀ All items
 - ▀ All items in a tree query
 - ▀ Feedback

You can also set a query as a personal favorite by opening the query and choosing the star icon.

Open **Work>Queries**. Next, open the *** actions icon menu of the shared query you want to favorite, and then select **Add to my favorites** or **Add to team favorites**.



The screenshot shows the 'Queries' page in the Azure DevOps interface. A context menu is open over a query result titled 'Product Backlog Item'. The menu includes options like 'Manage Tags', 'Run', 'Edit', 'Delete', 'Rename', 'Add to my favorites' (which is highlighted with a yellow star), 'Add to team favorites', 'Security...', and 'Add to dashboard'. The main pane displays a list of results under the heading 'Assigned to me', with one item selected: '358 Product Backlog Item'.

Favorite a delivery plan

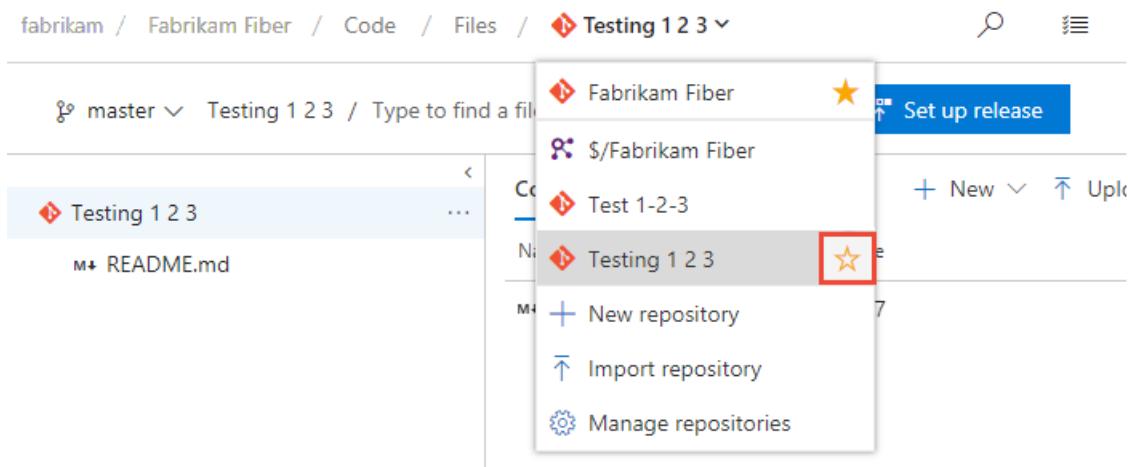
To learn more about delivery plans, see [Review team Delivery Plans](#).

To mark a delivery plan as a favorite, open the **Boards>Plans** page and choose the  star icon next to the Delivery Plan.

To mark a delivery plan as a favorite, open the **Work>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.



The screenshot shows the 'Code' page in the Azure DevOps interface. A context menu is open over a repository named 'Testing 1 2 3'. The menu includes options like 'Fabrikam Fiber', '\$/Fabrikam Fiber', 'Test 1-2-3', 'New repository', 'Import repository', and 'Manage repositories'. The 'Add to favorites' option is highlighted with a red box.

From any **Code** page, open the repository selector and choose the star icon next to the repository you want to favorite.

The screenshot shows the Azure DevOps Code interface. At the top, there's a navigation bar with 'Fabrikam Fiber' selected. Below it, a sidebar on the left lists repositories: 'Favorites', 'All repositories' (which is selected), 'Filter repositories', '\$/Fabrikam Fiber', 'Fabrikam Fiber' (with a yellow star icon highlighted by a red box), 'Testing 1 2 3', '+ New repository', 'Import repository', and 'Manage repositories'. The main area shows a list of files: 'Contents', 'History', and 'README'. The 'Contents' tab is selected, displaying a table with columns 'Name', 'Last change', and 'Commits'. The table contains four rows: 'page-1.md' (10/15/2015, 3458a6c7), 'page-2.md' (10/15/2015, 01a447ca), 'page-3.md' (9/21/2016, 68385e28), and 'README.md' (5/19/2017, fb9177d8).

Favorite a build pipeline

Open **Pipelines>Builds** and choose either **Mine** or **Definitions** page. 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 Azure DevOps Pipelines Builds interface. At the top, there's a search bar 'Build ID or build number' and buttons '+ New' and '+ Import'. Below it, a navigation bar has 'Mine' selected. The main area lists build definitions: 'Recently built' ('fabrikam build' and 'Fabrikam Fiber-Cl'), 'Status', 'Triggered by', and 'History'. A context menu is open for the 'fabrikam build' definition, with options like 'Queue new build...', 'Edit definition', 'Pause', 'View builds', 'Add to my favorites' (highlighted by a red box), 'Add to team favorites >', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', 'Security...', and '+ Add to dashboard >'.

Open **Build and Release>Builds** and choose either **Mine** or **Definitions** page. 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', 'All Definitions', 'Queued', and 'XAML'. A search bar at the top right contains the placeholder 'Build ID or build number' with a magnifying glass icon. Below the tabs, columns for 'Recently built', 'Status', and 'Triggered by' are shown. A specific build definition, 'fabrikam build', is selected, indicated by a checkmark icon and a star icon. A context menu is open next to the build name, listing options: 'Queue new build...', 'Edit...', 'View definition summary', 'Add to my favorites' (which is highlighted with a red box), 'Add to team favorites', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', and 'Security...'. The 'Add to my favorites' option is clearly the target of the user's action.

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.

To mark a test plan as a favorite, open the **Test>Test Plans** page and choose the star icon next to a test plan from the menu that shows All test plans.

Unfavorite a view you've favorited

You can unfavorite an artifact from your **Favorites** page. Choose the inbox icon, and then choose **Favorites**. Choose the favorited icon of a currently favorited artifact.

The screenshot shows the Microsoft Teams ribbon bar. The tabs visible are Work Items, Pull requests, and Favorites. The Favorites tab is highlighted with a red box. Other icons in the ribbon include a search icon, a grid icon, a file icon, and a user profile icon.

Projects

- Fabrikam Fiber

Teams

- Phone
 Voice
 Web

Dashboards

- Fabrikam Fiber Team Analytics

Plans

- Backlog team plans
 Fabrikam Fiber Feature plans

Queries

- All items
 All items on all projects
 Assigned to me

Similarly, you can unfavorite an artifact from the same page where you favorited it.

You can unfavorite an artifact from the **Projects>Favorites** page and choose the favorited icon of a currently favorited artifact.

Similarly, you can unfavorite an artifact from the same page where you favorited it.

Try this next

[Follow a user story, bug, issue, or other work item or pull request](#)

Related articles

- [Manage personal notifications](#)
- [Set your preferences](#)

Manage your notifications

3/5/2019 • 3 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

Feature availability: This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, **you must configure an SMTP server** for team members to see the Notifications option from their organization menu and to receive notifications.

As changes occur to your code base, builds, work items, and other operations, you can receive email notifications. For example, you can set an alert, so you're notified whenever a bug that you opened is resolved or you're assigned to a work item.

In this tutorial, you learn how to do the following tasks:

- View your notifications
- Add a custom subscription
- Unsubscribe or opt out of a team or project subscription

View your personal notifications

From the web portal, select the icon with your initials or picture, and then select **Notification settings** from the drop-down menu.

The screenshot shows the Azure DevOps web interface. At the top, there's a navigation bar with 'Azure DevOps' and a search bar. Below it, a sidebar on the left lists 'FabrikamFiber Web' (selected), 'Overview', 'Boards', 'Work Items' (selected), and 'Boards'. The main area is titled 'Work Items' with filters for 'Assigned to me', 'New Work Item', 'Open in Queries', and a 'Filter by keyword' input. On the right, there's a user profile for 'EB' with options like 'My profile', 'Security', 'Usage', and 'Notification settings'. The 'Notification settings' option is highlighted with a red box.

The screenshot shows the 'FabrikamFiber Team Overview' page. At the top, there's a navigation bar with 'FabrikamFiber / Fabrika...' and a search bar. The main area has sections for 'Welcome' (Get started using Visual Studio Team Services) and 'Work assigned to Jamal Hartnett (2)'. The 'Work assigned' section shows two bugs: one for 'ReadMe.txt missing from project' and another for 'Some bug work item here'. On the right, there's a user profile for 'Jamal Hartnett' with options like 'My profile', 'Security', 'Usage', and 'Notification settings'. The 'Notification settings' option is highlighted with a red box.

View all subscriptions

This view shows all subscriptions that you have created or that have been created by an administrator.

Subscriptions let you control what you are notified about. Those notifications you're subscribed to are indicated with the State as **On**.

Description	Type	Notifies	State
Build			
Build completes Notifies you when a build you queued or that was queued for you completes	Build completed (any project)	You	On
Code (Git)			
Pull request reviewers added or removed Notifies you when you are added to a pull request or when a user is added or removed from a pull request you created	Pull request (any project)	You	On
Pull request completion failures Notifies you when a pull request you created fails to complete	Pull request (any project)	You	On
Pull request changes Notifies you when changes are made to a pull request you created or are a reviewer for	Pull request (any project)	You	On
A comment is left on a pull request Notifies you about comments made to a pull request you created or a discussion you are involved in	Pull request comment (any project)	You	On

Description	Type	Notifies	State
Build			
Build completes Notifies you when a build you queued or that was queued for you compl...	Build completed (any project)	You	On
Code (Git)			
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	On
Pull request completion failures Notifies you when a pull request you created fails to complete	Pull request (any project)	You	On
Pull request changes Notifies you when changes are made to a pull request you created or are...	Pull request (any project)	You	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	On

A subscription can be just for you, or if you are a team admin, can be shared by everyone in the team.

Add a custom subscription

With custom personal subscriptions, you can define precise criteria for the events you want to receive notifications for. In contrast to a default subscription, which only notifies the users or groups directly associated with an event, a custom subscription can notify you about any event.

1. From your Notifications page, select **New subscription**.

User settings

General

Notifications

Usage

Security

Personal access tokens

Alternate credentials

SSH public keys

Notifications > Mine

+ New subscription

Description

Build

Build completes
Notifies you when a build you queued or that was queued for you completes

Pull request reviewers added or removed
Notifies you when you are added to a pull request or when a user is added or removed from a pull request

Security Notifications Usage

Notifications > Mine + New subscription Help

Description Type

Build

Build completes
Notifies you when a build you queued or that was queued for you completes Build completed (any project)

1. Choose the category and template you want to use. For a list of supported templates, see [Default and supported notifications](#).

Here we choose to get notified when a pull request is created within a specific project, Fabrikam Fiber.

New subscription

Category Template

Build

Code (Git)

Code (TFVC)

Work

Extension management

Release

A commit authored by me is pushed

A commit is pushed by me

A commit is pushed

A pull request is created or updated

Next Cancel

2. Modify the description to help you identify the subscription later. Also choose an email address for notifications to be delivered to. By default, your preferred email address is used. Optionally, include one or more fields to further specify the event criteria.

New subscription

Description	Subscriber		
A pull request is created or updated from Fabrikam Fiber	Raisa Pokrovskaya		
Deliver to	Address		
Preferred email	fabrikamfiber5@hotmail.com		
Filter			
<input type="radio"/> Any team project <input checked="" type="radio"/> A specific team project Fabrikam Fiber			
Filter criteria			
+ <input type="checkbox"/>	Field	Operator	Value
+ <input type="checkbox"/>	Status	Changes to	Abandoned
+ <input type="checkbox"/>	Reviewers	Contains	[Fabrikam Fiber]\Web
+ Add new clause			
Previous Finish Cancel			

NOTE

The fields available for filtering event criteria differ depending on the category and template you select.

3. Select **Finish** when you're done. The subscription now appears in the list under the category you selected.



Unsubscribe or opt out of a team or OOB subscription

You can choose to not receive notifications for certain team subscriptions by opting out of the subscription.

To unsubscribe from any notification, even one that you've defined, slide the State **On/Off** indicator to the Off position.

For example, here we turn off the Build completes subscription.

Notifications > Mine		New subscription	Help
Description	Type	Notifies	State
Build Build completes Notifies you when a build you queued or that was que...	Build completed (any project)	You	<input checked="" type="checkbox"/> Off

NOTE

Whether you are an administrator or not, toggling a shared team subscription from your notification settings only impacts you and not other team members.

Related articles

- [Set your preferences](#)
- [Default and supported notifications](#)
- [Follow a specific work item](#)
- [Manage notifications for a team](#)
- [Change your preferred email address](#)

Limitations

- The user interface no longer supports creating plain text email subscriptions.

Authenticate access with personal access tokens

6/18/2019 • 3 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

Personal access tokens (PATs) are alternate passwords that you can use to authenticate into Azure DevOps. In this article, we walk you through how to create or revoke PATS.

Azure DevOps uses enterprise-grade authentication to help protect and secure your data. Clients like Visual Studio and Eclipse (with the Team Explorer Everywhere plug-in) also support Microsoft account and Azure AD authentication. Since PATs are an alternate form of user authentication, using a PAT gives you the same access level. If you create a PAT with a narrower scope, your access is limited to that particular scope.

For non-Microsoft tools that integrate into Azure DevOps but don't support Microsoft account or Azure AD authentication, you must use PATs. Examples include Git, NuGet, or Xcode. To set up PATs for non-Microsoft tools, use [Git credential managers](#) or create them manually.

Create personal access tokens to authenticate access

1. Sign in to either your organization in Azure DevOps (<https://dev.azure.com/{yourorganization}>) or your Team Foundation Server web portal (<https://{{server}}:8080/tfs/>).
2. From your home page, open your profile. Go to your security details.

Azure DevOps Services

TFS 2017

3. Create a personal access token.

4. Name your token. Select a lifespan for your token.

If you're using Azure DevOps Services, and you have more than one organization, you can also select the organization where you want to use the token.

5. Select the [scopes](#) for this token to authorize for *your specific tasks*.

For example, to create a token to enable a [build and release agent](#) to authenticate to Azure DevOps Services or TFS, limit your token's scope to **Agent Pools (read, manage)**.

6. When you're done, make sure to *copy the token*. You'll use this token as your password.

NOTE

Remember that this token is your identity and acts as you when it's used. Keep your tokens secret and treat them like your password.

To keep your token more secure, use credential managers so that you don't have to enter your credentials every time. Here are some recommended credential managers:

- Git: [Git Credential Manager for macOS and Linux](#) or [Git Credential Manager for Windows](#) (requires [Git for Windows](#))
- NuGet: [NuGet Credential Provider](#)

Revoke personal access tokens to remove access

When you don't need your token anymore, just revoke it to remove access.

1. From your home page, open your profile. Go to your security details.

Azure DevOps Services



Azure DevOps Server (formerly TFS)



2. Revoke access.



See the following examples of using your PAT.

Username: `anything` Password: `your PAT here`

or

```
git clone https://anything:<PAT>@dev.azure.com/yourOrgName/yourProjectName/_git/yourRepoName
```

To learn more about how security and identity are managed, see [About security and identity](#).

To learn more about permissions and access levels for common user tasks, see [Default permissions and access for Azure DevOps](#).

For administrators to revoke organization user PATs, see [Revoke other users' personal access tokens](#).

Frequently asked questions

What is my Azure DevOps Services URL?

<https://dev.azure.com/{yourorganization}>

Where can I learn more about how to use PATs?

For examples of how to use PATs, see [Git credential managers](#), [REST APIs](#), [NuGet on a Mac](#), and [Reporting clients](#).

What notifications will I get about my PAT?

Users receive two notifications during the lifetime of a PAT, one at creation and the other seven days before the expiration.

The following notification is sent at PAT creation:

A new personal access token was added to your organization

[Learn more](#) about why you're receiving this email. If you did not make this change, your credentials may have been compromised and we suggest changing your password.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 10/30/2018

Origination IP

User agent

We sent you this notification due to a default subscription

Sent from Azure DevOps.

The following notification is sent - a PAT is near expiration:

One of your personal access tokens will be expiring on 8/4/2018.

Click below to manage your personal access tokens.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 8/4/2018

We sent you this notification due to a default subscription

Sent from Azure DevOps.

What do I do if I get an unexpected PAT notification?

An administrator or a tool might have created a PAT on your behalf. See the following examples:

- When you connect to an Azure DevOps Services Git repo through git.exe, it creates a token with a display name like "git: <https://MyOrganization.visualstudio.com/> on MyMachine."
- When you or an admin sets up an Azure App Service web app deployment, it creates a token with a display name like "Service Hooks :: Azure App Service :: Deploy web app."
- When you or an admin sets up web load testing as part of a pipeline, it creates a token with a display name like "WebAppLoadTestCDIntToken".
- When a Microsoft Teams Integration Messaging Extension is set up, it creates a token with a display name like "Microsoft Teams Integration".

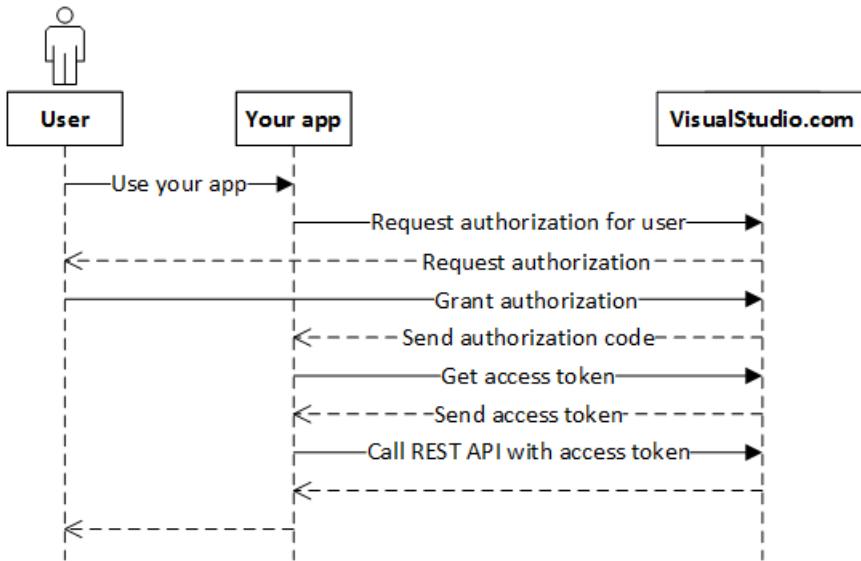
If you still believe that a PAT exists in error, we suggest that you [revoke the PAT](#). Next, change your password. As an Azure Active Directory user, check with your administrator to see if your organization was used from an unknown source or location.

Authorize access to REST APIs with OAuth 2.0

6/25/2019 • 13 minutes to read • [Edit Online](#)

Authenticate your web app's users to access the REST APIs so that your app doesn't have to keep asking for their usernames and passwords. Azure DevOps Services uses the [OAuth 2.0 protocol](#) to authorize your app for a user and generate an access token. Use this token when you call the REST APIs from your app.

First, you'll register your web app and get an app ID from Azure DevOps Services. Using that app ID, you'll send your users to Azure DevOps Services to authorize your app to access their organizations there. Once they've done that, you'll use that authorization to get an access token for that user. When you call Azure DevOps Services APIs on behalf of that user, you'll use that user's access token. Access tokens expire, so you'll also need to refresh the access token if it's expired.



For a C# example of the overall flow, see [vsts-auth-samples](#)

Register your app

Go to (<https://app.vsaex.visualstudio.com/app/register>) to register your app.

Make sure you select the [scopes](#) that your application needs, and then use the exact same scopes when you [authorize your app](#). If you registered your app using the preview APIs, you'll want to re-register because the scopes that you used are now deprecated.

When Azure DevOps Services presents the authorization approval page to your user, it will use your company name, and app name and descriptions, along with the URLs for your company's web site, your app's website, and your terms of service and privacy statements, like this.

Authorize application

fabrikam-fiber-oauth-sample by [Fabrikam Fiber](#)

Sample ASP.NET MVC app to show how to use Oauth with REST APIs for Visual Studio Online

[Or Visit application's website](#)

Review Requested Permissions

Full access to all resources

Provides this application the ability to act on your behalf with full access (read and write) to work items, Visual Studio Online accounts you can access.

Access to MSDN subscriptions

Provides this application the ability to access your MSDN subscription information including your level of access to MSDN Developer Services on your behalf.

[Learn more](#)

If you change your mind at any time, you can manage authorizations on your [profile page](#).

Accept

Deny

By clicking **Accept**, you agree to [Fabrikam Fiber Terms of Use](#) and [Privacy Statement](#).

When you call Azure DevOps Services to ask for a user's authorization, and the user grants it, Azure DevOps Services will redirect the user's browser to your authorization callback URL with the authorization code for that authorization. The callback URL must be a secure connection (<https://>) to transfer the code back to the app. It must exactly match the URL registered in your app. If it doesn't, a 400 error page is displayed instead of a page asking the user to grant authorization to your app.

When you register your app, the application settings page is displayed.

Application Settings

App ID:

App Secret:

Authorize URL: <https://app.vssps.visualstudio.com/oauth2/authorize>

Access Token URL: <https://app.vssps.visualstudio.com/oauth2/token>

Authorized Scopes: preview_api_all preview_msdn_licensing

Edit application

Delete

You'll call the authorization URL and pass your app ID and authorized scopes when you want to have a user authorize your app to access their organization. You'll call the access token URL when you want to get an access token to call an Azure DevOps Services REST API.

The settings for each app that you register are available from your profile (<https://app.vssps.visualstudio.com/profile/view>).

Authorize your app

If your user hasn't yet authorized your app to access their organization, call the authorization URL.

```
https://app.vssps.visualstudio.com/oauth2/authorize  
?client_id={app ID}  
&response_type=Assertion  
&state={state}  
&scope={scope}  
&redirect_uri={callback URL}
```

PARAMETER	TYPE	NOTES
client_id	GUID	The ID assigned to your app when it was registered
response_type	string	Assertion
state	string	Can be any value. Typically a generated string value that correlates the callback with its associated authorization request.
scope	string	Scopes registered with the app. Space separated. See available scopes .
redirect_uri	URL	Callback URL for your app. This must exactly match the URL registered with the app

Azure DevOps Services will ask your user to authorize your app. It will handle authentication and then call you back with an authorization code, if the user approves the authorization.

Add a link or button to your site that navigates the user to the Azure DevOps Services authorization endpoint:

```
https://app.vssps.visualstudio.com/oauth2/authorize  
?client_id=88e2dd5f-4e34-45c6-a75d-524eb2a0399e  
&response_type=Assertion  
&state=User1  
&scope=vso.work%20vso.code_write  
&redirect_uri=https://fabrikam.azurewebsites.net/myapp/oauth-callback
```

Azure DevOps Services will ask the user to authorize your app.

Assuming the user accepts, Azure DevOps Services will redirect the user's browser to your callback URL, including a short-lived authorization code and the state value provided in the authorization URL:

```
https://fabrikam.azurewebsites.net/myapp/oauth-callback  
?code={authorization code}  
&state=User1
```

Get an access and refresh token for the user

Now use the authorization code to request an access token (and refresh token) for the user. This requires your service making a service-to-service HTTP request to Azure DevOps Services.

URL

```
POST https://app.vssps.visualstudio.com/oauth2/token
```

HTTP request headers

HEADER	VALUE
Content-Type	application/x-www-form-urlencoded
Content-Length	Calculated string length of the request body (see below)

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 1322
```

HTTP request body

```
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&client_assertion={0}&grant_type=urn:ietf:params:oauth:grant-type:jwt-bearer&assertion={1}&redirect_uri={2}
```

Replace the placeholder values in the sample request body above:

- **{0}**: URL encoded client secret acquired when the app was registered
- **{1}**: URL encoded "code" provided via the `code` query parameter to your callback URL
- **{2}**: callback URL registered with the app

C# example to form the request body

```
public string GenerateRequestpostData(string appSecret, string authCode, string callbackUrl)
{
    return String.Format("client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-
bearer&client_assertion={0}&grant_type=urn:ietf:params:oauth:grant-type:jwt-bearer&assertion={1}&redirect_uri=
{2}",
        HttpUtility.UrlEncode(appSecret),
        HttpUtility.UrlEncode(authCode),
        callbackUrl
    );
}
```

Response

```
{
    "access_token": { access token for the user },
    "token_type": { type of token },
    "expires_in": { time in seconds that the token remains valid },
    "refresh_token": { refresh token to use to acquire a new access token }
}
```

Important: securely persist the `refresh_token` so your app does not need to prompt the user authorize again. Access tokens expire relatively quickly and should not be persisted.

Use the access token

To use an access token, include it as a bearer token in the Authorization header of your HTTP request:

```
Authorization: Bearer {access_token}
```

For example, the HTTP request to [get recent builds](#) for a project:

```
GET https://dev.azure.com/myaccount/myproject/_apis/build-release/builds?api-version=3.0
Authorization: Bearer {access_token}
```

Refresh an expired access token

If a user's access token expires, you can use the refresh token acquired in the authorization flow to get a new access token. This process is similar to the original process for exchanging the authorization code for an access token and refresh token.

URL

```
POST https://app.vssps.visualstudio.com/oauth2/token
```

HTTP request headers

HEADER	VALUE
Content-Type	application/x-www-form-urlencoded
Content-Length	Calculated string length of the request body (see below)

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 1654
```

HTTP request body

```
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&client_assertion={0}&grant_type=refresh_token&assertion={1}&redirect_uri={2}
```

Replace the placeholder values in the sample request body above:

- **{0}**: URL encoded client secret acquired when the app was registered
- **{1}**: URL encoded refresh token for the user
- **{2}**: callback URL registered with the app

Response

```
{
  "access_token": { access token for this user },
  "token_type": { type of token },
  "expires_in": { time in seconds that the token remains valid },
  "refresh_token": { new refresh token to use when the token has timed out }
}
```

Important: a new refresh token will be issued for the user. Persist this new token and use it the next time you

need to acquire a new access token for the user.

Scopes

IMPORTANT: Scopes only enable access to REST APIs and select Git endpoints. SOAP API access is not supported.

CATEGORY	SCOPE	NAME	DESCRIPTION
Agent Pools	<code>vso.agentpools</code>	Agent Pools (read)	Grants the ability to view tasks, pools, queues, agents, and currently running or recently completed jobs for agents.
	<code>vso.agentpools_manage</code>	Agent Pools (read, manage)	Grants the ability to manage pools, queues, and agents.
Build	<code>vso.build</code>	Build (read)	Grants the ability to access build artifacts, including build results, definitions, and requests, and the ability to receive notifications about build events via service hooks.
	<code>vso.build_execute</code>	Build (read and execute)	Grants the ability to access build artifacts, including build results, definitions, and requests, and the ability to queue a build, update build properties, and the ability to receive notifications about build events via service hooks.
Code	<code>vso.code</code>	Code (read)	Grants the ability to read source code and metadata about commits, changesets, branches, and other version control artifacts. Also grants the ability to search code and get notified about version control events via service hooks.
	<code>vso.code_write</code>	Code (read and write)	Grants the ability to read, update, and delete source code, access metadata about commits, changesets, branches, and other version control artifacts. Also grants the ability to create and manage pull requests and code reviews and to receive notifications about version control events via service hooks.

CATEGORY	SCOPE	NAME	DESCRIPTION
	vso.code_manage	Code (read, write, and manage)	Grants the ability to read, update, and delete source code, access metadata about commits, changesets, branches, and other version control artifacts. Also grants the ability to create and manage code repositories, create and manage pull requests and code reviews, and to receive notifications about version control events via service hooks.
	vso.code_full	Code (full)	Grants full access to source code, metadata about commits, changesets, branches, and other version control artifacts. Also grants the ability to create and manage code repositories, create and manage pull requests and code reviews, and to receive notifications about version control events via service hooks. Also includes limited support for Client OM APIs.
	vso.code_status	Code (status)	Grants the ability to read and write commit and pull request status.
Entitlements	vso.entitlements	Entitlements (Read)	Provides read only access to licensing entitlements endpoint to get account entitlements.
	vso.memberentitlementmanagement	MemberEntitlement Management (read)	Grants the ability to read users, their licenses as well as projects and extensions they can access.
	vso.memberentitlementmanagement	MemberEntitlement Management (write)	Grants the ability to manage users, their licenses as well as projects and extensions they can access.
Extensions	vso.extension	Extensions (read)	Grants the ability to read installed extensions.
	vso.extension_manage	Extensions (read and manage)	Grants the ability to install, uninstall, and perform other administrative actions on installed extensions.

CATEGORY	SCOPE	NAME	DESCRIPTION
	vso.extension.data	Extension data (read)	Grants the ability to read data (settings and documents) stored by installed extensions.
	vso.extension.data_write	Extension data (read and write)	Grants the ability to read and write data (settings and documents) stored by installed extensions.
Graph & identity	vso.graph	Graph (read)	Grants the ability to read user, group, scope, and group membership information.
	vso.graph_manage	Graph (manage)	Grants the ability to read user, group, scope and group membership information, and to add users, groups, and manage group memberships.
	vso.identity	Identity (read)	Grants the ability to read identities and groups.
	vso.identity_manage	Identity (manage)	Grants the ability to read, write, and manage identities and groups.
Load Test	vso.loadtest	Load test (read)	Grants the ability to read your load test runs, test results, and APM artifacts.
	vso.loadtest_write	Load test (read and write)	Grants the ability to create and update load test runs, and read metadata including test results and APM artifacts.
Machine Group	vso.machinegroup_manage	Deployment group (read, manage)	Provides ability to manage deployment group and agent pools.
Marketplace	vso.gallery	Marketplace	Grants read access to public and private items and publishers.
	vso.gallery_acquire	Marketplace (acquire)	Grants read access and the ability to acquire items.
	vso.gallery_publish	Marketplace (publish)	Grants read access and the ability to upload, update, and share items.

CATEGORY	SCOPE	NAME	DESCRIPTION
	vso.gallery_manage	Marketplace (manage)	Grants read access and the ability to publish and manage items and publishers.
Notifications	vso.notification	Notifications (read)	Provides read access to subscriptions and event metadata, including filterable field values.
	vso.notification_write	Notifications (write)	Provides read and write access to subscriptions and read access to event metadata, including filterable field values.
	vso.notification_manage	Notifications (manage)	Provides read, write, and management access to subscriptions and read access to event metadata, including filterable field values.
	vso.notification_diagnostics	Notifications (diagnostics)	Provides access to notification-related diagnostic logs and provides the ability to enable diagnostics for individual subscriptions.
Packaging	vso.packaging	Packaging (read)	Grants the ability to read feeds and packages.
	vso.packaging_write	Packaging (read and write)	Grants the ability to create and read feeds and packages.
	vso.packaging_manage	Packaging (read, write, and manage)	Grants the ability to create, read, update, and delete feeds and packages.
Project and Team	vso.project	Project and team (read)	Grants the ability to read projects and teams.
	vso.project_write	Project and team (read and write)	Grants the ability to read and update projects and teams.
	vso.project_manage	Project and team (read, write and manage)	Grants the ability to create, read, update, and delete projects and teams.
Release	vso.release	Release (read)	Grants the ability to read release artifacts, including releases, release definitions and release environment.

CATEGORY	SCOPE	NAME	DESCRIPTION
	vso.release_execute	Release (read, write and execute)	Grants the ability to read and update release artifacts, including releases, release definitions and release environment, and the ability to queue a new release.
	vso.release_manage	Release (read, write, execute and manage)	Grants the ability to read, update, and delete release artifacts, including releases, release definitions and release environment, and the ability to queue and approve a new release.
Security	vso.security_manage	Security (manage)	Grants the ability to read, write, and manage security permissions.
Service Connections	vso.serviceendpoint	Service Endpoints (read)	Grants the ability to read service endpoints.
	vso.serviceendpoint_query	Service Endpoints (read and query)	Grants the ability to read and query service endpoints.
	vso.serviceendpoint_manage	Service Endpoints (read, query and manage)	Grants the ability to read, query, and manage service endpoints.
Symbols	vso.symbols	Symbols (read)	Grants the ability to read symbols.
	vso.symbols_write	Symbols (read and write)	Grants the ability to read and write symbols.
	vso.symbols_manage	Symbols (read, write and manage)	Grants the ability to read, write, and manage symbols.
Task Groups	vso.taskgroups_read	Task Groups (read)	Grants the ability to read task groups.
	vso.taskgroups_write	Task Groups (read, create)	Grants the ability to read and create task groups.
	vso.taskgroups_manage	Task Groups (read, create and manage)	Grants the ability to read, create and manage taskgroups.
Team Dashboard	vso.dashboards	Team dashboards (read)	Grants the ability to read team dashboard information.

CATEGORY	SCOPE	NAME	DESCRIPTION
	vso.dashboards_manage	Team dashboards (manage)	Grants the ability to manage team dashboard information.
Test Management	vso.test	Test management (read)	Grants the ability to read test plans, cases, results and other test management related artifacts.
	vso.test_write	Test management (read and write)	Grants the ability to read, create, and update test plans, cases, results and other test management related artifacts.
Tokens	vso.tokens	Delegated Authorization Tokens	Grants the ability to manage delegated authorization tokens to users.
	vso.tokenadministration	Token Administration	Grants the ability to manage (view and revoke) existing tokens to organization administrators.
User Profile	vso.profile	User profile (read)	Grants the ability to read your profile, accounts, collections, projects, teams, and other top-level organizational artifacts.
	vso.profile_write	User profile (write)	Grants the ability to write to your profile.
Variable Groups	vso.variablegroups_read	Variable Groups (read)	Grants the ability to read variable groups.
	vso.variablegroups_write	Variable Groups (read, create)	Grants the ability to read and create variable groups.
	vso.variablegroups_manage	Variable Groups (read, create and manage)	Grants the ability to read, create and manage variable groups.
Wiki	vso.wiki	Wiki (read)	Grants the ability to read wikis, wiki pages and wiki attachments. Also grants the ability to search wiki pages.
	vso.wiki_write	Wiki (read and write)	Grants the ability to read, create and update wikis, wiki pages and wiki attachments.

CATEGORY	SCOPE	NAME	DESCRIPTION
Work Items	vso.work	Work items (read)	Grants the ability to read work items, queries, boards, area and iterations paths, and other work item tracking related metadata. Also grants the ability to execute queries, search work items and to receive notifications about work item events via service hooks.
	vso.work_write	Work items (read and write)	Grants the ability to read, create, and update work items and queries, update board metadata, read area and iterations paths other work item tracking related metadata, execute queries, and to receive notifications about work item events via service hooks.
	vso.work_full	Work items (full)	Grants full access to work items, queries, backlogs, plans, and work item tracking metadata. Also provides the ability to receive notifications about work item events via service hooks.

When you [register your app](#), you'll use scopes to indicate which permissions in Azure DevOps Services your app will require. When your users authorize your app to access their organization, they'll authorize it for those scopes. When you call to [request that authorization](#), you'll pass the same scopes that you registered.

Samples

You can find a C# sample that implements OAuth to call Azure DevOps Services REST APIs in our [C# OAuth GitHub Sample](#).

Q&A

Q: Can I use OAuth with my phone app?

A: No. Right now, Azure DevOps Services only support the web server flow, so there's no supported way to implement OAuth for Azure DevOps Services from an app like a phone app, since there's no way to securely store the app secret.

Q: What errors or special conditions do I need to handle in my code?

A: Make sure that you handle these conditions:

1. If your user denies your app access, no authorization code is returned. Don't use the authorization code without checking for that.
2. If your user revokes your app's authorization, the access token is no longer valid. When your app uses the token to access data, a 401 error is returned. You'll have to request authorization again.

Q: I want to debug my web app locally. Can I use localhost for the callback URL when I register my app?

A: Azure DevOps Services does not allow localhost to be the hostname in your callback URL. You can edit the hosts file on your local computer to map a hostname to 127.0.0.1. Then use this hostname when you register your app. Or, you can deploy your app when testing to a Microsoft Azure website to be able to debug and use HTTPS for the callback URL.

Q: I get an HTTP 400 error when I try to get an access token. What might be wrong?

A: Check that you set the content type to application/x-www-form-urlencoded in your request header.

Q: Can I use OAuth with the SOAP endpoints as well as the REST APIs?

A: No. OAuth is only supported in the REST APIs at this point.

2 minutes to read

Revoke personal access tokens for organization users

5/7/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

If an organization user's personal access token (PAT) has been compromised, we recommend taking immediate action. Revoke their access tokens, as a precaution to protect your organization. In this article, we show you how administrators of Azure DevOps organizations can revoke PATs for users.

Prerequisites

Only an organization administrator or project collection administrator (PCA) can revoke user PATs. If you're not a member of the **Project Collection Administrators** group, [get added as one](#). To learn how to find your organization's admin, see [Look up administrators and organization owner](#).

For users, if you want to create or revoke your own PATs, see [Create or revoke personal access tokens](#).

Revoke PATs

1. To revoke the OAuth authorizations, including PATs, for your organization's users, see [Token revocations - Revoke authorizations](#).
2. Use this [PowerShell script](#) to automate calling the new REST API by passing a list of user principal names (UPNs). If you don't know the UPN of the user who created the PAT, use this script, however it must be based on a date range.

NOTE

Keep in mind that when you use a date range any JSON web tokens (JWTs) are also revoked. Also be aware that any tooling that relies on these tokens won't work until refreshed with new tokens.

1. After you've successfully revoked the affected PATs, let your users know. They can recreate their tokens, as needed.

Token expiration

FedAuth tokens

A FedAuth token is issued when you sign-in. It is valid for a seven day sliding window. The expiry automatically extends another seven days whenever you refresh it within the sliding window. If users access the service regularly, only an initial sign-in is needed. After a period of inactivity extending seven days, the token becomes invalid and the user must sign in again.

Personal access tokens

Users can choose an expiry date for their personal access token, not to exceed one year. We recommend you use shorter time periods, generating new PATs upon expiry. Users receive a notification email one week before token expiry. Users can generate a new token, extend expiry of the existing token, or change the scope of the existing token, if needed.

Frequently asked questions (FAQs)

What if a user leaves my company?

A: Once a user is removed from Azure AD, the PATs and FedAuth tokens are invalidated within an hour, since the refresh token is valid only for one hour.

What about JSON web tokens (JWTs)?

A: Revoke JWTs, issued as part of the OAuth flow, via the [PowerShell script](#). However, you must use the date range option in the script.

Related articles

- [How Microsoft protects your projects and data in Azure DevOps](#)
- [Create or revoke your personal access tokens](#)

Manage teams

5/7/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Give your teams the autonomy they need as your organization grows. Add teams to give each team their set of Agile tools which they can configure their way.

5-Minute Quickstarts

- [Define area paths & assign to a team](#)
- [Define iteration paths \(sprints\) & configure team iterations](#)
- [Add a team, move from one default team to several teams](#)
- [Add a team administrator](#)
- [Manage teams and configure team tools](#)
- [Add users to a project or team](#)

Concepts

- [Area & iteration paths \(aka sprints\)](#)

How-to Guides

- [Manage teams and configure team tools](#)

Reference

- [Default permissions and access](#)

Resources

- [Web portal navigation](#)

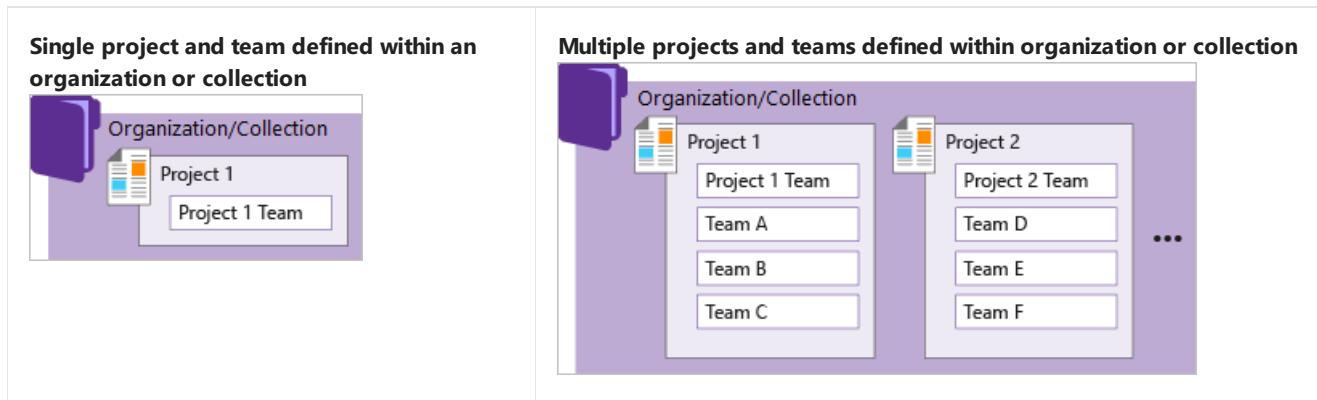
About projects and scaling your organization

6/3/2019 • 8 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

A project provides a repository for source code and a place for a group of people to plan, track progress, and collaborate on building software solutions. It represents a fundamental container where data is stored when added to Azure DevOps.

When you create your project, a team of the same name is automatically created. For small teams, this is sufficient. However, for enterprise-level organizations, it may be necessary to scale up, to create additional teams and/or projects. These can be created within the single account or collection.



The collection-project-team structure provides teams a high-level of autonomy to configure their tools in ways that work for them. It also supports administrative tasks to occur at the appropriate level. As your organization grows, your tools can grow to support a [culture of team autonomy as well as organizational alignment](#).

How do you manage work across the enterprise?

How do you scale your DevOps and Agile tools to support your growing enterprise?

When you connect to Azure DevOps, you connect to an organization or project collection. Within that container, one or more projects may be defined. At a minimum, at least one project must be created in order to use the system.

You can scale your organization in the following ways:

- To support different business units, you can add projects
- Within a project, you can add teams
- Add repositories and branches
- To support continuous integration and deployment, you can add agents, agent pools, and deployment pools
- To manage a large number of users, you can manage access through Azure Active Directory

You can scale your on-premises TFS deployment in the following ways:

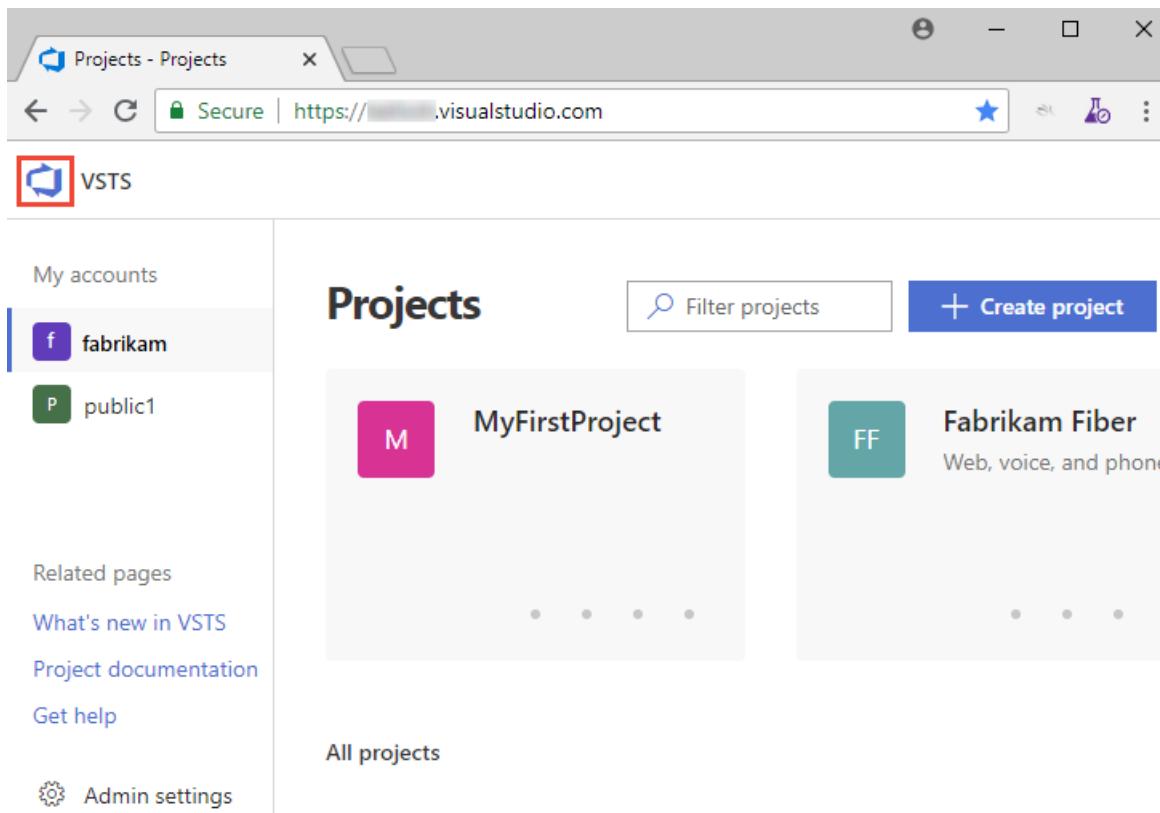
- To increase performance, you can add server instances
- To support different business units, you can add project collections and projects
- Within a project, you can add teams
- Add repositories and branches
- To support continuous integration and deployment, you can add agents, agent pools, and deployment pools
- To manage a large number of users, you can manage access through Active Directory

Both Azure DevOps Services and Azure DevOps Server are enterprise-ready platforms that support teams of any size, from tens to thousands. Azure DevOps Services, our cloud service, provides a scalable, reliable, and globally available hosted service. It is backed by a 99.9% SLA, monitored by our 24x7 operations team, and available in local data centers around the world.

How to view projects defined for your organization or collection

You can view the projects defined for your organization by opening the **Projects** page.

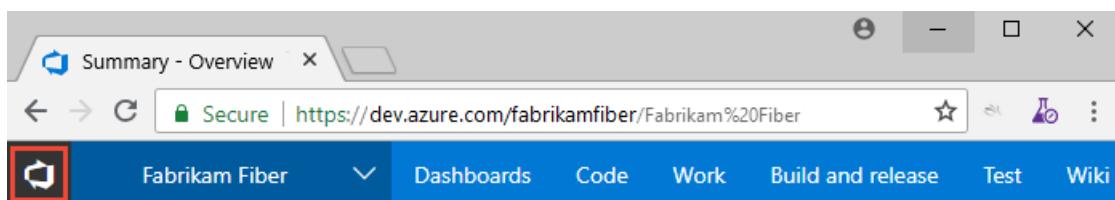
1. Choose the  Azure DevOps logo to open **Projects**.



The screenshot shows the 'Projects' page in VSTS. On the left, there's a sidebar with 'My accounts' (fabrikam, public1) and 'Related pages' (What's new in VSTS, Project documentation, Get help, Admin settings). The main area is titled 'Projects' with a search bar and a '+ Create project' button. It lists two projects: 'MyFirstProject' (pink icon, M) and 'Fabrikam Fiber' (teal icon, FF). Below the projects is a 'All projects' link.

2. From there, you can choose a project from the set of projects listed.

1. Choose the  Azure DevOps logo to open **Projects**.



The screenshot shows the 'Summary - Overview' page for the 'Fabrikam Fiber' project. At the top, it says 'Summary - Overview' and shows the URL 'https://dev.azure.com/fabrikamfiber/Fabrikam%20Fiber'. The page has a navigation bar with links: Dashboards, Code, Work, Build and release, Test, and Wiki. The 'Work' tab is highlighted.

2. From there, you can choose a project from the set of projects listed.

Search work items in this collection

Good evening, Jamal Hartnett

Projects My favorites My work items My pull requests ...

Filter projects and teams

New Project

Recent

FabrikamFiber

FabrikamFiberTest

1. Choose the name of the server.

Visual Studio Team Foundation Server 2015 / Fabrikam Fiber

HOME CODE WORK BUILD TEST

Welcome | Overview +

2. From there, you can choose a project from the set of projects listed.

When to add another project

In general, we recommend that you use a single project to support your organization or enterprise. A single project minimizes the maintenance of administrative tasks and supports the most optimized / full-flexibility [cross-link object](#) experience.

Even if you have many teams working on hundreds of different applications and software projects, you can most easily manage them within a single project. A project serves to isolate data stored within it; you can't easily move data from one project to another. When you move data from one project to another, you typically lose the history associated with that data.

Reasons to add another project

Instances where you may want to add another project include the following:

- To prohibit or manage access to the information contained within a project to select groups
- 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 prior to rolling out changes to the working project
- To support an Open Source Software (OSS) project

Instances where you may want to add another project include the following:

- To prohibit or manage access to the information contained 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 prior to rolling out changes to the working project

Private and public projects

You can add either public or private projects to your organization. You can also [change the visibility of a project from private to public](#).

Private projects require that you add and manage user access. Users must sign-in to gain access to a project, even if it is read-only access. All users added to a project gain access to information contained with the project and organization. For details, see [Resources granted to project members](#).

A public project, on the other hand, doesn't require users to sign in to gain read-only access to many of the services. Public projects provide support to share code with others and to support continuous integration/continuous deployment (CI/CD) of open source software. To learn more about public projects, see [What is a public project?](#).

Structure your project

When you add a project, look at using the following elements to structure it to support your business needs:

- [Create a Git repository](#) for each sub-project or application, or [create root folders within a TFVC repository](#) for each sub-project.
- [Define area paths](#) to support different sub-projects, products, features, or teams.
- [Define iteration paths \(aka sprints\)](#) that can be shared across teams.
- [Add a team](#) for each product team that develops a set of features for a product. Note that each team you create automatically creates a security group for that team which you can use to manage permissions for a team. See also, [Portfolio management](#).
- [Grant or restrict access to select 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.

Customizing and configuring projects

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 perform the following tasks. For a comprehensive view of what 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 their 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 details, see [Customize an inheritance process](#).
- **Build and Release:** You can fully customize your build and release pipelines, define build steps, release environments, and deployment schedule. For details, see [Build and Release](#).
- **Test:** You can define and configure test plans, test suites, and test cases as well as configure test environments; additionally you can add test steps within your build pipelines. For details, see [Exploratory & Manual Testing](#) and [continuous testing for your builds](#).
- **Dashboards:** Each team can [configure their set of dashboards](#) to share information and monitor their 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 details, see [Customize the On-premises XML process model](#).
- **Build and Release:** You can fully customize your build and release pipelines, define build steps, release

environments, and deployment schedule. For details, see [Build and Release](#).

- **Test:** You can define and configure test plans, test suites, and test cases as well as configure test environments; additionally you can add test steps within your build pipelines. For details, see [Exploratory & Manual Testing](#) and [continuous testing for your builds](#).

When to add a team, scaling Agile tools across the enterprise

As your organization grows, you'll want to add teams to provide them the Agile tools that each team can configure to meet their workflow. To learn more, see the following articles.

- [Scale Agile to large teams](#)
- [About teams and Agile tools](#)
- Manage a [portfolio of backlogs](#) and gain insight into each team's progress as well as the progress of all programs.
- Use [Delivery plans](#) to review the schedule of stories or features your teams plan to deliver. Delivery plans show the 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](#).

To review stories and short videos on how Microsoft transitioned from waterfall to Agile, see [Scaling Agile Across the Enterprise](#).

Clients that support connection to a project

In addition to connecting through 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](#)
- [Eclipse: Team Explorer Everywhere](#)
- [Office Excel](#)
- [Office Project](#)
- [PowerPoint Storyboarding](#)
- [Azure Test Plans \(formerly Test Manager\)](#)
- [Microsoft Feedback Client](#)

See also, [Compatibility with Azure DevOps Server versions](#).

Related articles

- [Get started as an administrator](#)
- [Web portal navigation](#)
- [What do I get with a project?](#)
- [Understand differences between Azure DevOps](#)

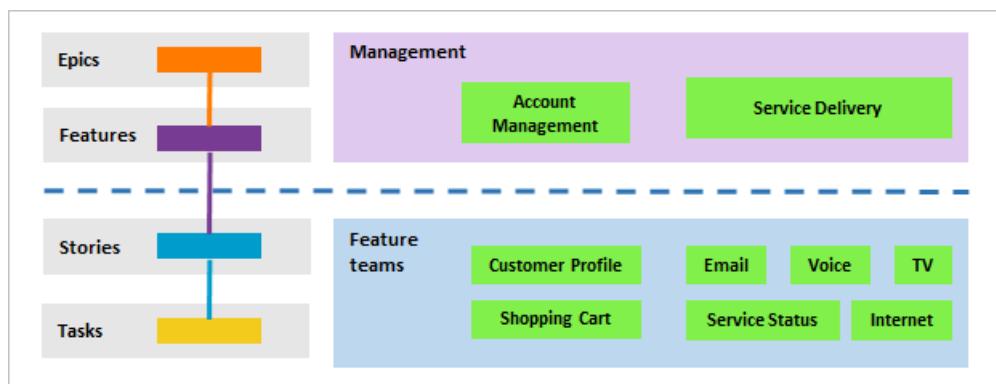
About teams and Agile tools

5/24/2019 • 8 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Adding a team is the #1 way in which Agile tools supports a growing organization. Once your team grows beyond its optimum size—typically anywhere from 6 to 9 members—you might consider moving from a one team structure to a two team structure. For enterprises adopting Agile tools, setting up a hierarchical team structure provides several advantages to portfolio and program managers to track progress across several teams.

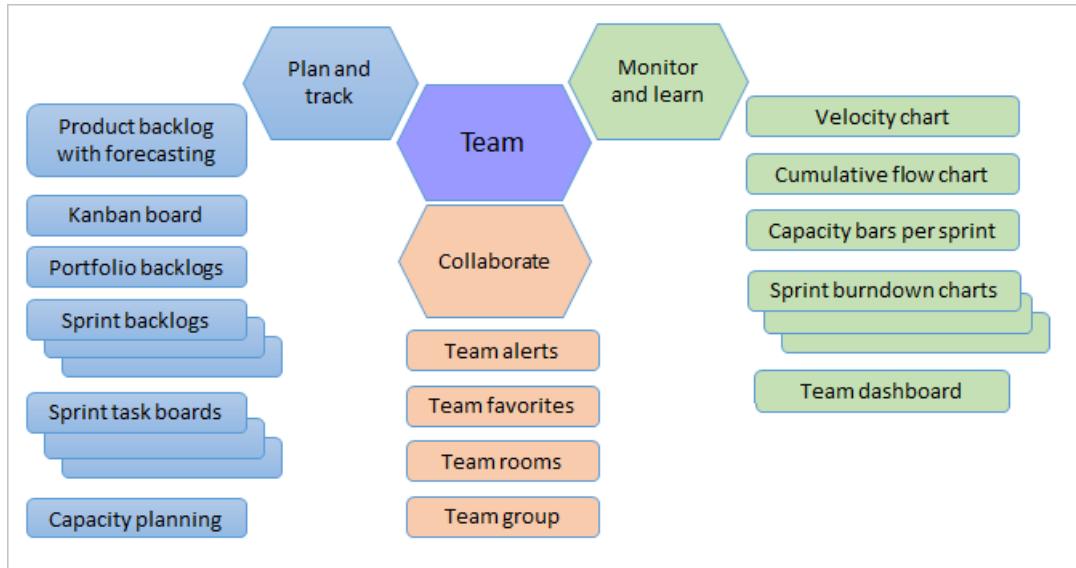
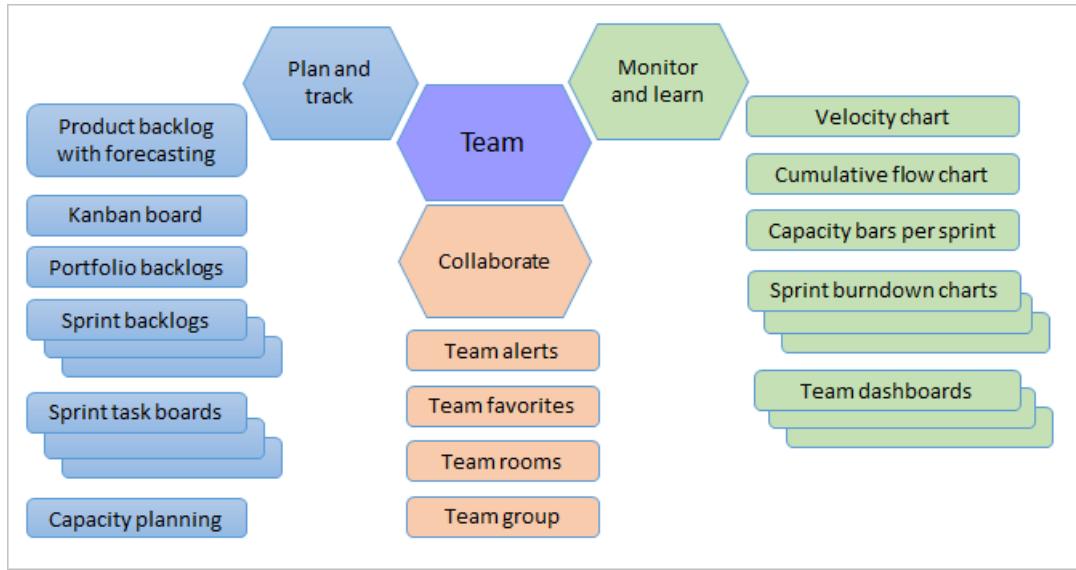
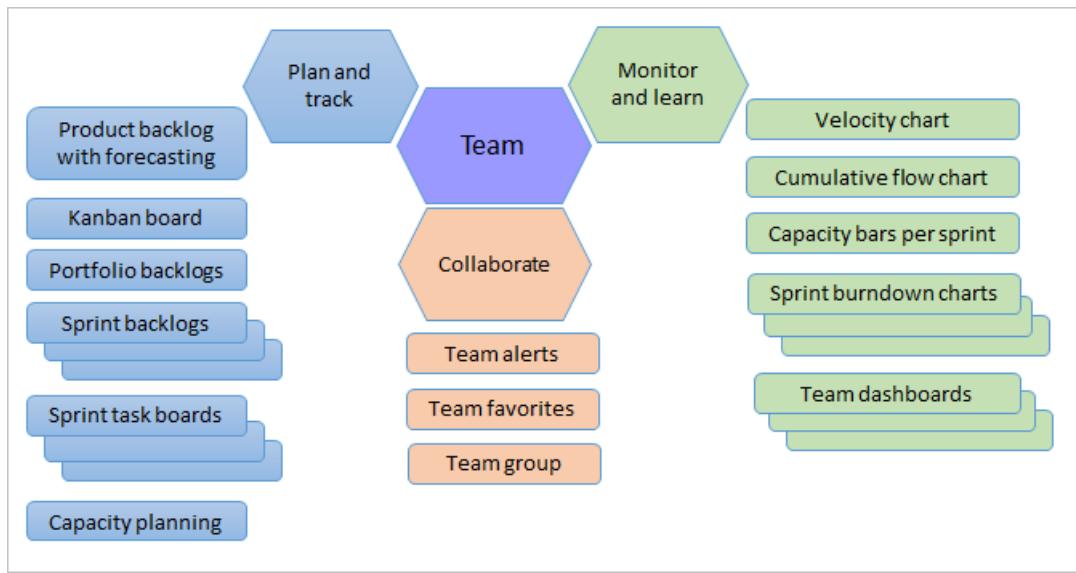
Depending on the size of your organization and your tracking needs, you can set up a team structure similar to the one shown. You do this by defining teams and their associated area path(s).



For example, each feature team can be associated with a single feature area path—such as *Customer Profile*, *Shopping Cart*, *Email*—or several area paths. Each management team, which focuses on a set of features, can choose several area paths to monitor. This allows each feature team to have their distinct backlog to plan, prioritize, and track their work. And, portfolio or product owners can create their vision, road map, and goals for each release, monitor progress across their portfolio of projects, and manage risks and dependencies. To learn more, see [Portfolio management](#).

Each team gets their own set of tools

Each team you create gets access to a suite of Agile tools and team assets. These tools provide teams the ability to work autonomously and collaborate with other teams across the enterprise. Each team can configure and customize each tool to support how they work.



These tools reference the team's default area path, iteration path, and selected sprints to automatically filter the set of work items they display. To learn more about each tool and the configuration settings for each tool, see the corresponding articles.

AREA	TOOL	TEAM CONFIGURATION TASKS
------	------	--------------------------

Backlogs	<ul style="list-style-type: none"> Product backlog Features backlog Epics backlog Forecast 	<ul style="list-style-type: none"> Configure area paths Select active iteration paths (sprints) Select backlog levels Show bugs on backlogs & boards
Sprints and Scrum	<ul style="list-style-type: none"> Sprint backlogs Sprint capacity Task board Sprint burndown 	<ul style="list-style-type: none"> Select active iteration paths (sprints) Set working days
Kanban boards	<ul style="list-style-type: none"> Kanban board Features board Epics board Cumulative flow 	<ul style="list-style-type: none"> Configure area paths Select default iteration path Select backlog levels Show bugs on backlogs & boards
Widgets	<ul style="list-style-type: none"> New work item Sprint burndown Sprint capacity Sprint overview Team members 	<ul style="list-style-type: none"> Configure area paths Select active iteration paths (sprints) Add team members
Other tools	<ul style="list-style-type: none"> Favorites Work item templates Delivery plans Queries Velocity Dashboards Alerts 	Not applicable

AREA	TOOL	TEAM CONFIGURATION TASKS
Backlogs	<ul style="list-style-type: none"> Product backlog Features backlog Epics backlog Forecast 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Select backlog levels Show bugs on backlogs & boards
Sprints and Scrum	<ul style="list-style-type: none"> Sprint backlogs Sprint capacity Task board Sprint burndown 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Set working days
Kanban boards	<ul style="list-style-type: none"> Kanban board Features board Epics board Cumulative flow 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Select backlog levels Show bugs on backlogs & boards

Widgets	<ul style="list-style-type: none"> New work item Sprint burndown Sprint capacity Sprint overview Team members 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Add team members
Other tools	<ul style="list-style-type: none"> Favorites Work item templates Queries Velocity Dashboards Team rooms Alerts 	Not applicable

AREA	TOOL	TEAM CONFIGURATION TASKS
Backlogs	<ul style="list-style-type: none"> Product backlog Features backlog Forecast 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Show bugs on backlogs & boards
Sprints and Scrum	<ul style="list-style-type: none"> Sprint backlog Sprint capacity Task board Sprint burndown 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Set working days
Kanban boards	<ul style="list-style-type: none"> Kanban board Features board Cumulative flow 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Select backlog levels Show bugs on backlogs & boards
Widgets	<ul style="list-style-type: none"> New work item Sprint burndown Sprint capacity Sprint overview Team members 	<ul style="list-style-type: none"> Configure area paths Select default, current, and active iteration paths (sprints) Add team members
Other tools	<ul style="list-style-type: none"> Favorites Work item templates Queries Velocity Team home page Team rooms Alerts 	Not applicable

Many of these tools are built from system queries that reference the team area path. For example, a team's default area path filters the work items that appear on a team's backlog. Also, work items that you create using an Agile tool auto-assign the areas and iterations based on team defaults.

Team defaults referenced by backlogs and boards

What work items appear on team backlogs and boards? When you add work items to a backlog or board, how are team defaults used to assign field values?

Teams are associated with one or more area paths and a backlog iteration path which determine what items appear on their backlogs and boards.

When you define a team, you define the team's:

- Selected area path(s)
- Default area path
- Selected iteration path(s)
- Backlog iteration path
- Default iteration path

All Agile tools reference the area path(s) defined for a team. The set of work items that appear on a backlog or board depend on the current State of a work item or it's parent-child status.

In addition, several tools reference the team's default iteration and selected iteration paths or sprints. For example, when you add new work items from a backlog or board view, or from a team dashboard, the system assigns the team's default area path and default iteration path to these work items.

AGILE TOOL	AREA PATH (SEE NOTE 1)	ITERATION PATH	STATE
Portfolio or product backlogs	Selected area path(s)	Equal to or under team's backlog iteration path	Active (corresponds to a Proposed or InProgress state category, see notes 2, 3)
Kanban boards (see note 4)	Selected area path(s)	Equal to or under team's backlog iteration path	Any state (see notes 3, 5)
Sprint backlogs (see note 4)	Selected area path(s)	Team's selected iteration paths	Any state (see notes 3, 5)
Task boards (see note 4)	Selected area path(s)	Team's selected iteration paths	Any state (see notes 3, 5)
New work item widget	Default area path	Default iteration path	n/a

Notes:

1. Agile tools filter items based on the team's selected area path(s). Teams can choose [whether to include or exclude items assigned to subarea paths](#).
2. Work items whose State equals Closed, Done, or Removed (corresponding to a Completed category state) don't appear on portfolio and product backlogs.
3. You can add custom workflow states and assign them to one of three state categories. The [state categories](#) determine which work items appear on backlog and board views.
4. Kanban boards, sprint backlogs, and task boards only show the last node in a hierarchy, called the leaf node. For example, if you link items within a hierarchy that is four levels deep, only the items at the fourth level appear on the Kanban board, sprint backlog, and task board. To learn more, see [parent-child links between items](#).
5. Work items whose State equals Removed don't appear on boards.

Structure hierarchical teams or scale agility within an enterprise

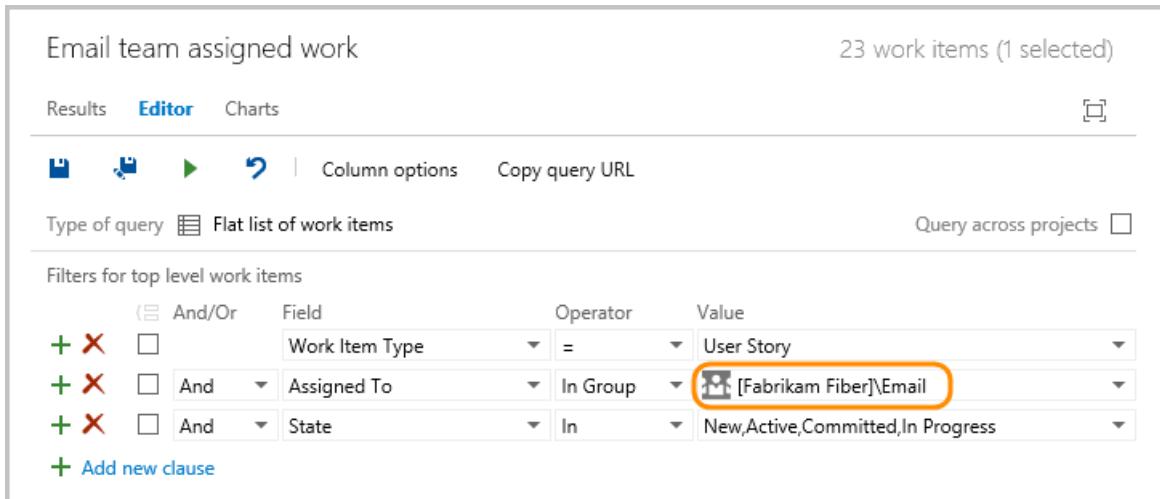
Although there is no concept of sub-teams, you can create teams whose area paths are under another team, which effectively creates a hierarchy of teams. To learn more, see [Add another team](#).

Also, these topics can walk you through the steps for configuring teams, area paths, and iterations to support portfolio management or enterprise organizations:

- [Portfolio management](#)
- [Implement Scaled Agile Framework to support epics, release trains, and multiple backlogs](#)

Team groups

When you add a team, a security group is automatically created with the team name. You can use this group to filter queries. The name of team groups follows the pattern **[Project Name]\Team Name**. For example, the following query finds work assigned to members of the **[Fabrikam Fiber]\Email** team group.



The screenshot shows a query editor interface with the title "Email team assigned work" and a count of "23 work items (1 selected)". Below the title are tabs for "Results", "Editor" (which is selected), and "Charts". There are also icons for export, copy, and search, along with "Column options" and "Copy query URL". Under "Type of query", the "Flat list of work items" option is selected. A checkbox for "Query across projects" is present. The main area is titled "Filters for top level work items" and contains the following clauses:

And/Or	Field	Operator	Value
+ X	Work Item Type	=	User Story
+ X	Assigned To	In Group	[Fabrikam Fiber]\Email
+ X	State	In	New,Active,Committed,In Progress

A green "+ Add new clause" button is at the bottom left.

You can also use the **@mention** control within discussions and pull requests to notify all members of a team. Simply start typing the name of a team or a security group, click the search icon and then select from the options listed. To learn more, see [Use @mentions to further discussion](#).

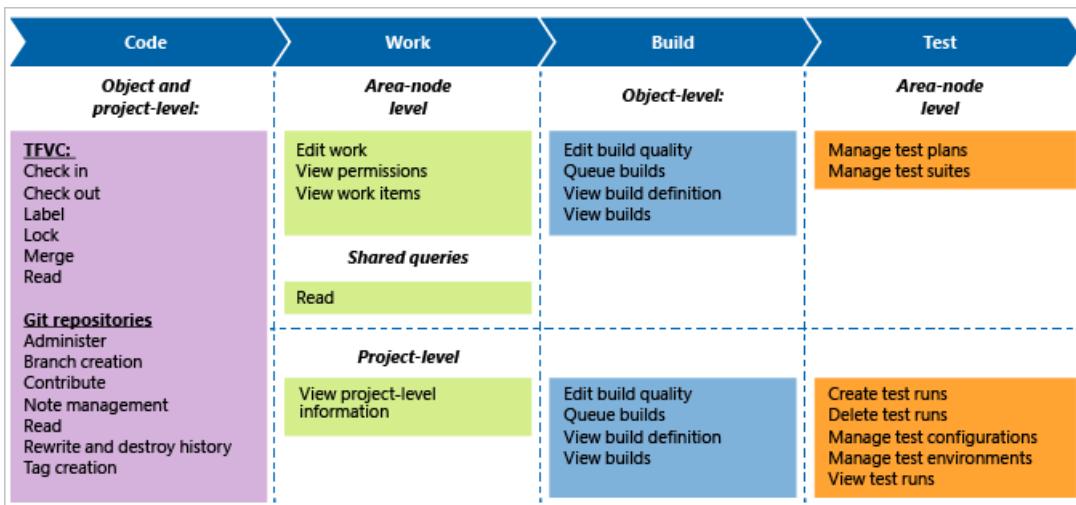
Work on more than one team

Can a user account belong to more than one team?

Yes. When you add user accounts to a project, you can add them as members of the project, or you can add them to one or more teams added to the project. If you work on two or more Scrum teams, you'll want to make sure you, [specify your sprint capacity for each team you work on](#).

Team member permissions

By default, team members inherit the permissions afforded to members of the project Contributors group. Members of this group can add and modify source code, create and delete test runs, and create and modify work items. They can collaborate with other team members and [collaborate on a Git project](#) or [check in work to the team's code base](#).



You can choose to limit access to select features by making a user a [Stakeholder](#) or limiting their access to read-only. For an overview of default permissions and access assignments set for work tracking features and built-in groups, see [Permissions and access for work tracking](#).

Summary

- Every team owns their own backlog, to create a new backlog you [create a new team](#)
- Every backlog has a corresponding [Kanban board](#) you can use to track progress and update status
- The team's specified area and iteration paths determine which work items appear on the backlog and Kanban board—you can easily decide to include or exclude work items under a specific area path
- Each team can control how [bugs show up on their backlogs and boards](#)
- For an overview of all team assets and how to configure them, see [Manage teams and configure team tools](#)
- To have work performed by several teams roll up in to a portfolio backlog, you'll want to [setup the team hierarchy](#)
- To add fields or work item types, see [Customize your work tracking experience](#).

Related articles

- [Add another team](#)
- [Configure team settings](#)
- [Work across projects](#)

Define area paths and assign to a team

6/14/2019 • 8 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

You can add area paths to support teams and to group work items based on product, feature, or business areas. Then, define area paths at the project level and assign them to a team under the team configuration. You can also create a hierarchy of area paths to support subcategories within categories.

Each team has access to a number of Agile tools as described in [About teams and Agile tools](#). Each tool references the team's default area path(s). Most teams choose one area path and several iteration paths to support their work tracking activities. However, to support other scenarios, it's possible for teams to choose several area paths to appear on their backlogs and boards.

New projects contain a single, root area that corresponds to the project name. A team is created with the same project name and the root area path is assigned to that team.

To understand how the system uses area paths, see [About area and iteration paths](#).

IMPORTANT

Make sure that you select the correct version of this article for Azure DevOps Services or Azure DevOps Server, renamed from Team Foundation Server (TFS). The version selector is located above the table of contents.

Prerequisites

- Add Area Paths to a project. If you don't have a project yet, [create one now](#).
- Ensure you're a member of the **Project Administrators** group to add an Area Path under the root node or edit or delete any child node. To acquire these permissions, see [Set permissions at the project- or collection-level](#).
- Have one or more of the following permissions set to **Allow**, to add, edit, and manage Area Paths under a node:
 - **Create child nodes**
 - **Delete this node**
 - **Edit this node**
 - **View permissions in this node**
- Ensure you're [added as a team administrator](#) or are a member of the **Project Administrators** group to set team Area Paths.

For naming restrictions on Area Paths, see [About areas and iterations, Naming restrictions](#).

Get started sequence

If you're new to managing projects and teams, the most straight forward sequence for configuring your project and teams is as follows:

1. Determine the number and names of Area Paths that you want to support to categorize your work. At a minimum, you'll want to add one Area Path for each team that you'll define. For guidance, review [About areas and iterations](#).
2. Determine the number and names of teams you want to support. For guidance, review [About teams and Agile tools](#).
3. Open **Project settings>Project configuration** and define the Area Paths to support steps 1 and 2 at the project level. Follow the steps provided later in this article: [Open Project Settings](#), [Project configuration](#) and [Add area paths](#).
4. Define the teams you need to support step 2. For guidance, see [Add a team, move from one default team to several teams](#).
5. Open the team configuration and assign the default and additional Area Path(s) to each team. Follow the steps provided later in this article: [Open team settings](#) and [Set team default area path\(s\)](#).
6. Assign the Area Path of work items to an area path you defined. Use [bulk modify](#) to modify several work items at once.

NOTE

While you can assign the same area path to more than one team, this can cause problems if two teams claim ownership over the same set of work items. To learn more, see [About boards and Kanban](#), [Limitations of multi-team Kanban board views](#).

As needed, you can do the following actions at any time:

- Add additional child nodes
- Rename an Area Path (except the root area path)
- Move a child node under another node
- Delete a child node
- Rename a team
- Change the Area Path assignments made to a team

Open Project Settings

You define both areas and iterations for a project from the **Project Settings>Work>Project configuration**.

1. From the web portal, open **Project Settings**.
2. Choose (1) **Project Settings**, expand **Work** if needed, and choose (2) **Project configuration** and then (3) **Areas**.

Project Settings > Project configuration

General

- Iterations
- Areas** (highlighted)
- Overview
- Services
- Teams
- Security
- Notifications
- Service hooks
- Dashboards

Boards

- Project configuration** (highlighted)
- Team configuration

Work

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](#).

New	New child	[+]	[x]
Areas	Teams		
Fabrikam Fiber		Fabrikam Fiber Team, Management team	
Customer Service		Customer Service, Fabrikam Fiber Team	
Email		Email, Fabrikam Fiber Team	
Phone		Fabrikam Fiber Team, Phone	
Voice		Fabrikam Fiber Team, Voice	
Web		Fabrikam Fiber Team, Web	

You define both areas and iterations from the **Work** pages of the project admin context. From the user context, you open the admin context by choosing the gear icon.

- From the web portal for the project, choose the gear icon.

Fabrikam Fiber

Backlogs (highlighted)

Work Items

Work Backlogs Queries* Plans

If you're currently working from a team context, then hover over the and choose **Project settings**.

Fabrikam Fiber / Fabrika...

Files (highlighted)

Commits Pushes Branches Tags Pull

master < Fabrikam Fiber / Type to find a file or folder...

Name ↑	Last change
M+ page-1.md	10/15/2023
M+ page-2.md	10/15/2023
M+ page-3.md	9/21/2023
M+ README.md	5/19/2023

Project settings (highlighted)

2. Choose **Work**.

1. From the web portal, choose the gear icon to open project administration pages. Then choose **Areas**.



The screenshot shows the Visual Studio Team Foundation Server 2015 web interface. At the top, there's a navigation bar with links for HOME, CODE, WORK, BUILD, and TEST. Below the navigation bar, the page title is "Fabrikam Fiber". On the right side of the header, there's a user profile for "Helena Peterson" and icons for settings and help. A search bar labeled "Search work items" is also present. The main content area has tabs for "Welcome" and "Overview" (which is currently selected), and a green plus sign icon.

Add an area path

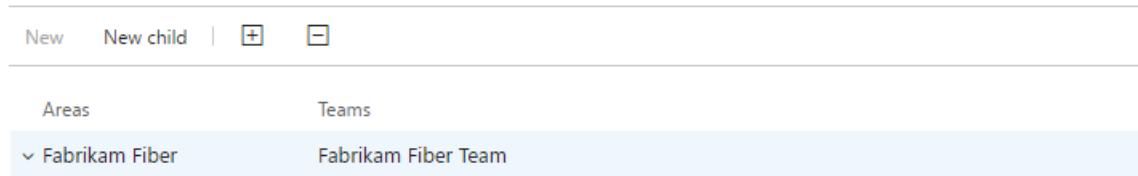
If you haven't added any areas or teams, you'll see that only one area is defined. You add area paths under the root area path for the project, or as a child to another area path.

Work

Iterations **Areas**

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
▼ Fabrikam Fiber	Fabrikam Fiber Team

- To add a child node, highlight the area path and then choose **New child**. Optionally, you can open the **...** context menu for the area path and choose **New child**.

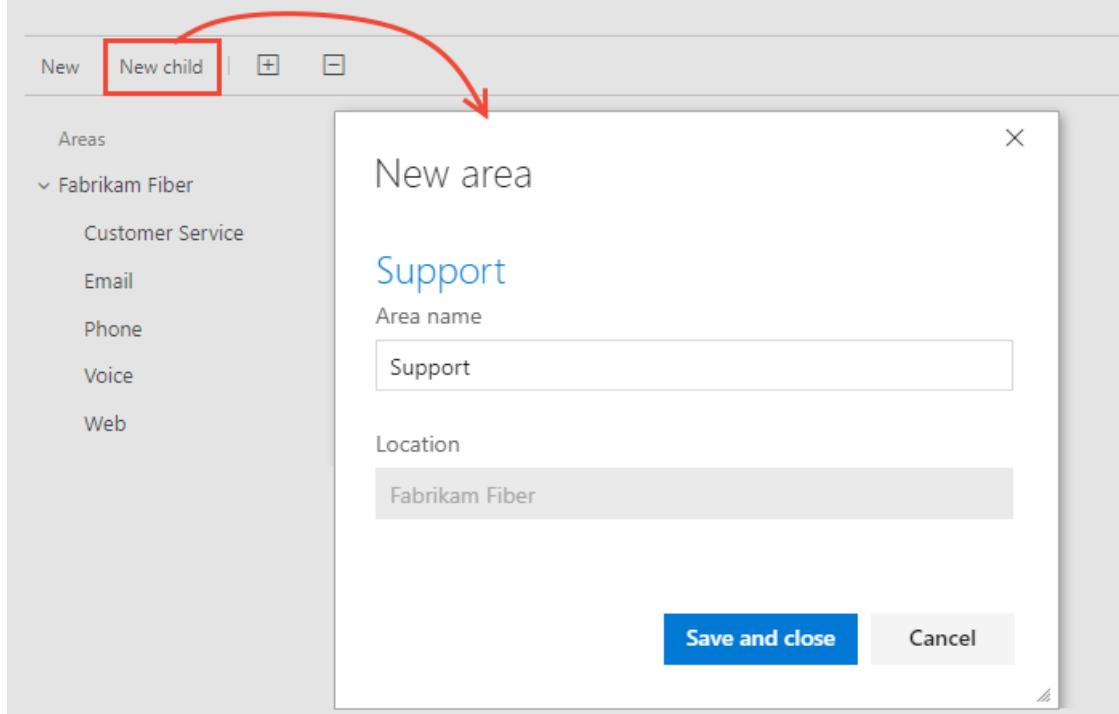
Enter a name (255 characters or less) for the node. For additional name restrictions, see [About areas and iterations](#), [Naming restrictions](#).

Work

Iterations [Areas](#)

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](#).



Work

Iterations [Areas](#)

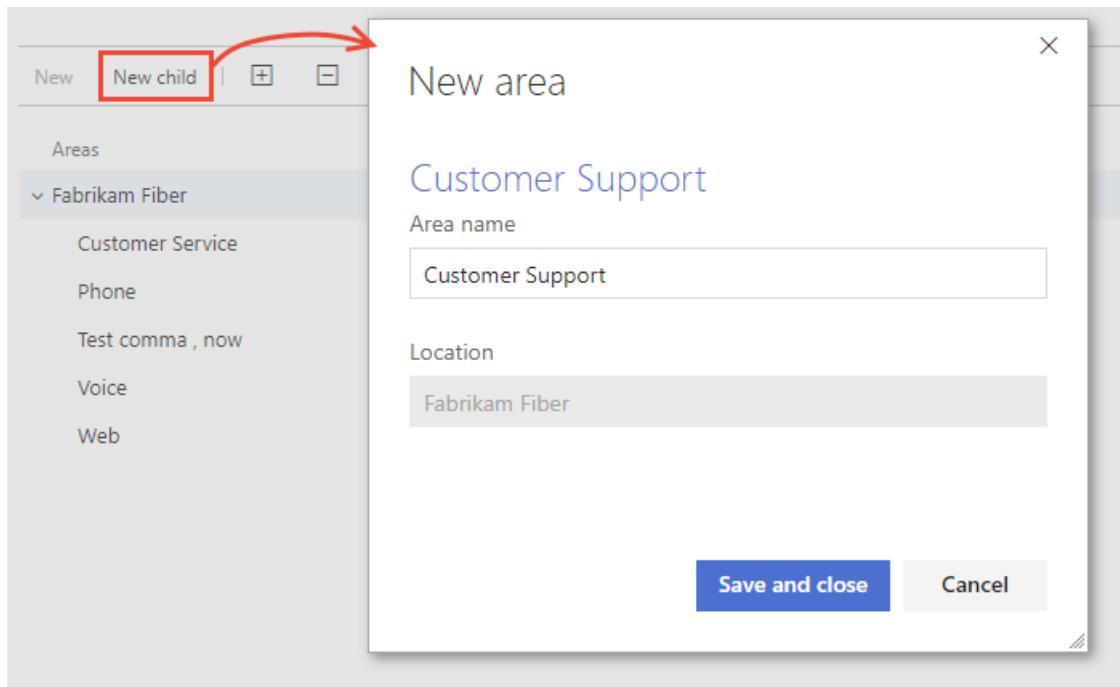
Create and manage the areas for this project. These areas will be used by teams to determine what shows up on the team's backlog and what work items the team is responsible for. [Learn more about customizing areas and iterations ↗](#)

To select areas for the team, go to [the default team's settings](#).

New	New child		[+]	[x]
Areas	Teams			
✓ Fabrikam Fiber	Fabrikam Fiber Team			

- To add a child node, highlight the area path and then choose **New child**. Optionally, you can open the **... context menu** for the area path and choose **New child**.

Enter a name (255 characters or less) for the node. For additional name restrictions, see [About areas and iterations](#), [Naming restrictions](#).



1. Open **Areas**.

Areas		
<input type="checkbox"/> Fabrikam-Fiber-Git	default area	sub-areas are included
<input type="checkbox"/> Backend		
<input type="checkbox"/> Database		
<input type="checkbox"/> Middle-tier		
<input type="checkbox"/> Devices		
<input type="checkbox"/> iPhone		
<input type="checkbox"/> Surface		
<input type="checkbox"/> Windows Phone		
<input type="checkbox"/> Website		

From the areas page, you can set the default area path used to filter the backlog. The default area path is also used when new work items a user creates new work items.

2. Add a new child node to the area you've selected.

Control panel > DefaultCollection > **Fabrikam-Fiber-Git**

Overview Iterations Areas Security Alerts Version Control Settings

Areas

Areas

Select the areas your team owns. Selected areas will determine what shows up on your team's backlog and what work items your team is responsible for.

New **New child**

Areas

- Fabrikam-Fiber-Git
 - Backend
 - Database
 - Middle-tier
 - Devices
 - iPhone
 - Surface
 - Windows Phone
 - Website

Area name Location

Save and close Cancel

Open team settings

You set team defaults from team settings. If you're not a team administrator, [get added as one](#). Only team or project administrators can change team settings.

From a web browser, open the web portal administrative context for your team.

You define both areas and iterations from **Project Settings>Boards>Team configuration**. You can quickly navigate to it from a team work tracking backlog, board, or dashboard.

1. Open a backlog or board for a team and choose the team profile icon. Then choose **Team Settings**.

Here we open the Board for the Web team and from there the team profile.

Azure DevOps fabrikam / Fabrikam Fiber / Work / Board

FF Fabrikam Fiber +

- Overview
- Boards**
- Work Items
- Boards
- Backlogs
- Sprints
- Queries

Web Backlog items backlog

New Approved

	New item	
	Change initial view	
	Raisa Pokrovskaya	5
	Web	
	0/1	
	GSP locator interface	
	Jamal Hartnett	8
	Change backlog	

Web
Fabrikam Fiber **Team Settings**

Items Members (2)

All Items

Web Boards

Web Backlogs

Sprint 3 Sprints

2. Choose **Iterations and areas**.

The screenshot shows the 'Team Profile' page for the 'Web' team. On the left, there's a sidebar with sections like 'Name', 'Description', 'Administrators', and 'Iterations and areas'. The 'Iterations and areas' section is highlighted with a red box. The main area shows 'Members' with two users listed: 'Jamal Hartnett' and 'Raisa Pokrovskaya'. Below them is a link to 'Manage other settings for this team'.

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

The screenshot shows the 'Project Settings > Team configuration' page. The breadcrumb navigation is 'Project Settings > Team configuration > Web'. A dropdown menu for 'Web' is open, showing a list of teams: 'Phone (Fabrikam Fiber)', 'Voice (Fabrikam Fiber)', 'Web (Fabrikam Fiber)' (which is selected and highlighted), 'Customer Service (Fabrikam Fiber)', 'Fabrikam Fiber Team (Fabrikam F...)', 'Management team (Fabrikam Fib...)', and 'More teams'. Other options in the dropdown include 'Epics', 'Features', and 'Backlog'.

You open team settings from the top navigation bar. Select the team you want and then choose the gear icon. To learn more about switching your team focus, see [Switch project, repository, team](#)

The screenshot shows the top navigation bar with tabs for 'Dashboards', 'Code', 'Work', 'Build and release', 'Wiki', and a gear icon. The 'Work' tab is selected. Below the navigation bar, a secondary navigation bar shows 'Overview', 'Work' (selected), 'Security', 'Version Control', 'Policies', 'Agent Queues', 'Notifications', and 'Service Hooks'. Under the 'Work' tab, there are sub-tabs: 'General', 'Iterations', 'Areas', and 'Templates'. The word 'Work' is also repeated at the bottom of the page.

Set team default area path(s)

All work items assigned to the area paths selected for a team appear on the backlogs and boards for that team. You can select one or more area paths and optionally include their sub-area paths. Choose to include sub-area paths when you want to support rollup views of work performed across several teams or areas.

All work items assigned to the area paths selected for a team appear on the backlogs and boards for that team. You can select a single area path, and optionally include their sub-area paths. Choose to include sub-area paths when you want to support rollup views of work performed across several teams or areas.

The default area path determines the default area path assigned to work items that are created from the team context.

IMPORTANT

Work items that appear on more than one team's Kanban board can yield query results that don't meet your expectations. Because each team can customize the Kanban board [columns](#) and [swimlanes](#), the values assigned to work items which appear on different boards may not be the same. The primary work around for this issue is to maintain single ownership of work items by team area path.

1. Open **Areas** for the team context.

Here, we show the Areas for the Web team.

General Iterations **Areas** Templates

ⓘ To manage areas for the project, navigate to [Project settings](#)

Areas

Select the areas your team owns below. The selected area paths will determine what shows up on your team's backlog and what work items your team is responsible for.

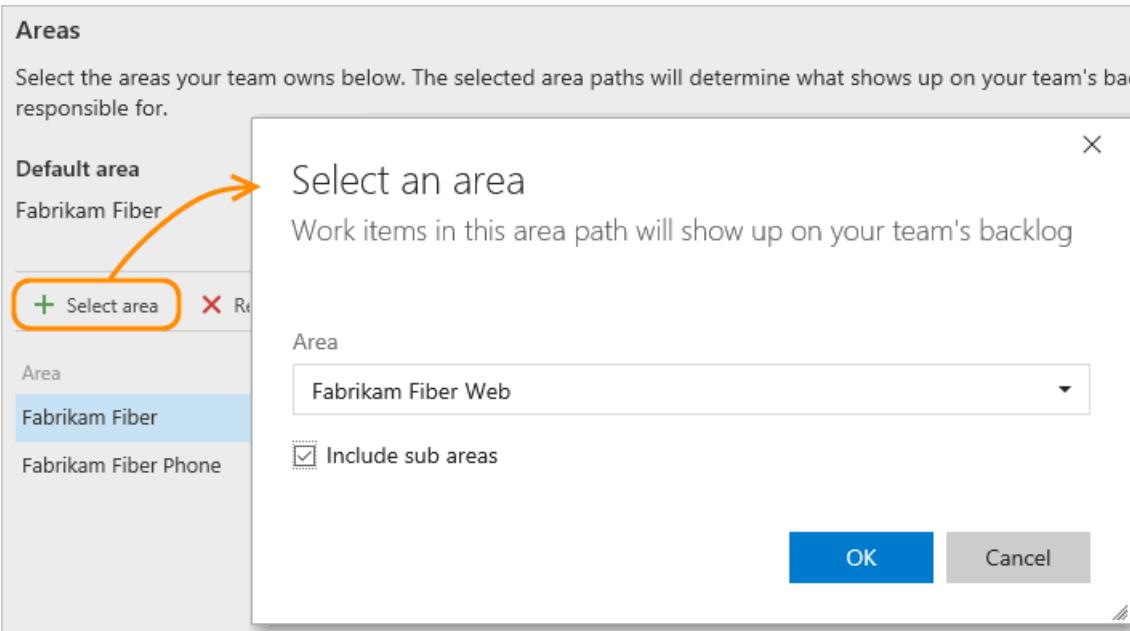
Default area

Fabrikam Fiber\Web [Change](#)

+ Select area(s) X Remove | New New child

Area	... default area	sub-areas are included
Fabrikam Fiber\Web		

2. Choose the area path(s) to be active for each team.



In this instance, we choose to activate all three sub-area paths for the project. The management team can now track progress across all three teams.

Area	... default area
Fabrikam Fiber Customer support	sub-areas are included
Fabrikam Fiber Phone	sub-areas are included
Fabrikam Fiber Web	sub-areas are included

3. When you've finished, refresh the product backlog page for the team, and you'll see those work items assigned to the team. Add Area Path to the columns shown to see the assignments made to work items.

The screenshot shows the 'Backlog items' section of the Azure DevOps interface. On the left, a sidebar lists 'Epics', 'Features', and 'Backlog items'. The 'Backlog items' section is selected and displays a table of backlog items. The table has columns for Order, State, Title, and Area Path. The first item is 'Hello World Web Site' (Committed). The 10th item is 'Switch context issues' (Approved), which is highlighted with a gray background. The 11th and 12th items are also Committed.

	Order	State	Title	Area Path
+	1	● Committed	> Hello World Web Site	... Fabrikam Fiber\Web
	2	● Committed	> Slow response on information form	Fabrikam Fiber\Web
	3	● New	> Add an information form	Fabrikam Fiber
	4	● New	> Change initial view	Fabrikam Fiber\Web
	5	● Committed	> Secure sign-in	Fabrikam Fiber\Phone
	6	● Approved	> Welcome back page	Fabrikam Fiber\Phone
	7	● Committed	> Cancel order form	Fabrikam Fiber\Voice
	8	● Approved	> Interim save on long form	Fabrikam Fiber\Web
	9	● Approved	> Canadian addresses don't display	Fabrikam Fiber\Web
+	10	● Approved	> Switch context issues	... Fabrikam Fiber\Phone
	11	● Committed	> Hello World Web Site	Fabrikam Fiber\Web
	12	● Committed	> Cancel order form	Fabrikam Fiber\Phone

1. Open the Areas admin page for the team context.

Here, we navigate to the Web team. The checked box indicates the area paths selected for the team. To exclude sub-areas, select the option from the area path context menu.

Control panel > DefaultCollection > Fabrikam Fiber > Web

Areas

Areas

Select the areas your team owns. Selected areas will determine what shows up on your team's backlog and what work items your team is responsible for.

New New child

Areas

- Fabrikam Fiber
- Customer Service
- Phone
- Voice
- Web

default area sub-areas are included

New
New child
Open
Delete
Security
Set as default area for team
Exclude sub-areas

2. Refresh the product backlog page for the team, and you'll see only those work items assigned to the Fabrikam Fiber\Web area path.

Visual Studio Team Services / Fabrikam Fiber / Web

HOME CODE WORK BUILD TEST RELEASE

Backlogs Queries

Features Backlog items

Past Current

- Sprint 4
- Future**
- Sprint 5
- Sprint 6

Backlog items

New Create query Column options

Order	State	Title	Area Path
1	New	Research architecture changes	Fabrikam Fiber\Web
2	Committed	Change initial view	Fabrikam Fiber\Web
3	Approved	Request support	Fabrikam Fiber\Web
4	Committed	Secure sign-in	Fabrikam Fiber\Web

Rename, move, or delete an area path

When you rename an area or an iteration, or move the node within the tree hierarchy, the system automatically updates the work items and queries that reference the existing path or paths.

1. To rename an area or iteration path, choose the *** actions icon for the node, and select **Edit**.

The screenshot shows the 'Areas' section of the TFS interface. On the left, there's a tree view with 'Areas' expanded, showing 'Fabrikam Fiber' which contains 'Customer Service', 'Phone', 'Test comma , now', 'Voice', and 'Web'. To the right, under 'Teams', it lists 'Fabrikam Fiber Team, Management team'. A context menu is open over the 'Customer Service' node, with the 'Edit' option highlighted by a red box.

2. In the dialog that opens, enter the new name.

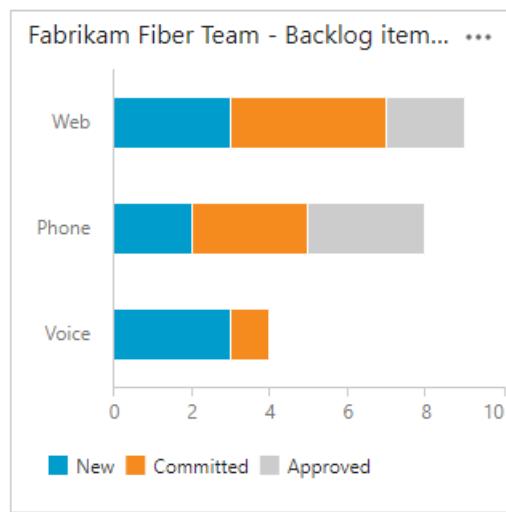
The screenshot shows the 'Edit area' dialog box. It has a title 'Edit area' and a sub-section 'Customer Service'. Under 'Area name', the text 'Customer Service' is entered. Under 'Location', 'Fabrikam Fiber' is selected from a dropdown. At the bottom, there are 'Save and close' and 'Cancel' buttons.

3. To move the node within the hierarchy, change the Location field.
4. To delete a node, choose the **Delete** option from the actions menu.

=tfs-2017 <= tfs-2018> [!NOTE] When you delete an area node or change the Location field for a node, the system automatically updates the existing work items with the node that you enter at the deletion prompt.

Chart progress by area

You can quickly generate [queries](#) to view the progress based on an area path. For example, [visualize progress of work items that are assigned to each team's area path](#), as shown in the following stacked bar chart. Choose Node Name to get the leaf node of the Area Path.



Q & A

Q: Do I have to assign an area path to a team?

A: No. You assign area paths to teams so that the work items assigned to that area path appear on the team's backlog and boards. By default, all work items are assigned to the root area path and show up in the default team that's defined for the project.

Next steps

[Set iteration paths or sprints](#)

Related articles

As you can see, areas play a major role in supporting Agile tools and managing work items. Learn more about working with these fields from the following articles:

- [About areas and iterations](#)
- [Add another team](#)
- [Configure team settings and add team administrators](#)
- [Agile tools that rely on areas or iterations](#)
- [Query by area or iteration path](#)
- [Set permissions and access for work tracking](#)

Define Iteration Paths (aka sprints) and configure team iterations

6/14/2019 • 12 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

You add Iteration Paths to support teams who implement Scrum or use sprint planning to group work items based on a time-box interval or sprint. You define Iteration Paths at the project level and then each team selects the ones they want to be active for them under the team configuration. You can create a flat iteration path structure or a hierarchy of paths to support releases, sub-releases, and sprints.

Each team has access to a number of Agile tools as described in [About teams and Agile tools](#). Each tool references the team's default area path(s). Several tools reference the team's default and selected Iteration Paths or sprints. Most teams choose one Area Path and several Iteration Paths to support their work tracking activities. However, to support other scenarios, it's possible for teams to choose several Area Paths to appear on their backlogs and boards.

Newly created projects contain a single, root Area Path that corresponds to the project name. You add Area Paths under this root. Also, each project typically specifies a predefined set of Iteration Paths to help you get started tracking your work. All you need to do is specify the dates.

IMPORTANT

Make sure that you select the correct version of this article for Azure DevOps Services or Azure DevOps Server, renamed from Team Foundation Server (TFS). The version selector is located above the table of contents.

Prerequisites

- You add Iteration Paths to a project. If you don't have a project yet, [create one now](#).
- To add an Iteration Path under the root node or edit or delete any child node, you must be a member of the **Project Administrators** group. To acquire these permissions, see [Set permissions at the project- or collection-level](#).
- Or, to add, edit, and manage Iteration Paths under a node, you must have one or more of the following permissions set to **Allow** for the node you want to manage: **Create child nodes**, **Delete this node**, and **Edit this node**, and **View permissions for this node**. By default, the user who created the project has these permissions set. To learn more, see [Set permissions and access for work tracking](#).
- To set team Iteration Paths, you must be [added as the team administrator](#) or be a member of the **Project Administrators** group.

For naming restrictions on Iteration Paths, see [About areas and iterations](#), [Naming restrictions](#).

Get started sequence

If you are new to managing projects and teams, the most straight forward sequence for configuring iterations for your project and teams is as follows:

1. First, define the Area Paths and teams following the guidance provided in [Define area paths and assign to a team](#).

2. Determine the length of the iteration you want to support. Recommended practice is to have all teams use the same sprint cadence. For guidance, review [About areas and iterations](#).
3. Determine if you want a flat structure or hierarchy of sprints and releases.
4. Open **Project settings>Project configuration** and define the Iteration Paths to support steps 2 and 3 at the project level. Follow the steps provided later in this article: [Open Project Settings, Project configuration](#) and [Add iterations and set iteration dates](#).
5. Open the team configuration and assign the default and additional Area Path(s) to each team. Follow the steps provided later in this article: [Open team settings](#) and [Set team default iteration path\(s\)](#).
6. Each team should assign the default Iteration Path they selected to their work items. This is needed in order for those work items to show up on their product backlogs and boards. Use [bulk modify](#) to modify several work items at once. See also [Assign backlog items to a sprint](#). As needed, you can perform the following actions at any time:
 - Add additional child iteration nodes
 - Rename an Iteration Path (except the root path)
 - Move a child Iteration Path under another node
 - Delete a child Iteration Path
 - Change the default and selected Iteration Paths assigned to a team

Backlog iteration versus default iteration

Teams can set a default iteration different from the backlog iteration. The backlog iteration determines which items appear on the team's backlogs and boards. And, the default iteration determines what value is assigned to work items created from the team context.

All work items that you create from your team context are automatically assigned both the team's default area path and default iteration path.

For TFS 2015 and earlier versions, the default iteration is the same as the backlog iteration. The one value selected both filters items that appear on the team's backlogs and boards, and is assigned to work items created from the team context.

Open Project Settings

From the web portal, open **Project Settings**.

You define both areas and iterations for a project from the **Project Settings>Work>Project configuration**.

1. Choose (1) **Project Settings**, expand **Boards** if needed, and choose (2) **Project configuration** and then (3) **Iterations**.

The screenshot shows the 'Project Settings > Project configuration' page in the Azure DevOps web portal. The left sidebar lists project management features like Overview, Boards, Repos, Pipelines, Test Plans, and Artifacts. The main area shows 'General' settings with links to Overview, Services, Teams, Security, Notifications, Service hooks, and Dashboards. A 'Work' section is expanded, showing 'Iterations' (which is highlighted with a red box and circled with a red number 3), 'Areas', and a description of iterations for project planning. Below this is a table for managing iterations, with one entry for 'Fabrikam Fiber' and three sprints listed: Sprint 1, Sprint 2, and Sprint 3. A 'Boards' section is also visible, with 'Project configuration' highlighted with a red box and circled with a red number 2.

You define both areas and iterations from the **Work** pages of the project admin context. From the user context, you open the admin context by choosing the gear icon.

1. From the web portal, open **Project settings**.
2. From the web portal for the project context, choose the gear icon..

The screenshot shows the top navigation bar of the Azure DevOps web portal. It includes links for Dashboards, Code, Work, Build and Release, Test, Wiki, and a gear icon. Below the navigation bar, there are tabs for Work Items, Backlogs, Queries*, and Plans. The 'Backlogs' tab is currently selected.

If you're currently working from a team context, then hover over the and choose **Project settings**.

The screenshot shows a team context in the Azure DevOps web portal. The top navigation bar includes links for Dashboards, Code, Work, Build and release, and a gear icon. Below the navigation bar, there are tabs for Files, Commits, Pushes, Branches, Tags, and Pull. The 'Files' tab is selected. On the left, there's a file tree for 'Fabrikam Fiber' with files like 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md'. The right side shows a list of files with columns for Name, Last change, and Date. A red arrow points from the gear icon in the top navigation to a dropdown menu that appears, listing various project management options: Overview, Work, Security, Version Control, Policies, Agent Queues, Notifications, Service Hooks, Services, Test, Release, Dashboards, Project settings (which is highlighted with a red box), and Organization settings.

3. Choose **Work**.

From the web portal, choose the gear icon to open project administration pages. Then, choose **Iterations**.



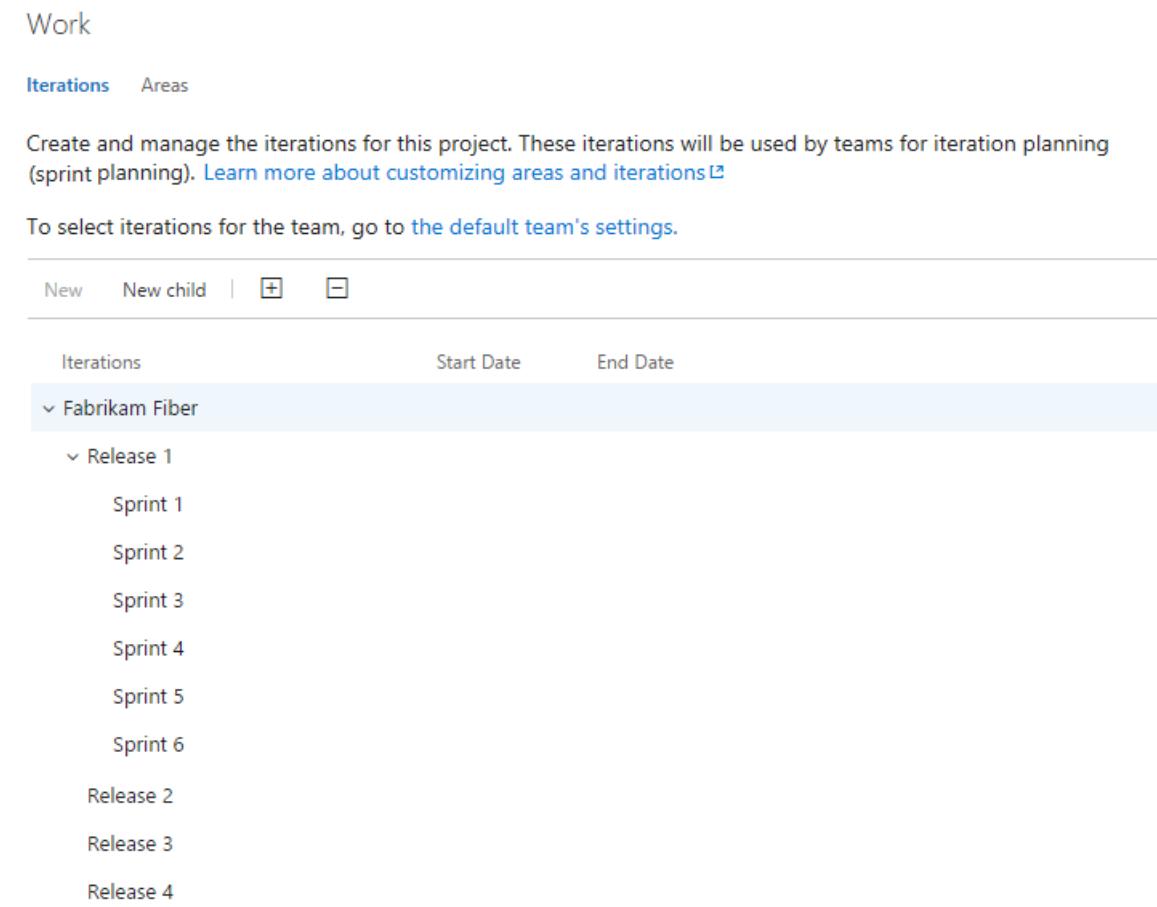
The screenshot shows the TFS 2015 web interface. At the top, there's a blue header bar with the TFS logo, the text "Visual Studio Team Foundation Server 2015 / Fabrikam Fiber", and user info "Helena Peterson". To the right of the user info are three icons: a gear (highlighted with a red box), a question mark, and a magnifying glass. Below the header is a navigation bar with links: HOME, CODE, WORK, BUILD, TEST. The "WORK" link is underlined. To the right of the navigation is a search bar with the placeholder "Search work items" and a magnifying glass icon. Below the navigation is a breadcrumb trail: "Welcome | Overview +".

Add iterations and set iteration dates

From **Iterations**, you can add iterations that teams can then select for their use. You add iterations in the same way you add areas. For more information about working within a sprint cadence, see [Scrum and sprint planning tools](#).

You add and modify area paths from the **Work, Iterations** page from the project admin or settings context.

For Scrum-based projects, you'll see the following set of sprints.



Iterations	Start Date	End Date
✓ Fabrikam Fiber		
✓ Release 1		
Sprint 1		
Sprint 2		
Sprint 3		
Sprint 4		
Sprint 5		
Sprint 6		
Release 2		
Release 3		
Release 4		

1. To schedule the start and end dates for each sprint your teams use, Highlight the sprint and choose **Set dates**. Or, you can open the **...** context menu for the iteration path and choose **Edit**.

Choose the calendar icon to choose new dates.

Edit iteration

Sprint 1

Iteration name

Sprint 1

Start date

4/2/2018

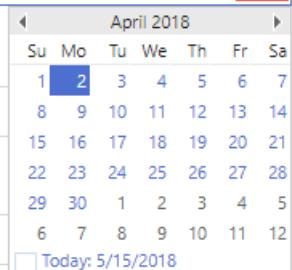


End date

4/20/2018

Location

Fabrikam Fiber\Release 1



Save and close

Cancel

- When you're finished, you'll have a set of sprints scheduled - like this:

New	New child		+	-
Iterations	Start Date	End Date		
Fabrikam Fiber				
Release 1				
Sprint 1	3/27/2017	4/14/2017		
Sprint 2	4/17/2017	5/5/2017		
Sprint 3	5/8/2017	5/26/2017		
Sprint 4	5/29/2017	6/16/2017		
Sprint 5	6/19/2017	7/7/2017		
Sprint 6	7/10/2017	7/28/2017		
Release 2				
Release 3				
Release 4				

Your next step is to [choose the sprints each team uses](#).

- Open the **Iterations** tab for the project context.

For Scrum-based projects, you'll see these set of sprints.

Iterations

Iterations

Select the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.

New New child

Iterations	Start Date	End Date
▲ Fabrikam Fiber	Set dates	Backlog iteration for this team
<input checked="" type="checkbox"/> ▲ Sprint 1		
<input checked="" type="checkbox"/> Sprint 2		
<input checked="" type="checkbox"/> Sprint 3		
<input checked="" type="checkbox"/> Sprint 4		
<input type="checkbox"/> Sprint 5		
<input type="checkbox"/> Sprint 6		

You can change the name, location within the tree hierarchy, or set dates for any sprint. Simply open it (double-click or press Enter key) and specify the info you want.

2. Schedule the start and end dates for those sprints you plan to use.

Iterations

Iterations

Select the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.

New New child

Iterations	Start Date	End Date
▲ Fabrikam Fiber	Set dates	
<input type="checkbox"/> ▲ Sprint 1		
<input type="checkbox"/> Sprint 2		
<input type="checkbox"/> Sprint 3		
<input type="checkbox"/> Sprint 4		
<input type="checkbox"/> Sprint 5		

Sprint 1

Iteration Name:

Start Date: 1 Set dates 2 May 2015

End Date:

Location:

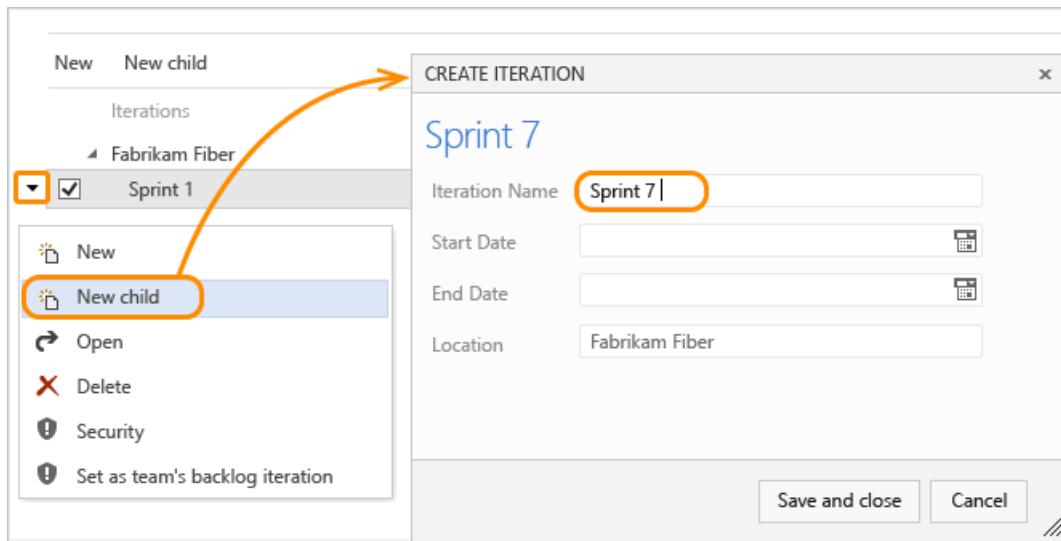
May 2015

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Today: 4/17/2015

After you set the start and end dates for one iteration, the calendar tool automatically attempts to set the next set of dates, based on the same iteration length you specified for the first. For example, if you set a three week sprint for Sprint 1, then when you select the start date for Sprint 2, the calendar tool automatically determines the start and end dates based on the next three weeks. You can accept or change these dates.

3. To add another sprint, select **New child** and name it what you want. Here, we call it Sprint 7.



Your next step is to [select the sprints each team uses](#).

Open team settings

You set team defaults from team settings. If you're not a team administrator, [get added as one](#). Only team or project administrators can change team settings.

From a web browser, open the web portal administrative context for your team.

You define both areas and iterations from **Project Settings>Boards>Team configuration**. You can quickly navigate to it from a team work tracking backlog, board, or dashboard.

1. Open a backlog or board for a team and choose the team profile icon. Then choose **Team Settings**.

Here we open the Board for the Web team and from there the team profile.

Web
Fabrikam Fiber
Team Settings

Items Members (2)

All Items

- Web Boards
- Web Backlogs
- Sprint 3 Sprints

2. Choose **Iterations and areas**.

Team Profile



Name

Web

Description

Enter a description

Administrators

Jamal Hartnett

Raisa Pokrovskaya

[+ Add](#)

Manage other settings for this team

[Notifications](#)

[Dashboards](#)

[Iterations and areas](#)

Web

Members

[+ Add...](#) |

Display Name

Jamal Hartnett

Username Or Scope

fabrikamfiber4@hotmail.com

[Remove](#)

Raisa Pokrovskaya

fabrikamfiber5@hotmail.com

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

The screenshot shows the 'Project Settings' interface. In the top navigation bar, the 'Team configuration' breadcrumb is visible. Below it, the 'Work' section is selected. A dropdown menu for 'Team' is open, showing a list of teams: Phone (Fabrikam Fiber), Voice (Fabrikam Fiber), Web (Fabrikam Fiber) (selected), Customer Service (Fabrikam Fiber), Fabrikam Fiber Team (Fabrikam F...), Management team (Fabrikam Fib...), More teams, and Email (Fabrikam Fiber). The 'Web (Fabrikam Fiber)' team is highlighted with a gray background.

You open team settings from the top navigation bar. Select the team you want and then choose the gear icon. To learn more about switching your team focus, see [Switch project, repository, team](#)

The screenshot shows the 'Work' tab selected in the top navigation bar. The gear icon in the top right corner is highlighted with a red box.

Work

[General](#) [Iterations](#) [Areas](#) [Templates](#)

Select team sprints and default iteration path

You [define sprints for the project](#) and then select them to be active for each team. You assign the default

iteration to use when creating new work items.

1. Open **Project settings>Boards>Team Configuration>Iterations** for a team.

Here, we navigate to the Fabrikam Fiber Team.

The screenshot shows the 'Iterations' page within the 'Team configuration' section of the 'Fabrikam Fiber Team' settings. The 'Iterations' tab is active. A red box highlights the 'Fabrikam Fiber Team' dropdown in the top navigation bar. Another red box highlights the 'Iterations' tab in the sub-navigation bar. The page includes sections for 'Default iteration' (set to '@CurrentIteration') and 'Backlog iteration' (set to 'Fabrikam Fiber'). A note states that iterations will appear in the Backlogs hub. A 'Select iteration(s)' button is also visible.

2. **Backlog iteration.** Only work items assigned to an iteration equal to or under this backlog iteration appear in the team's backlogs and boards.

The screenshot shows the 'Backlog iteration' section. The 'Fabrikam Fiber' iteration is selected, and a red box highlights the 'Change' button.

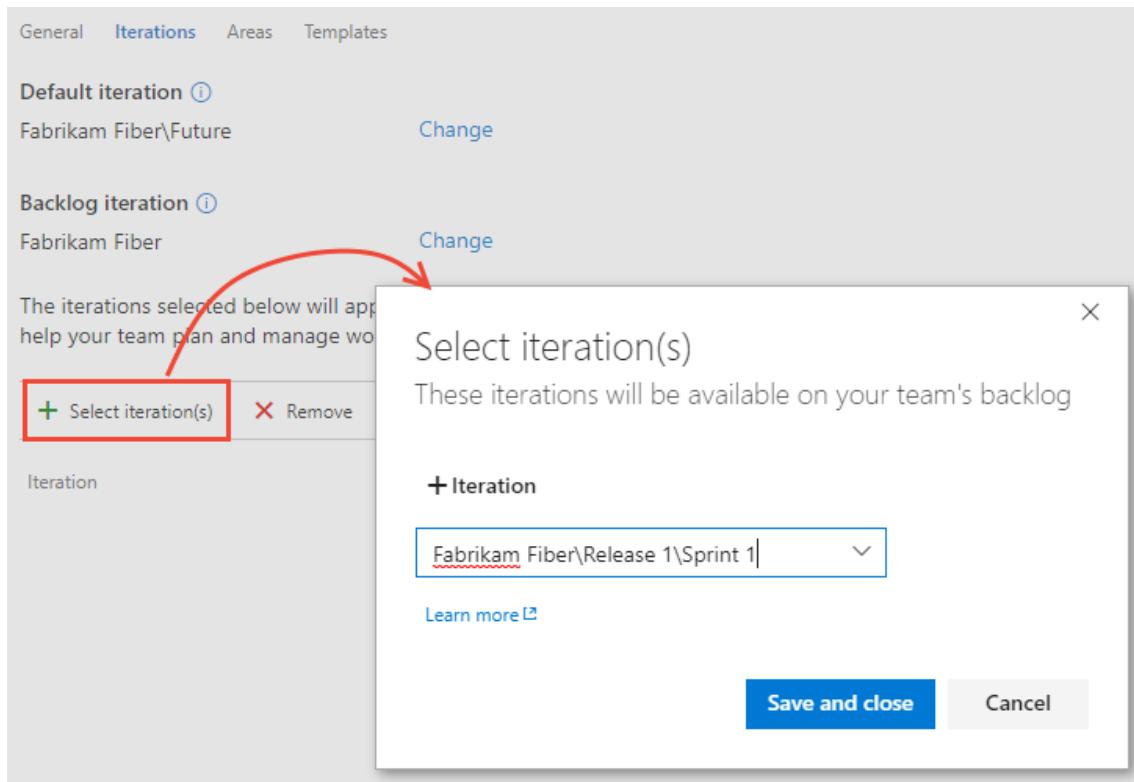
Also, all work items added through a team's backlog or board are assigned the backlog iteration.

3. **Default iteration.** The default iteration defines the iteration used when a work item is created from the team dashboard (new work item widget) and queries page. You can use an explicit value or use **@CurrentIteration** to assign new work items to the team's current iteration. This is the same macro used in [queries to list work items assigned to the currently active iteration assigned to the team](#).

For example, you might want all new work items to be added to a future iteration path which you use to triage and assign to specific sprints at periodic intervals.

The screenshot shows the 'Default iteration' selection dialog. The 'Future' iteration is selected, highlighted with a red box. Other options shown include 'Iteration 1', 'Iteration 2', and 'Iteration 3'. Buttons for 'Set' and 'Cancel' are at the bottom.

4. **Active sprints.** Add an iteration for each sprint backlog you want active for the team. Add each sprint, one by one, by selecting it from the menu.



When you're done, you should see a list of sprints, similar to the following.

Iteration		Start Date	End Date
Fabrikam Fiber\Release 1\Sprint 1		6/11/2018	6/29/2018
Fabrikam Fiber\Release 1\Sprint 2		7/2/2018	7/20/2018
Fabrikam Fiber\Release 1\Sprint 3		7/23/2018	8/10/2018
Fabrikam Fiber\Release 1\Sprint 4			
Fabrikam Fiber\Release 1\Sprint 5			

If you don't see the sprints you need, or the dates aren't set, you can add or edit iterations for the project, provided you have the required permissions. To learn more, see [Define iteration paths \(aka sprints\)](#).

5. To see the newly activated sprint backlogs, refresh your team's [product backlog page](#).

1. Open **Work>Iterations** for a team.

Here, we navigate to the Fabrikam Fiber Team.

Control panel > DefaultCollection > Fabrikam Fiber > **Fabrikam Fiber Team**

Overview Work Security Alerts Version Control Service Hooks Services Test

Work

General Iterations Areas

Iterations

To create, edit or manage iterations, you must navigate to [Project settings](#)

Backlog iteration

Fabrikam Fiber [Change](#)

Default iteration

@CurrentIteration [Set](#) [Cancel](#)

[+ Select iteration](#) [Remove](#)

Iteration	Start Date	End Date
-----------	------------	----------

1. **Backlog iteration.** Only work items assigned to an iteration equal to or under this backlog iteration appear in the team's backlogs and boards.

Backlog iteration

Fabrikam Fiber [Change](#)

Also, all work items added through a team's backlog or board are assigned the backlog iteration.

2. **Default iteration.** The default iteration defines the iteration used when a work item is created from the team dashboard (new work item widget) and queries page. You can use an explicit value or use **@CurrentIteration** to assign new work items to the team's current iteration. This is the same macro used in [queries to list work items assigned to the currently active iteration assigned to the team](#).

For example, you might want all new work items to be added to a future iteration path which you use to triage and assign to specific sprints at periodic intervals.

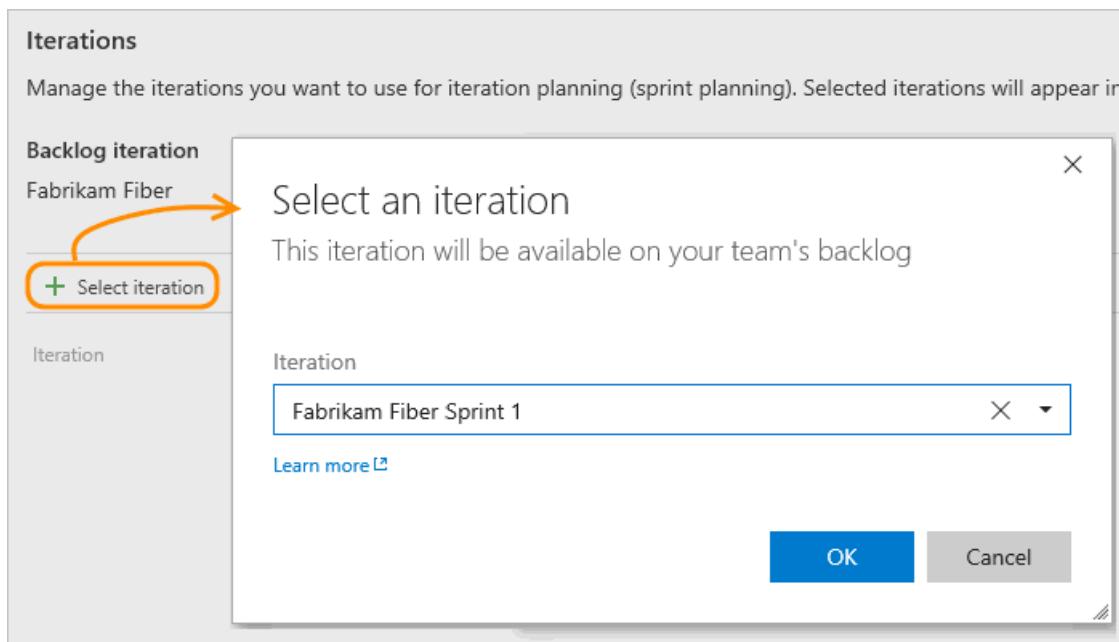
Default iteration

@CurrentIteration [X](#) [Set](#) [Cancel](#)

@CurrentIteration
Fabrikam Fiber
Future

Iteration	Start Date	End Date
Iteration 1		
Iteration 2		
Iteration 3		

3. **Active sprints.** Add an iteration for each sprint backlog you want active for the team. Add each sprint, one by one, by selecting it from the menu.



When you're done, you should see a list of sprints, similar to the following.

Work

General **Iterations** Areas

Iterations

Manage the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.

Backlog iteration

Fabrikam Fiber	▼	Set Cancel
----------------	---	------------

+ Select iteration **X Remove**

Iteration	Start Date	End Date
Fabrikam Fiber Sprint 1	5/2/2016	5/20/2016
Fabrikam Fiber Sprint 2	5/23/2016	6/10/2016
Fabrikam Fiber Sprint 3	6/13/2016	7/1/2016
Fabrikam Fiber Sprint 4	7/4/2016	7/22/2016

If you don't see the sprints you need, or the dates aren't set, then [return to the project admin context and define them there](#).

4. To see the newly activated sprint backlogs, refresh your team's [product backlog page](#).
1. Open the Iterations page for the team context.

Here we open the Iterations page for the Web team.

Overview

Iterations

Areas

Security

Alerts

Version Control

Service Hooks

Iterations

Iterations

Select the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.

If your team isn't listed in the navigation row, open the Overview tab, select your team, and then return to the Iterations tab.

2. **Default iteration.** Only work items assigned to an iteration equal to or under the default iteration appear in the team's backlogs and boards. Also, the default iteration defines the iteration used when a work item is created from the team dashboard (new work item widget) and queries page.

Open the context menu for the iteration path you want.

Here we set the P1 1 path. Only child iterations of the backlog iteration can be active for a team.

Iterations	Start Date	End Date
Fabrikam Fiber		Backlog iteration for this team
Iteration 1		
Iteration 2		
Iteration 3		
P1 1	Set dates	
New	6/16/2014	6/27/2014
New child	6/30/2014	7/11/2014
Open	7/28/2014	8/8/2014
Delete	8/11/2014	8/15/2014
Security	8/31/2015	9/11/2015
Set as team's backlog iteration		

This path determines which work items appear in your team backlogs and boards, and [the default assigned to](#) work items created from any area under your team's context.

3. **Active sprints.** Check each box under the default iteration that you want active for the team.

Here, the Fabrikam Fiber Web team activates Sprints 1 through 7.

Iterations

Iterations

Select the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.

New New child

Iterations	Start Date	End Date
▲ Fabrikam Fiber		
Iteration 1		
Iteration 2		
Iteration 3		
▼ P1 1	Set dates	Backlog iteration for this team
<input checked="" type="checkbox"/> Sprint 1	6/16/2014	6/27/2014
<input checked="" type="checkbox"/> Sprint 2	6/30/2014	7/11/2014
<input checked="" type="checkbox"/> Sprint 4	7/28/2014	8/8/2014
<input checked="" type="checkbox"/> IP Sprint	8/11/2014	8/15/2014
<input checked="" type="checkbox"/> Sprint 3	8/31/2015	9/11/2015
P1 2		
P1 3		

Check boxes only appear for sprints defined under the default iteration path.

4. To see the newly activated sprint backlogs, refresh your team's [product backlog page](#).

Rename, move, or delete an iteration

When you rename an iteration, or move the node within the tree hierarchy, the system automatically updates the work items and queries that reference the existing path or paths.

1. To rename an iteration path, choose the **...** actions icon for the node, and select **Edit**.

Iterations	Start Date	End Date
Sprint 1	4/2/2018	4/20/2018
Sprint 2	4/23/2018	5/11/2018
Sprint 3	5/14/2018	6/1/2018
Sprint 4	6/4/2018	6/22/2018
Sprint 5	3/2018	
Sprint 6	3/2018	
Sprint 7	4/2018	
Sprint 8	4/2018	
Sprint 9	5/2018	
Sprint 10	10/8/2018	10/26/2018



2. In the dialog that opens, enter the new name.

Edit iteration

Sprint 4

Iteration name

Start date

End date

Location

3. To move the node within the hierarchy, change the Location field.

4. To delete a node, choose the **Delete** option from the actions menu.

NOTE

When you delete an iteration node, the system automatically updates the existing work items with the node that you enter at the deletion prompt.

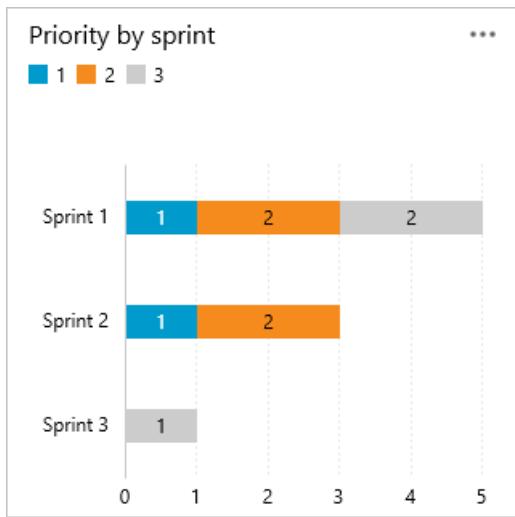
Archive iteration paths

After a while, you may want to archive iteration paths that were used for sprints that are a year or more out of date. You can do that by moving the iteration path under a node that you label "Archive". All work items are updated with the moved iteration path. Also, teams can de-select those sprints that have past. All data is maintained in the data store with the new iteration path assignments.

Prior to archiving the iterations, consider if you have captured all the reports that you may want.

Chart progress by iteration

You can quickly generate [queries](#) to view the progress for those areas. As an example, you can [visualize progress of work items assigned to sprints](#) as shown in the following stacked bar chart.



Q & A

Q: Do I have to assign iteration paths to a team?

A: If your team doesn't use sprints to plan and track work, then no. You can leave the defaults assigned to the team as they are. You can then use the product and portfolio backlogs and boards, however you won't be able to gain much use of sprint planning tools.

Related articles

As you can see, iterations play a major role in supporting Agile tools and managing work items. You can learn more about working with these fields from these articles:

- [About areas and iterations](#)
- [Add another team](#)
- [Configure team settings and add team administrators](#)
- [Assign backlog items to a sprint](#)
- [Agile tools that rely on areas or iterations](#)
- [Query by date or current iteration](#)
- [Query by area or iteration path](#)
- [Set permissions and access for work tracking](#)

Add a team, move from one default team to several teams

6/14/2019 • 7 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

As your organization grows, you'll want to make sure that you configure your Agile tools to support that growth. To enable each feature team the autonomy it needs to manage their backlog and plan their sprints, they need their own set of team tools. For more information about features assigned to teams, see [About teams and Agile tools](#).

NOTE

This article describes how to add a team or team members to a project defined in Azure DevOps. To learn about Microsoft Teams, see the Marketplace extension, [Microsoft Teams Integration](#).

For a good understanding on how to remain Agile as you add teams, review the [Scale Agile to Large Teams](#) article.

As your team grows, you can easily move from one team to two. In this example, we add two feature teams, Email and Voice, and maintain the Fabrikam Fiber team with visibility across each of these two teams.

Prerequisites

- If you don't have a project yet, [create one](#).
- If you're not a project administrator, [get added as one](#). Only members of the Project Administrators group can add and delete teams.

Add two feature teams

Add and configure two teams, Email and Voice. Here we show you how to add and configure the Email team.

1. From the web portal, choose **Project settings** and open **Teams**.

Project Settings > Teams

General

Teams

New team |

Team Name ↑	Members	Description
Fabrikam Fiber Team	7	The default pr...

Overview Services Security Notifications Service hooks Dashboards

> Boards

> Build and release

> Code

> Test

> Extensions

Project settings

2. Choose **New team**. Give the team a name, and optionally a description.

Teams

New team |

Team Name ↑

Fabrikam Fiber Team

Create new team

PROFILE SETTINGS

Team name
Email

Description

Permissions

You can add your team to any existing security group to automatically inherit permissions.

[Fabrikam Fiber]\Contributors

Create team Cancel

3. Select the team to configure it. To select the set of sprints and area paths the team plans to use, choose **Iterations and areas**. See [Define area paths and assign to a team](#) and [Define iteration paths \(aka sprints\) and configure team iterations](#).

Team Profile



Name
Email
Description
Enter a description
Administrators
Raisa Pokrovskaya 
[+ Add](#)

Manage other settings for this team

[Notifications](#)
[Dashboards](#)
[Iterations and areas](#)

Email

Members

 [Add...](#) | 

Display Name	Username Or Scope
 Raisa Pokrovskaya	fabrikamfiber5@hotmail.com
	Remove

IMPORTANT

Team tools aren't available until the team's default area path is set. If you haven't created one or more Area Paths for the team to use, then [do that now](#). Area Paths must be created for the project first, then assigned to the team.

From the team profile, you can perform these additional tasks:

- [Add team administrators](#)
- [Add team members](#)
- [Navigate to team notifications](#)
- [Navigate to and set default team dashboard permissions](#)

To configure other team features, see [Manage teams and configure team tools](#).

1. From the web portal, choose the  gear settings icon to open the **Project settings** page for the project.

Fabrikam Fiber

Dashboards

Code

Work

Build & Release

Test

Settings

Fabrikam Fiber ☆

Briefly describe your project...

Get started with your new project!

2. Choose **New team**. Give the team a name, and make sure to select **Create an area path with the name of the team**. Or, leave it unchecked and assign the default area path for the team after it is created. You can choose an existing area path or add a new one at that time. Team tools aren't available until the team's default area path is set.

Teams

New team

Team

Create new team

PROFILE SETTINGS

Team name

Email

Description

Permissions

You can add your team to any existing security group to automatically inherit permissions.

[Fabrikam Fiber]\Contributors

Team area

Create an area path with the name of the team.

Create team

Cancel

3. Select the team to configure it.

Teams

Team Name ↑	Members	Description
Email	...	5
Fabrikam Fiber Team	10	The default project team.
Web	1	

The Team Profile opens. From the team profile, you can [Add team members](#) and [Add team administrators](#).

Team Profile



Name

Email

Description

Enter a description

Administrators

Raisa Pokrovskaya 

[+ Add](#)

Email

Members

[+ Add...](#) | 

Display Name	Username Or Scope	Remove
 Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

4. To select the set of sprints and area paths the team plans to use, see [Define iteration paths \(aka sprints\) and configure team iterations](#).

IMPORTANT

Team tools aren't available until the team's default area path is set.

To configure other team features, see [Manage teams and configure team tools](#).

1. From the web portal, choose the  gear settings icon to open **Project Settings**.



2. Create a new team. Give the team a name, and make sure to select **Create an area path with the name of the team**.

Or, leave it unchecked and assign the default area path for the team after it is created. You can choose an existing area path or add a new one at that time. Team tools aren't available until the team's default area path is set.

Control panel > DefaultCollection > **Fabrikam Fiber**

Team Name	Members	Description
Fabrikam Fiber Team	1 member	The default project team.

CREATE NEW TEAM

PROFILE **SETTINGS**

Team name:

Email:

Description:

Permissions:

Team area: Create an area path with the name of the team.

Create team **Cancel**

3. Select the team from the Overview tab to configure it.

Control panel > DefaultCollection > **Fabrikam Fiber**

Team Name	Members	Description
Email	1 member	
Fabrikam Fiber Team	1 member	The default project team.
Voice	1 member	Develops voice apps

- To select the set of sprints the team plans to use, open the **Iterations** page for the team. See [Define iteration paths \(aka sprints\) and configure team iterations](#).
- To change the area paths assigned to the team, open the **Areas** page. See [Set team defaults](#), [Set team default area path\(s\)](#).

Add team members

If you're moving from one team to two teams, team members already have access to the project. If you're setting up a team structure for the first time, adding user accounts as team members provides them access to the project and team assets. Access to the project is required to support sharing code and planning and tracking work.

Several Agile tools, like capacity planning and team alerts, and dashboard widgets are team-scoped. That is, they automatically reference the user accounts of team members to support planning activities or sending alerts.

NOTE

You must first [add user to a project or to your organization](#) or [setup your account to work with Azure AD](#). This way you can add user identities to a team.

NOTE

The first time you add a user account, you must enter the full domain name and the alias. Afterwards, you can browse for that name by display name as well as account name. To learn more, see [Set up groups for use in Azure DevOps Server deployments](#).

For details, see [Add users to a project or specific team](#).

Move work items under teams

Now that your two feature teams are configured, you need to move existing work items from their current assignments to the team's default area path. This way, the work items show up on each team's backlog.

1. The quickest way to do this, is to [create a query](#) of all work items you want to reassign, multi-select those items belonging to each team, and [bulk edit the area path](#).

All Queries > Shared Queries > Product Backlog

Results Editor Charts | Run query + New Save query Rename Save item

ID	State	Title	Tags
366	Committed	Hello World Web Site	Service
364	Committed	Slow response on information form	
352	New	Add an information form	
360	New	Request support	
384	Committed	Self-report coverage dead zones	
363	Approved	Data cache improvements	
390	Committed	Performance boost in low-bandwidth modems	
361	Approved	Hello World Web Site	
400	Approved	Slow response on information form	
377	Approved	Request support	
436	Committed	Add an information form	
396	Committed	Self-report coverage dead zones	
376	New	Data cache improvements	
516	New	Performance boost in low-bandwidth modems	
362	New	Hello World Web Site	

Edit work items

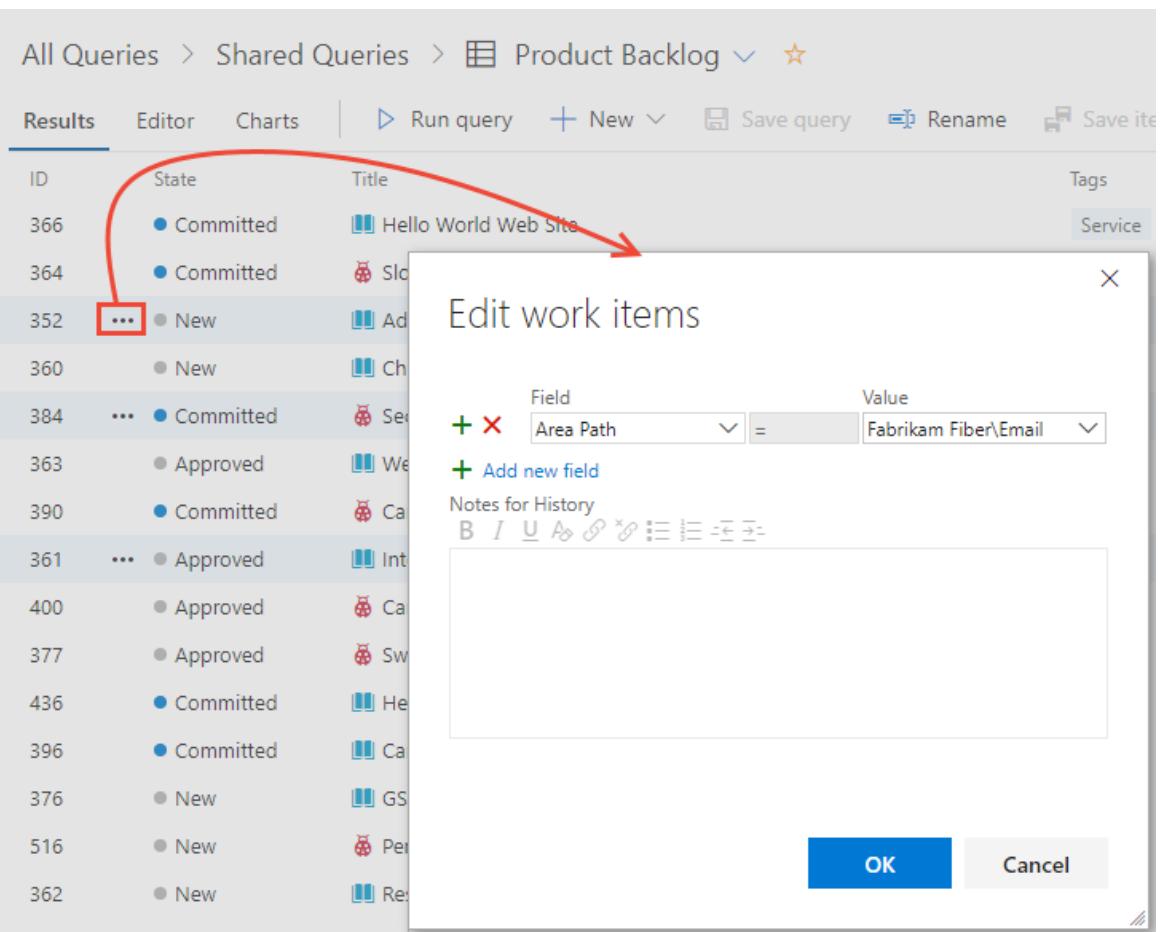
Field Value

+ Area Path = Fabrikam Fiber\Email

+ Add new field

Notes for History

OK Cancel



Product Planning

7 work items (3 selected)

Results Editor Charts Work item pane Off

ID	Title	Area Path
18	Self-report coverage dead zones	Fabrikam Fiber
19	Data cache improvements	Fabrikam Fiber
17	Performance boost in low-bandwidth modems	Fabrikam Fiber
1	Hello World Web Site	Fabrikam Fiber
5	Slow response on information form	Fabrikam Fiber
4	Request support	Fabrikam Fiber
6	Add an information form	Fabrikam Fiber

EDIT WORK ITEMS

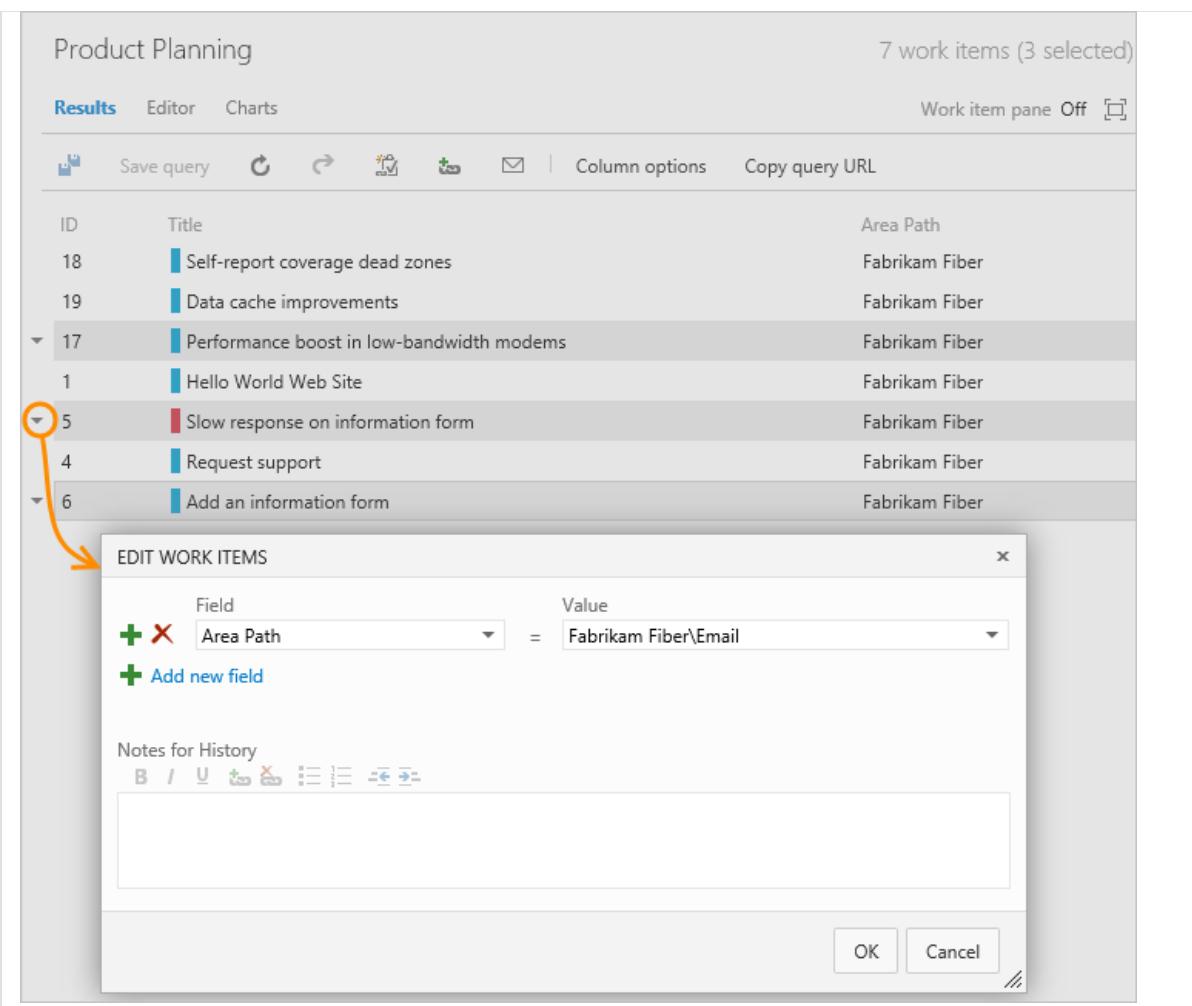
Field Value

+ Area Path = Fabrikam Fiber\Email

+ Add new field

Notes for History

OK Cancel



2. After you bulk modify, do a bulk save.

Product Planning			7 work items (3 selected)
Results Editor Charts			Work item pane Off
ID	Title	Area Path	
18	Self-report coverage dead zones	Fabrikam Fiber	
19	Data cache improvements	Fabrikam Fiber	
17	Performance boost in low-bandwidth modems	Fabrikam Fiber\Email	
1	Hello World Web Site	Fabrikam Fiber	
5	Slow response on information form	Fabrikam Fiber\Email	
4	Request support	Fabrikam Fiber	
6	Add an information form	Fabrikam Fiber\Email	

Configure the default project team

One last step in moving from one team to two teams requires configuring the default project team to exclude sub-areas.

1. Open **Project Settings>Team Configuration** settings page for the default project team, and change the setting as shown.

Project Settings > Team configuration > Fabrikam Fiber Team

The screenshot shows the 'Areas' settings page for the 'Fabrikam Fiber' team. On the left, there's a navigation sidebar with sections like General, Boards, Project configuration, Team configuration (which is selected), Build and release, and Code. The main area has tabs for Work, General, Iterations, Areas (which is selected), and Templates. A note says 'This project is currently using the MyScrum process. To customize your work'. Below that, a message says 'To manage areas for the project, navigate to Project settings'. The 'Areas' section shows 'Fabrikam Fiber' as the default area, with a 'Change' link. Below it is a button bar with '+ Select area(s)', 'Remove', 'New', and 'New child'. The 'Area' list shows 'Fabrikam Fiber' with a '... default area' button. A context menu is open over this button, listing options: New, New child, Edit, Remove, Security, Set as default area for team, and Exclude sub areas. The 'Exclude sub areas' option is highlighted with a red box and a red arrow pointing to it from the bottom of the image.

2. Refresh the product backlog page for the team, and you'll see only those work items assigned to the *Fabrikam Fiber* area path.

The screenshot shows the backlog items board for the 'Fabrikam Fiber' team. At the top, there are buttons for 'New Work Item', 'Backlog items Board', and '...'. Below is a table with columns: Order, State, Title, and Area Path. The table lists 12 backlog items:

Order	State	Title	Area Path
1	Committed	> Hello World Web Site	... Fabrikam Fiber\Web
2	Committed	> Slow response on information form	Fabrikam Fiber\Web
3	New	> Add an information form	Fabrikam Fiber
4	New	> Change initial view	Fabrikam Fiber\Web
5	Committed	> Secure sign-in	Fabrikam Fiber\Phone
6	Approved	> Welcome back page	Fabrikam Fiber\Phone
7	Committed	> Cancel order form	Fabrikam Fiber\Voice
8	Approved	> Interim save on long form	Fabrikam Fiber\Web
9	Approved	> Canadian addresses don't display correctly	Fabrikam Fiber\Web
10	Approved	> Switch context issues	Fabrikam Fiber\Phone
11	Committed	> Hello World Web Site	Fabrikam Fiber\Web
12	Committed	> Cancel order form	Fabrikam Fiber\Phone

1. Open the **Work>Areas** settings page for the default project team, and change the setting as shown.

Work

General Iterations **Areas** Templates**Areas**

Select the areas your team owns below. The selected area paths will determine what shows up on your team's backlog.

Default area

Fabrikam Fiber

[Change](#)[+ Select area\(s\)](#) [✖ Remove](#) | [New](#) [New child](#)

Area

Fabrikam Fiber

... default area

sub-areas are included

-  New
-  New child
-  Edit
-  Remove
-  Security
-  Set as default area for team
-  Exclude sub areas

2. Refresh the product backlog page for the team, and you'll see only those work items assigned to the *Fabrikam Fiber* area path.

The screenshot shows the 'Product backlog' page in Microsoft Azure DevOps. The left sidebar has tabs for 'Epics', 'Features', and 'Backlog items' (selected). The main area shows a table of backlog items:

	Order	State	Title	Area Path
+	1	● Committed	> Hello World Web Site	... Fabrikam Fiber\Web
	2	● Committed	> Slow response on information form	Fabrikam Fiber\Web
	3	● New	> Add an information form	Fabrikam Fiber
	4	● New	> Change initial view	Fabrikam Fiber\Web
	5	● Committed	> Secure sign-in	Fabrikam Fiber\Phone
	6	● Approved	> Welcome back page	Fabrikam Fiber\Phone
	7	● Committed	> Cancel order form	Fabrikam Fiber\Voice
	8	● Approved	Interim save on long form	Fabrikam Fiber\Web
	9	● Approved	Canadian addresses don't display	Fabrikam Fiber\Web
+	10	● Approved	Switch context issues	... Fabrikam Fiber\Phone
	11	● Committed	> Hello World Web Site	Fabrikam Fiber\Web
	12	● Committed	> Cancel order form	Fabrikam Fiber\Phone

1. Open the **Areas** settings page for the default project team, and change the setting as shown.

The screenshot shows the 'Areas' settings page in the Control panel. The 'Fabrikam Fiber' project is selected. The 'Areas' tab is active. The 'Areas' section contains the following text and controls:

Select the areas your team owns. Selected areas will determine what shows up on your team's backlog and what work items your team is responsible for.

New New child

Areas

[Fabrikam Fiber](#) default area sub-areas are included

[New](#)
 [New child](#)
 [Open](#)
 [Delete](#)
 [Security](#)
 [Set as default area for team](#)
 [Exclude sub-areas](#)

2. Refresh the product backlog page for the team, and you'll see only those work items assigned to the *Fabrikam Fiber* area path.

Delete a team

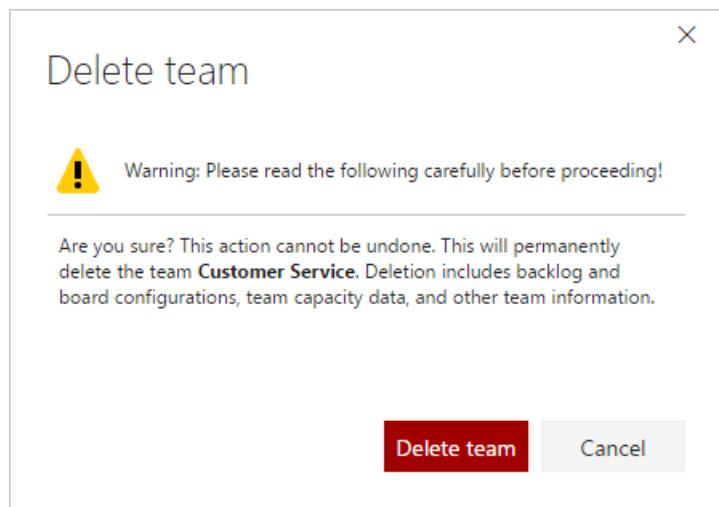
1. To delete a team, open **Project Settings > Teams**, choose the ... context menu for the team you want to delete, and select the **Delete** option.

Team Name	Members	Description
Customer Service	7	
Email	1	
Fabrikam Fiber Team	7	The default project team.
Management team	1	
Phone	1	
Voice	1	
Web	1	

IMPORTANT

Deleting a team deletes all team configuration settings, including team dashboards, backlogs, and boards. Data defined for work items assigned to the team are left unchanged. Once deleted, you can't recover the team configurations.

2. To complete the delete operation, you must type the name of the WIT as shown.



1. To delete a team, open **Project Settings>Work>Overview**, choose the ... context menu for the team you want to delete, and select the **Delete** option.

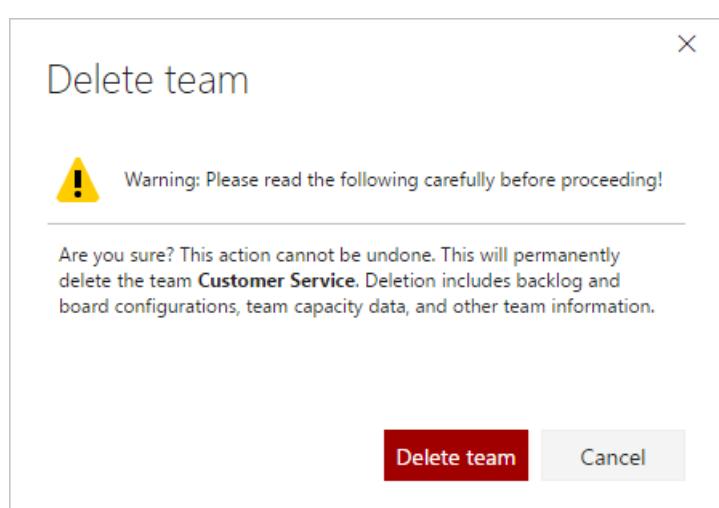
A screenshot of the 'Fabrikam Fiber' project settings under the 'Work' tab. In the 'Teams' section, there is a list of teams: 'Customer Service' (selected), 'Fabrikam Fiber Team' (highlighted with a blue border), 'Management team', and 'Phone'. A context menu is open over 'Fabrikam Fiber Team', with the 'Delete' option highlighted by a red oval. Other options in the menu include 'Set team as project default' and 'Edit'. The 'Fabrikam Fiber Team' row has a tooltip 'Set as project team.'

Team Name ↑	Members	Description
Customer Service	7	
Fabrikam Fiber Team	...	Set as project team.
Management team		
Phone	1	

IMPORTANT

Deleting a team deletes all team configuration settings, including team dashboards, backlogs, and boards. Data defined for work items assigned to the team are left unchanged. Once deleted, you can't recover the team configurations.

2. To complete the delete operation, you must type the name of the WIT as shown.



Grant team members additional permissions

For teams to work autonomously, you may want to provide them with permissions that they don't have by default. Suggested tasks include providing team administrators or team leads permissions to:

- Create and edit child nodes under their default area path
- Create and edit child nodes under an existing iteration node
- Create shared queries and folders under the Shared Queries folder

For more information on setting the above permissions or restricting access for select users, see [Set permissions and access for work tracking](#).

If your Azure DevOps Server or TFS deployment is integrated with SQL Server Reports, you'll need to [Grant permissions to view or create SQL Server reports to team members](#).

If your TFS deployment is integrated with a SharePoint product or SQL Server Reports, you'll need to manage membership for those products separately from their websites.

- [Set SharePoint site permissions](#)
- [Grant permissions to view or create SQL Server reports in TFS](#).

Try this next

Once you've created a team, you'll want to configure your Agile tools to support how your team works. Also, consider adding one or more users as team administrators. Team administrators have the necessary permissions to add team members, add a picture to the team profile, and configure and manage all team features.

[Add team administrator](#) or [Manage teams and configure team tools](#)

Add a team administrator

6/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

It's always a good idea to have more than one person with administration permissions for an area. You need to be a team administrator to [Manage teams and configure team tools](#).

As a team administrator, you can configure, customize, and manage all team-related activities for your team. These include being able to add team members, add team admins, and configure Agile tools and team assets.

Prerequisites

- You must be a member of a project. If you don't have a project yet, [create one](#).
- You must be a [member of the Project Administrators group](#), or a team administrator for the team you want to update.
- You must be a member of a project. If you don't have a project yet, [create one](#). * You must be a [member of the Project Administrators group](#), or a team administrator for the team you want to update.

To get added as a team administrator, ask another team admin, the organization owner, or a member of the [Project Administrators group](#) to add you.

If you need to add a team, see [Add teams](#).

Open Project Settings>Team Profile and add an administrator

From the web portal, open the admin page for the team.

1. Choose **Project Settings** and choose **Teams**.

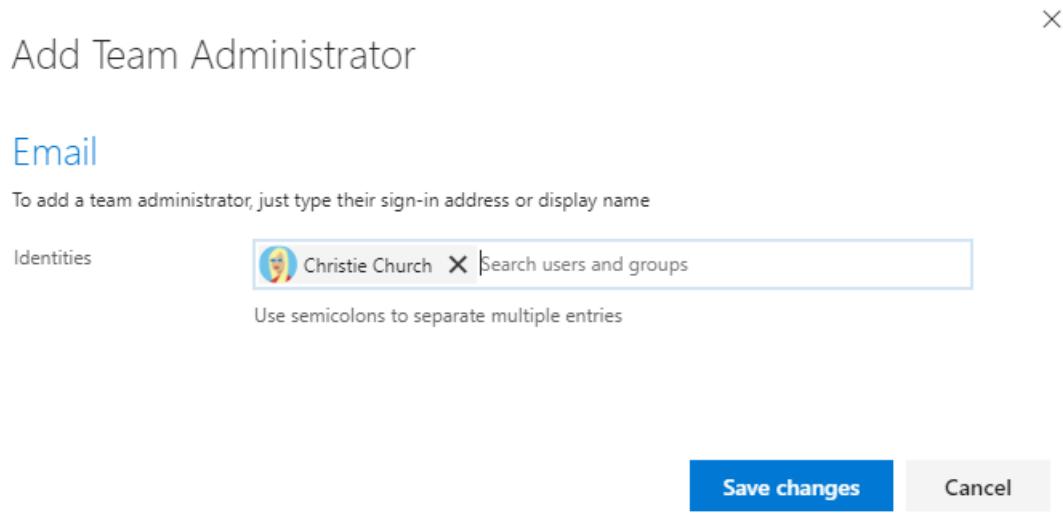
The screenshot shows the 'Project Settings > Teams' page. On the left, there's a sidebar with icons for Overview, Boards, Repos, Pipelines, Test Plans, Artifacts, and 'Project settings'. The 'Project settings' button is highlighted with a red box. The main area has a 'General' section with 'Teams' selected (also highlighted with a red box). Below it are sections for Overview, Services, Security, Notifications, Service hooks, and Dashboards. There are also collapsed sections for Boards, Build and release, Code, and Test. At the bottom right, there's a table showing a team named 'Fabrikam Fiber Team' with 7 members and a description 'The default pr...'. A 'New team' button and a refresh icon are also present.

2. Choose the team to configure, and then choose the **Add** link to open the dialog for adding user identities.

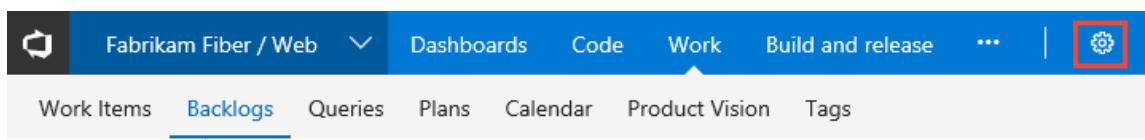
The screenshot shows the 'Team Profile' page for the 'Fabrikam Fiber Team'. It includes sections for 'Name' (Fabrikam Fiber), 'Email' (fabrikamfiber@outlook.com), 'Description' (Enter a description), 'Administrators' (Raisa Pokrovskaya, with a red X next to her name), and a '+ Add' button (highlighted with a red box). Other sections like 'Notifications', 'Dashboards', and 'Iterations and areas' are also visible.

Display Name	Username Or Scope	Action
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	Remove

3. Enter the identities you want to add to the team administrator role.

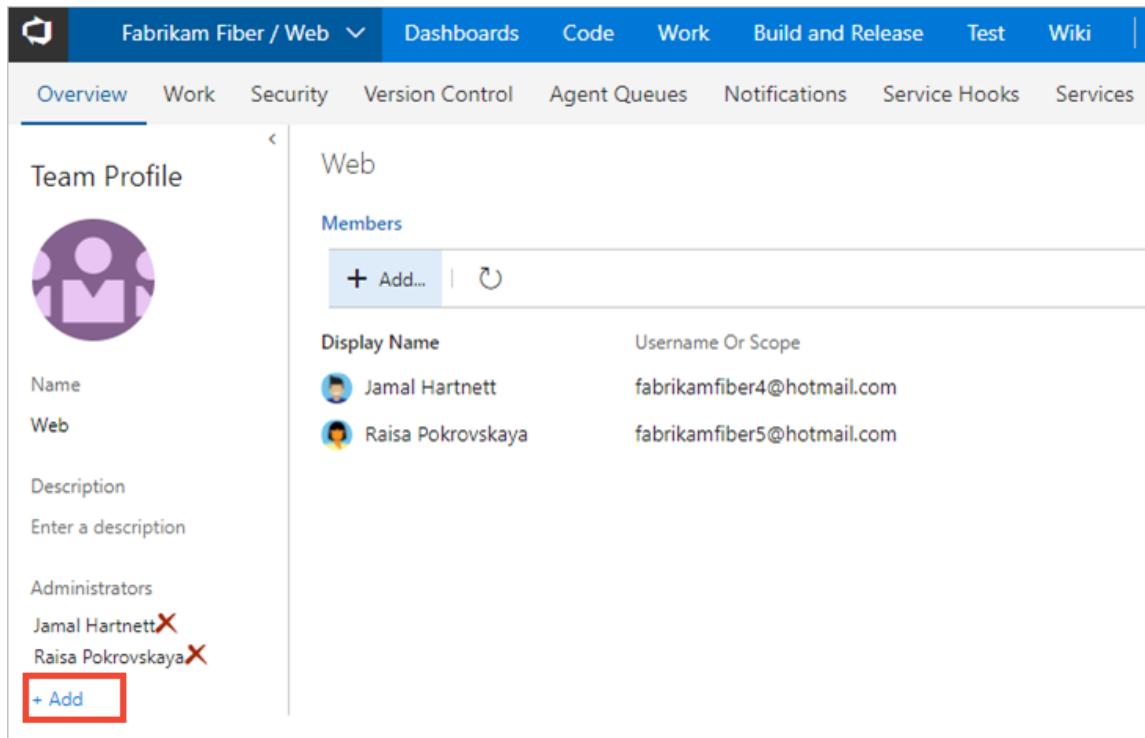


1. From the web portal and team context, choose the gear icon to open **Team Settings**.



If you choose the gear icon from the project context, then choose **Overview**, and select the team you want to configure.

2. Choose the **Add** link to open the dialog for adding user identities.



3. Enter the identities you want to add to the team administrator role.

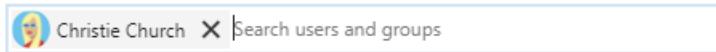
X

Add Team Administrator

Email

To add a team administrator, just type their sign-in address or display name

Identities



Save changes

Cancel

1. From the web portal and team context, choose the gear icon to open the administration page.

If you choose the gear icon from the project context, then choose **Overview**, and select the team you want to add an administrator to.

2. Choose the **Add** link to open the dialog for adding user identities.

Display Name	Username or Scope
Christie Church (Fabrikam)	NORTHAMERICA\ctsoapo
Chuck Reinhart (Fabrikam)	NORTHAMERICA\ctsoapm
Francis Totten (Fabrikam)	NORTHAMERICA\ctsodev2
Helena Petersen (Fabrikam)	NORTHAMERICA\ctsoita
Jamal Hartnett (Fabrikam)	NORTHAMERICA\ctsoasm
Jia-hao Tseng (Fabrikam)	NORTHAMERICA\ctsora
Johnnie McLeod (Fabrikam)	NORTHAMERICA\ctsotst1
Mateo Escobedo (Fabrikam)	NORTHAMERICA\ctsobld

3. Enter the identities you want to add to the team administrator role.

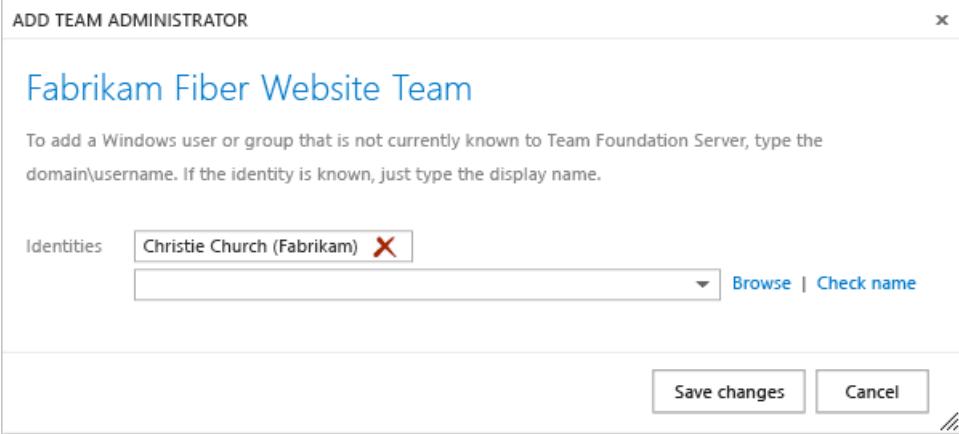
ADD TEAM ADMINISTRATOR X

Fabrikam Fiber Website Team

To add a Windows user or group that is not currently known to Team Foundation Server, type the domain\username. If the identity is known, just type the display name.

Identities X

//



Try this next

[Manage teams and configure team tools](#)

Related articles

- [About teams & Agile tools](#)
- [Manage portfolios](#)
- [Set team favorites](#)

Add users to a project or team

6/13/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In this quickstart, you learn how to add users to a project or specific team. For anyone to access a project, they must be added to one of the default security groups or a custom group. Usually you add them to the Contributors group. For a quick look at what permissions are assigned to the default groups, see [Permissions and access](#).

The easiest way to add a number of users to a project is to add groups defined in [Azure Active Directory \(Azure AD\)](#) or [Active Directory \(AD\)](#).

IMPORTANT

If you're adding users to an organization in Azure DevOps and you don't use Azure AD, then you need to [add their "personal" Microsoft accounts to your account or project](#). After you've added them to one project, you can add them to additional projects using the procedures provided in this article.

Once users have been added to a project, you can browse for their display name or user name (email alias). Also, you can [add them to a specific team](#). To add a team, see [Add a team](#).

Prerequisites

- You must have a project. If you don't have a project yet, [create one](#).
- To add users to a project, you must be a member of the [Project Administrators group](#) or have your [Edit project-level information](#) set to Allow. You can add Stakeholders to the Project Administrators group and then they can add users to an organization or project.
- To add users to a team, you must be [added as a team administrator](#), or you must be a member of the Project Administrators Group, or have your [Edit project-level information](#) set to Allow.

Add users to a project

If you are adding a user to Azure DevOps for the first time, see [Add account users for Azure DevOps](#).

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose **Project Settings** and then **Security**.

To see the full image, click to expand.

The screenshot shows the 'Project Settings' page for the 'Fabrikam Fiber' project. On the left, there's a sidebar with icons for Overview, Work, Code, Build and release, and Packages. Below this is a 'Project settings' button, which is highlighted with a red box and a '1' in a red circle. The main area is titled 'Project Settings' and has a 'General' section expanded. Under 'General', there are links for Overview, Services, Teams, Security (which is highlighted with a red box and a '2' in a red circle), Notifications, Service hooks, and Dashboards. Below these are expandable sections for Boards, Build and release, Code, Test, and Extensions. To the right of the main content is a 'Create group' panel with a 'Filter users and groups' input field. This panel lists several groups under 'Teams': Customer Service, Email, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. It also lists 'Azure DevOps Groups': Build Administrators, Contributors, Deployment Group Administrators, Disallow access group, Endpoint Administrators, Endpoint Creators, Project Administrators, Project Collection Valid Users, and Security Service Group.

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

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

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

Here we choose the **Contributors** group.

The screenshot shows the 'Contributors' group page. On the left, there's a sidebar titled 'Create group' with sections for 'Teams' and 'Azure DevOps Groups'. Under 'Teams', 'Contributors' is highlighted with a red box. The main area is titled 'Fabrikam Fiber > Contributors' and has tabs for 'Permissions', 'Members' (which is selected and highlighted with a red box), and 'Member of'. Below these are buttons for '+ Add...', 'Edit...', and 'Search'. A table lists members with columns for 'Display Name', 'Username Or Scope', and 'Remove'. The members listed are: Customer Service, Fabrikam Fiber Team, Management team, Phone, Voice, Web, and Jia-hao Tseng (with the email fabrikamfiber9@hotmail.com).

By default, the default team group and any other teams you add to the project, are 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.
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 meet your requirements.

The screenshot shows the 'Add users and groups' dialog box. At the top, it says 'Add users and groups'. Below that, a instruction says 'To add users or groups to this group, just type their sign-in addresses or group aliases'. A text input field contains 'Chris'. Below the input field, a search result for 'Christie Church' is shown, with the email 'fabrikamfiber1@hotmail.com'. At the bottom, there are 'Save changes' and 'Cancel' buttons.

NOTE

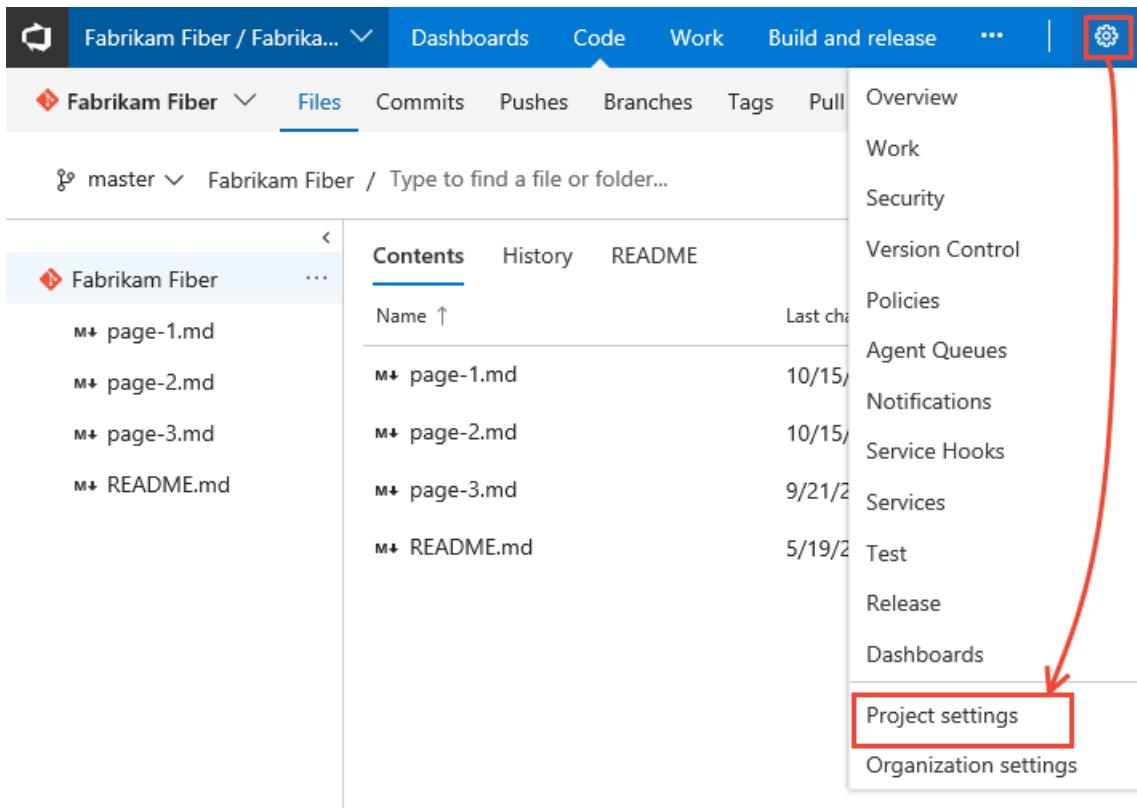
The first time you add a user or group to Azure DevOps, you can't browse to it or check the friendly name. After the identity has been added, you can just enter the friendly name.

7. In **Identities**, specify the name of the user or group you want to add.
8. Depending on the user, you may customize their permissions for other functionality in the project. For example, in [areas and iterations](#) or [shared queries](#).

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open the administrative context.



3. Choose **Security** and under **Groups**, choose one of the following options:

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

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

Here we choose the Contributors group.

Display Name	Username Or Scope	
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Management team	[Fabrikam Fiber]	
Phone	[Fabrikam Fiber]	
Voice	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Jia-hao Tseng	fabrikamfiber9@hotmail.com	

TIP

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

By default, the default team group and any other teams you add to the project, are 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.

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

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group	
Chris	 Christie Church fabrikamfiber1@hotmail.com Edit

Showing 1 result

Save changes **Cancel**

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.

- In **Identities**, specify the name of the user or group you want to add.
- You may want to customize user permissions for other functionality within the project, such as [areas and iterations](#) or [shared queries](#).

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

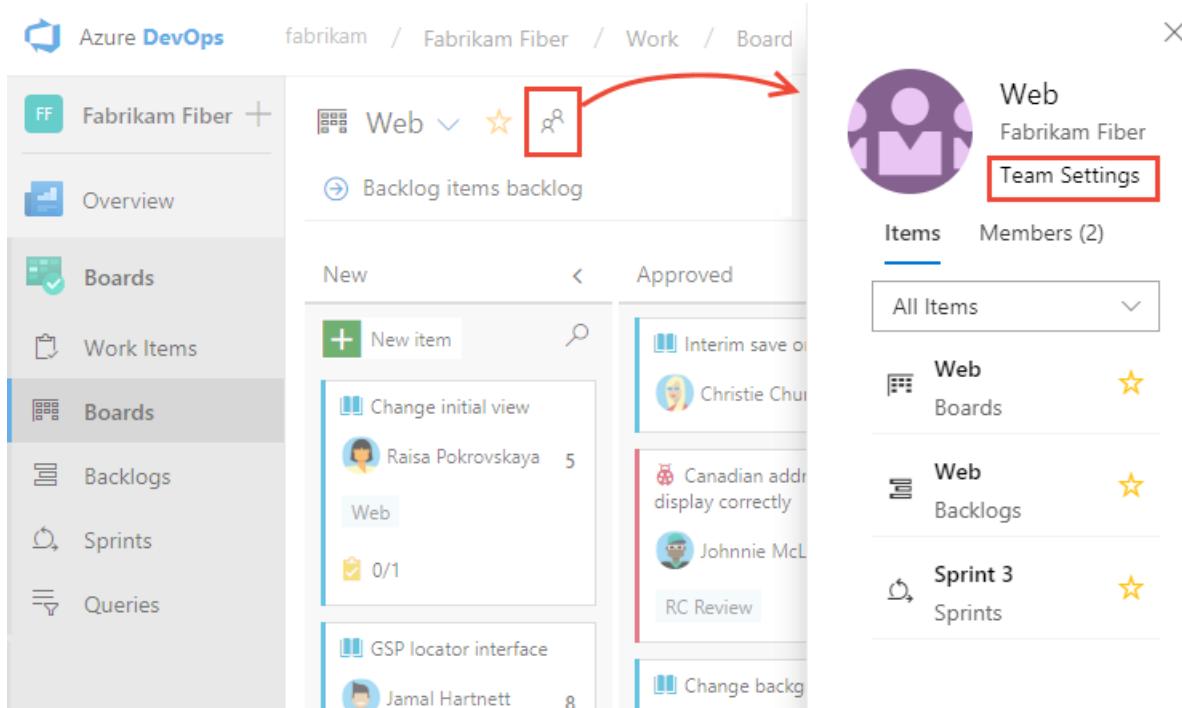
Add users to a team

Several Agile tools, like capacity planning, team alerts, and dashboard widgets are team-scoped. That is, they automatically reference the user accounts added as members of a team to support planning activities or sending alerts. To learn more, see [About teams and Agile tools](#).

You add team members from **Project Settings>Work>Team configuration**. You can quickly navigate to it from a team work tracking backlog, board, or dashboard.

- Open a backlog or board for a team and choose the  team profile icon. Then choose **Team Settings**.

Here we open the Board for the Web team and from there the team profile.



The screenshot illustrates the process of navigating to the Team Settings page. On the left, the navigation menu shows 'Boards' selected. In the center, a 'Backlog items backlog' board for the 'Web' team is displayed. A red box highlights the team profile icon (a person icon with a gear) next to the team name 'Web'. An arrow points from this icon to the 'Team Settings' button on the right. The right side shows the 'Team Settings' page for the 'Web' team, which includes sections for 'Items' and 'Members (2)'. The 'Members' section lists two team members: 'Web' (Boards) and 'Web' (Backlogs). Below this, 'Sprint 3' is listed under 'Sprints'.

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

Project Settings > Team configuration > Web

General

Work General Iterations

Overview Services Teams Security Notifications Service hooks

Backlogs See only the backlog Backlog navigation

Epics Features Backlog i

3. Choose **Add**.

Team Profile



Name

Web

Description

Enter a description

Administrators

Jamal Hartnett

Raisa Pokrovskaya

[+ Add](#)

Web

Members

[+ Add...](#)



Display Name	Username Or Scope	
Jamal Hartnett	fabrikamfiber4@hotmail.com	Remove
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

4. Enter the sign-in addresses or display name for each account you want to add. Add them one at a time or all at the same time. You can enter several identities into the text box, separated by commas.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

Chris

Christie Church fabrikamfiber1@hotmail.com

Showing 1 result

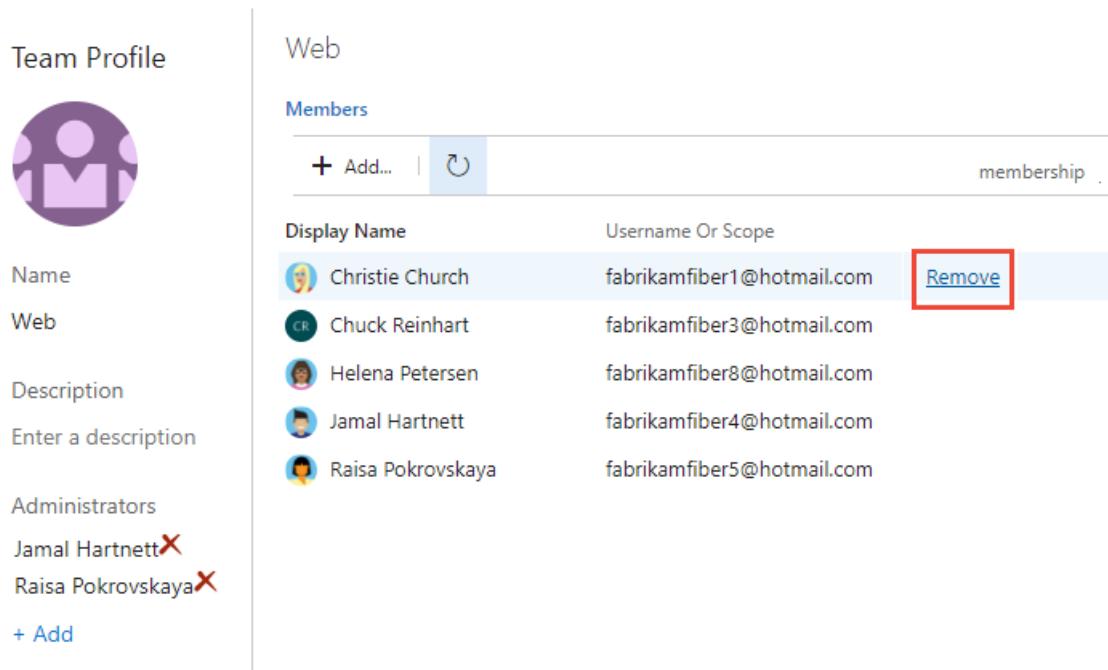
[Save changes](#) [Cancel](#)

TIP

You must enter user and group names one at a time. However, after entering a name, the account is added to the list, and you can enter another name in the Identities text box before choosing to save your changes.

You may need to choose the  refresh icon to see your updates.

5. To remove members, return to this page, highlight the user name and choose **Remove**.



The screenshot shows the 'Team Profile' page for a team named 'Web'. On the left, there's a sidebar with 'Name' (Web), 'Web', 'Description' (Enter a description), 'Administrators' (Jamal Hartnett, Raisa Pokrovskaya, both with a red X), and a '+ Add' button. The main area is titled 'Members' and contains a table with columns 'Display Name' and 'Username Or Scope'. The table lists five users: Christie Church (fabrikamfiber1@hotmail.com), Chuck Reinhart (fabrikamfiber3@hotmail.com), Helena Petersen (fabrikamfiber8@hotmail.com), Jamal Hartnett (fabrikamfiber4@hotmail.com), and Raisa Pokrovskaya (fabrikamfiber5@hotmail.com). The 'Remove' link for Christie Church is highlighted with a red box.

Display Name	Username Or Scope	
Christie Church	fabrikamfiber1@hotmail.com	Remove
Chuck Reinhart	fabrikamfiber3@hotmail.com	
Helena Petersen	fabrikamfiber8@hotmail.com	
Jamal Hartnett	fabrikamfiber4@hotmail.com	
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

NOTE

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

6. To add an account as a team administrator, choose **Add** located in the Team Profile page. For details, see [Add a team administrator](#).
1. From the project admin context, open the **Overview** page, and then choose the team you want to add team members to.

Project profile

Teams

Team Name ↑	Members	Description
Customer Service	7	
Fabrikam Fiber Team	7	The default project team.
Management team	1	
Phone	1	
Voice	1	
Web	2	

2. Choose the **+ Add** to add a user or a user group.
3. Enter the sign-in addresses or display name for each user you want to add. Add them one at a time or all at the same time. You can enter several identities into the text box, separated by commas.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

Chris

Christie Church
fabrikamfiber1@hotmail.com

Showing 1 result

Save changes Cancel

TIP

You must enter user and group names one at a time. However, after entering a name, it is added to the list, and you can enter another name in the Identities text box before choosing to save your changes.

You may need to choose the refresh icon to see your updates.

4. To remove members, return to this page, highlight the user name, and then choose **Remove**.

Team Profile



Phone

Members

+ Add... | ⚡

Display Name	Username Or Scope
Christie Church	fabrikamfiber1@hotmail.com
Chuck Reinhart	fabrikamfiber3@hotmail.com
Cristina Potra	fabrikamfiber6@hotmail.com
Jamal Hartnett	fabrikamfiber4@hotmail.com
Johnnie McLeod	fabrikamfiber2@hotmail.com
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com

Name: Customer Service
Description: Enter a description
Administrators: Cristina Potra 
+ Add

[Remove](#)

NOTE

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

5. To add an account as a team administrator, choose **Add** located in the Team Profile page. For details, see [Add a team administrator](#).

Add users or groups to an access level

For on-premises deployments, you may need to set the access level for a user or group, particularly if those groups don't belong to the default access level. To learn more, see [Change access levels](#).

Add users or groups to SQL Server Reports

If your on-premises deployment is integrated with SQL Server Reports, you need to manage membership for those products separately from their websites. See [Grant permissions to view or create SQL Server reports in Azure DevOps](#).

Add users or groups to SharePoint or SQL Server Reports

If your on-premises deployment is integrated with a SharePoint product or SQL Server Reports, you need to manage membership for those products separately from their websites.

- [Set SharePoint site permissions](#)
- [Grant permissions to view or create SQL Server reports in Azure DevOps Server](#)

Next steps

[Add administrators or set permissions at the project or collection level](#)

Related articles

- To view permissions for yourself or another user, see [View permissions](#).
- [Set Git or TFVC repository permissions](#)
- [Set Git branch permissions](#)
- [Set build and release permissions](#)
- [Set permissions and access for work tracking](#)

Portfolio management

5/24/2019 • 5 minutes to read • [Edit Online](#)

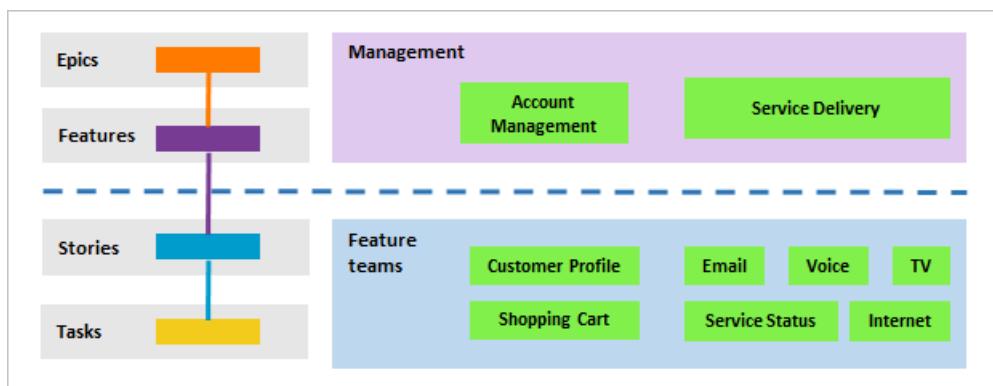
[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Portfolio backlogs provide product owners insight into the work performed by several agile feature teams. Product owners can define the high-level goals as Epics or Features, and feature teams can break these down into the user stories they'll prioritize and develop.

In this article you'll learn:

- How to support a management view of multiple team progress
- How feature teams can focus on their team backlog progress
- How to assign work from a common backlog
- How to set up a hierarchical set of teams and backlogs

By setting up a team structure like the one shown, you provide each feature team with their distinct backlog to plan, prioritize, and track their work. And, portfolio or product owners can create their vision, roadmap, and goals for each release, monitor progress across their portfolio of projects, and manage risks and dependencies.



[Set up a hierarchical team and backlog structure](#) when you want to support the following elements:

- Autonomous feature teams that can organize and manage their backlog of work
- Portfolio management views for planning epics and features and monitoring progress of subordinate feature teams
- Assign backlog items to feature teams from a common backlog

Management view of team progress

In this example, we show the **Epics** portfolio backlog for the **Management** team. Drilling down, you can see all the backlog items and features, even though they belong to one of three different teams: Customer Service, Phone, and Web.

Management team

+ New Work Item Epics Board ...

Order	Node Name	State	Title
	Fabrikam Fiber	New	Phase 1 - Customer access and engagement
(1)	Phone	In Progress	Customer Phone - Phase 1
(1)	Phone	Approved	Phone sign in
(1)	Web	Committed	Request support
(1)	Web	New	Customer Web - Phase 1
(1)	Web	New	Add an information form
(1)	Web	Committed	Hello World Web Site
(1)	Web	Committed	Slow response on information form
(1)	Web	New	Change initial view
	Fabrikam Fiber	New	Customer service - improve UI performance
(1)	Customer Service	New	Customer Service - Phone
(1)	Customer Service	New	GSP locator interface
(1)	Customer Service	Committed	Check service status
(1)	Customer Service	Approved	Switch context issues
(1)	Customer Service	New	Customer Service - Web
(1)	Customer Service	New	Scheduler
(1)	Customer Service	New	Technician dashboard improvements
(1)	Customer Service	New	Check issues with permissions

In this example, we show the **Epics** portfolio backlog for the **Management** team. Drilling down, you can see all the backlog items and features, even though they belong to one of three different teams: Customer Service, Phone, and Web.

Epics

- > Past
- ▽ Current
- Sprint 2**
- ▽ Future

Product backlog

Backlog Board

New	[]	[]	Create query	Column options	[]
Order	Node Name	State	Title		
+	1	Fabrikam Fiber	...	● New	▼ 🏆 Phase 1 - Customer access and engag
		① Phone	● In Progress	▼ 🏆	Customer Phone - Phase 1
		① Phone	● Approved	>	Phone sign in
		① Web	● Committed	>	Request support
		① Web	● New	▼ 🏆	Customer Web - Phase 1
		① Web	● Committed	>	Hello World Web Site
		① Web	● Committed	>	🐞 Slow response on information fo
		① Web	● New	>	Hello World Web Site
		① Web	● New	>	Add an information form
		① Web	● New	>	Change initial view
	2	Fabrikam Fiber	● New	▼ 🏆	Customer service - improve UI perform
		① Customer Service	● New	▼ 🏆	Customer Service - Phone
		① Customer Service	● New	>	GSP locator interface
		① Customer Service	● Committed		Check service status
		① Customer Service	● Approved		🐞 Switch context issues
		① Customer Service	● New	▼ 🏆	Customer Service - Web
		① Customer Service	● New		Scheduler
		① Customer Service	● New		Technician dashboard improver
		① Customer Service	● New	>	🐞 Check issues with permissions

The Fabrikam Account Management portfolio owner has several campaigns to initiate and deliver in the coming year. He creates an epic for each campaign and then breaks each epic down into various features that contribute to each campaign.

With the hierarchical structure implemented, portfolio owners working in Account Management can view the epic, feature, and product backlog for their area.

Order	State	Work Item Type	Title
1	New	Epic	Support customers using mobile apps
	New	Feature	Mobile feedback
	New	Feature	Mobile shopping cart
	New	Feature	Text alerts
	New	Product Backlog Item	Research available solutions
	New	Product Backlog Item	Enable feedback via text alerts
	New	Product Backlog Item	Support automatic broadcast alerts
	New	Feature	Mobile account update
	New	Feature	Pay bill via mobile app
2	New	Epic	Performance and security review
3	New	Epic	Promotional program support
4	New	Epic	Chat support
5	New	Epic	Streamline and enhance standard services

All work items under the Fabrikam/Account Management area path appear in their backlog view. You can expand a single item or use the expand and collapse icons to expand or collapse one level of the hierarchy.

TIP

Program managers can also gain insight into progress across teams using [Delivery plans](#). See also [Visibility across teams](#).

Feature team backlog ownership and view of progress

Each feature team has its own team home page or dashboards, product and portfolio backlogs, Kanban boards, and taskboards. These pages only show work relevant to each team, based on assignments made to the work item area and iteration paths. For details, see [About teams and Agile tools](#).

TIP

Add **Node Name** to the column options to show the team assigned to the work item.

The Customer Service feature team's view of the backlog only includes those work items assigned to their area path, **Fabrikam Fiber/Customer Service**. Here we show parents which provide a few of the features and epics to which the backlog items belong. Items that are owned by other teams appear with hollow-filled bars. For example, Mobile feedback and Text alerts belong to the Account Management team.

Items that are owned by other teams appear with an information icon, .



New Work Item Backlog items Board ... Backlog items Filter Gear Refresh

Order	State	Node Name	Title
+	● New	Fabrikam Fiber	Customer service - improve UI performance
	● New	Customer Service	Customer Service - Phone
	● New	Customer Service	GSP locator interface
	● Committed	Customer Service	Check service status
	● Approved	Customer Service	Switch context issues
	● New	Customer Service	Customer Service - Web
	● New	Customer Service	Scheduler
	● New	Customer Service	Technician dashboard improvements
	● New	Customer Service	Check issues with permissions

Items that are owned by other teams appear with an information icon, ⓘ.

Epics Features Backlog items

Backlog Board Parents Show In progress items Show Mapping Off Gear Refresh

New | + | Create query | Column options |

Order	Node Name	State	Title
+	● New	Fabrikam Fiber	Customer service - improve UI performance
	● New	Customer Service	Customer Service - Phone
	● New	Customer Service	GSP locator interface
	● Committed	Customer Service	Check service status
	● Approved	Customer Service	Switch context issues
	● New	Customer Service	Customer Service - Web
	● New	Customer Service	Scheduler
	● New	Customer Service	Technician dashboard improvements
	● New	Customer Service	Check issues with permissions

Backlog displays with work item icons is supported for TFS 2017.2 and later versions. For TFS 2017.1 and earlier versions, items that are owned by other teams appear with hollow-filled bars.

Backlogs Queries

- █ Epics
- █ Features
- █ Backlog items

Customer Service Backlog items

Backlog Board

Work Item Type	Title	Area Path
Epic	Customer service - improve UI performance	Scrum
Feature	Customer Service - Phone	Scrum\Customer Service
Product Backlog Item	Check service status	Scrum\Customer Service
Bug	Switch context issues	Scrum\Customer Service
Product Backlog Item	GPS locator interface	Scrum\Customer Service
Feature	Customer Service - Web	Scrum\Customer Service
Product Backlog Item	Technician dashboard improvements	Scrum\Customer Service
Product Backlog Item	Scheduler	Scrum\Customer Service

The Customer Profile feature team's view of the backlog only includes those work items assigned to their area path, **Fabrikam/Account Management/Customer Profile**. Here we show parents which provides a few of the features and epics to which the backlog items belong. Items that are owned by other teams appear with hollow-filled bars. For example, Mobile feedback and Text alerts belong to the Account Management team.

Visual Studio Team Foundation Server 2015 / Fabrikam / **Customer Profile**

HOME CODE **WORK** BUILD TEST

Backlogs Queries

- █ Features
- █ Backlog items

Customer Profile Backlog items

Backlog Board Mapping Off **Parents Show**

New	Work Item Type	Title	Node Name
	Epic	Support mobile apps	Account Management
	Feature	Mobile feedback	Account Management
	Product Backlog Item	Design mobile interface	Customer Profile
	Feature	Text alerts	Account Management
	Product Backlog Item	Research available solutions	Customer Profile
	Product Backlog Item	Enable feedback via text alerts	Customer Profile
	Product Backlog Item	Support broadcast alerts	Customer Profile

Assign work from a common backlog

While the hierarchical team and backlog structure works well to support autonomous teams to take ownership of their backlog, it also supports assigning work to teams from a common backlog. During a sprint or product planning meeting, product owners and development leads can review the backlog and assign select items to various teams, by assigning them to the feature team Area Path.

In this view of the Account Management backlog, all items still assigned to **Account Management** have yet to be assigned.

Account Management

New Work Item Epics Board ...

Epics

Order	State	Node Name	Title
+	● New	Account Management	... 🏆 Support mobile apps
	● New	Account Management	🏆 Mobile feedback
	● New	Customer Profile	Design feedback interface
	● New	Account Management	Develop mobile interface
	● New	Account Management	🏆 Mobile shopping cart
	● New	Account Management	Check out
	● New	Account Management	Add an item
	● New	Account Management	Clear an item
	● New	Account Management	Design UI
	● New	Account Management	🏆 Text alerts

During the planning meeting, you can open each item, make notes, and assign the item to the team to work on it.

TIP

You can multi-select work items and perform a bulk edit of the area path. See [Bulk modify work items](#).

Here, all backlog items have been assigned to feature teams. While all features and epics remain owned by Account Management.

Account Management

New Work Item Epics Board ...

Epics

Order	State	Node Name	Title
+	● New	Account Management	... 🏆 Support mobile apps
	● New	Account Management	🏆 Mobile feedback
	● New	Customer Profile	Design feedback interface
	● New	Shopping Cart	Develop mobile interface
	● New	Account Management	🏆 Mobile shopping cart
	● New	Shopping Cart	Check out
	● New	Shopping Cart	Add an item
	● New	Shopping Cart	Clear an item
	● New	Shopping Cart	Design UI
	● New	Account Management	🏆 Text alerts

In this view of the Account Management backlog, all items still assigned to **Account Management** have yet to be assigned.

Permission	Description	Setting
Bypass rules on work item updates	Change process of team project.	Not set
Create tag definition	Create test runs	Allow (inherited)
Delete and restore work items	Delete shared Analytics views	Allow (inherited)
Delete shared Analytics views	Delete team project	Not set
Delete team project	Delete test runs	Allow (inherited)
Delete test runs	Edit project-level information	Not set
Edit project-level information	Edit shared Analytics views	Allow (inherited)
Edit shared Analytics views	Manage project properties	Not set
Manage project properties	Manage test configurations	Allow (inherited)
Manage test configurations	Manage test environments	Allow (inherited)
Manage test environments	Move work items out of this project	Not set
Move work items out of this project	Permanently delete work items	Not set
Permanently delete work items	Rename team project	Not set
Rename team project	Suppress notifications for work item updates	Not set
Suppress notifications for work item updates	Update project visibility	Not set
Update project visibility	View analytics	Allow (inherited)
View analytics	View project-level information	Allow (inherited)

During the planning meeting, you can open each item, make notes, and assign the item to the team to work on it.

TIP

You can multi-select work items and perform a bulk edit of the area path. See [Bulk modify work items](#).

Here, all backlog items have been assigned to feature teams. While all features and epics remain owned by Account Management.

Order	Node Name	Title
New	Account Management	Support mobile apps
New	Account Management	Mobile feedback
New	Customer Profile	Design feedback interface
New	Shopping Cart	Develop mobile interface
New	Account Management	Mobile shopping cart
New	Shopping Cart	Check out
New	Shopping Cart	Add an item
New	Shopping Cart	Clear an item
New	Shopping Cart	Design UI
New	Account Management	Text alerts

In this view of the Account Management backlog, all items still assigned to **Account Management** have yet to be assigned.

Work Item Type	Title	Node Name
Epic	Support mobile apps	Account Management
Feature	Mobile feedback	Account Management
Product Backlog Item	Design feedback interface	Customer Profile
Product Backlog Item	Develop mobile interface	Account Management
Feature	Mobile shopping cart	Account Management
Product Backlog Item	Design UI	Account Management
Product Backlog Item	Clear an item	Account Management
Product Backlog Item	Add an item	Account Management
Product Backlog Item	Check out	Account Management
Feature	Text alerts	Account Management

During the planning meeting, you can open each item, make notes, and assign the item to the team to work on it.

Here, all backlog items have been assigned to feature teams. While all features and epics remain owned by Account Management.

Work Item Type	Title	Node Name	Tags
Epic	Support mobile apps	Account Management	
Feature	Mobile feedback	Account Management	
Product Backlog Item	Design feedback interface	Customer Profile	
Product Backlog Item	Develop mobile interface	Shopping Cart	
Feature	Mobile shopping cart	Account Management	
Product Backlog Item	Design UI	Shopping Cart	
Product Backlog Item	Clear an item	Shopping Cart	
Product Backlog Item	Add an item	Shopping Cart	
Product Backlog Item	Check out	Shopping Cart	

Add portfolio backlogs

If you need more than three backlog levels, you can add more. To learn how, see [Customize your backlogs or boards for a process](#).

If you need more than three backlog levels, you can add more. To learn how, see [Add portfolio backlogs](#).

Track dependencies across teams

The simplest way to track dependencies across teams is to link work items using the **Related** link type. You can then create queries that find work items containing these relationships.

See [Manage dependencies, link work items to support traceability](#) to learn more.

Try this next

[Configure a hierarchy of teams](#)

Related articles

- [Create your backlog](#)
- [Kanban quickstart](#)
- [Assign work to sprints](#)
- [Organize your backlog](#)
- [Limitations of multi-team Kanban board views](#)

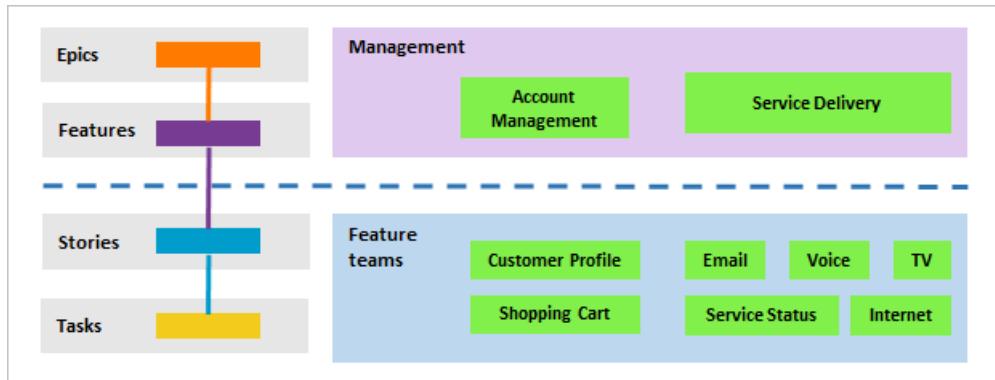
Configure a hierarchy of teams

6/13/2019 • 7 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

In [Portfolio management](#) we showed how management teams and feature teams can use their backlogs to focus on the work that's most important to them. In this article, we show how to configure teams that best supports the different backlog views of management and feature teams.

Specifically, we'll show you how to configure a team structure like the one shown in the image below.



In this article you'll learn how to:

- Set up a hierarchical set of teams and backlogs
- Define a single sprint cadence for all teams
- Review which area paths are assigned to teams
- Set up a hierarchical set of teams and backlogs
- Define a single sprint cadence for all teams
- Review which area paths are assigned to teams

Prerequisites

- If you don't have a project yet, [create one](#).
- If you're not a project administrator, [get added as one](#). Only members of the Project Administrators group or those who have been [granted explicit permissions to edit project information](#) can add teams and configure the project.

Add teams

The first step is to add a team for each feature team and management area. You can also rename teams that you've already added. When you finish, you'll have a set of teams similar to the ones shown.

Teams

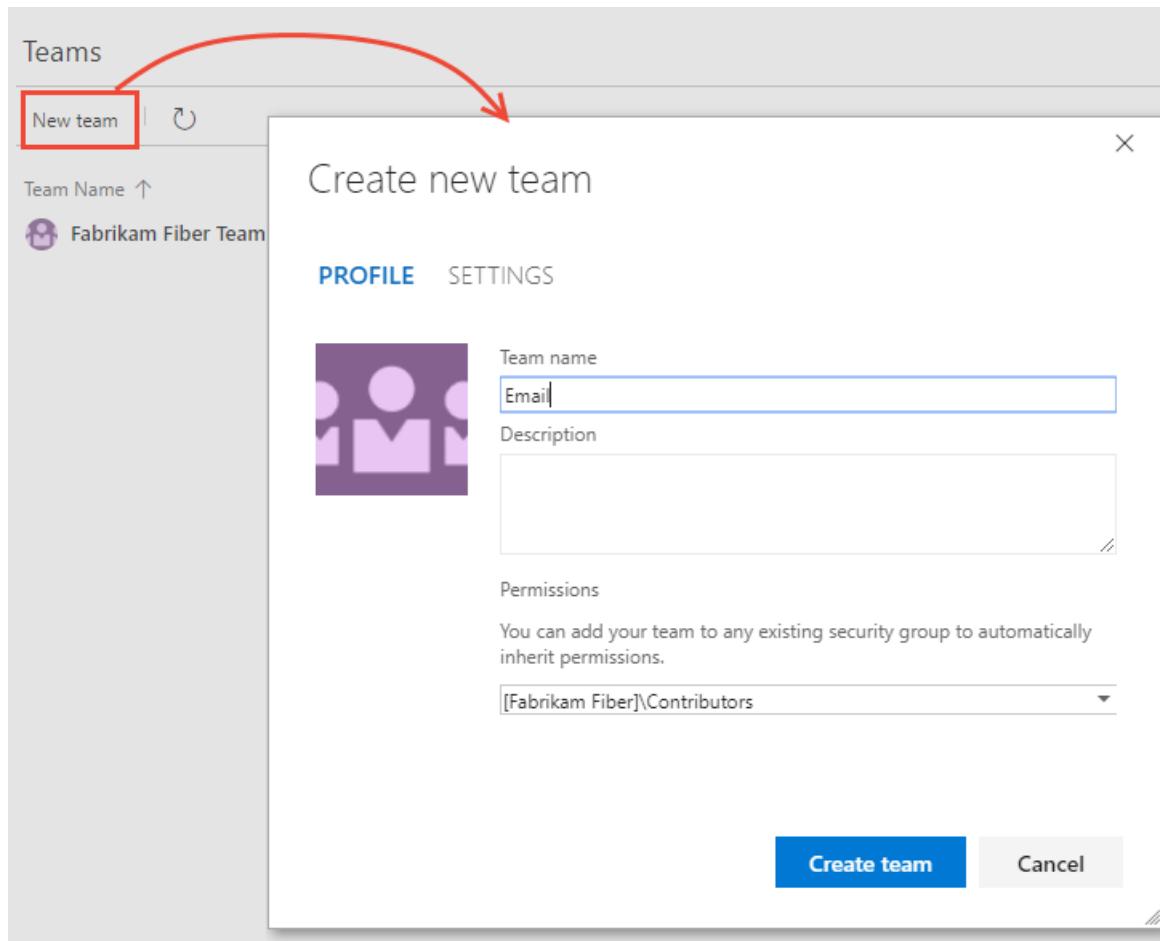
Team Name ↑	Members	Description
Account Management	1	Management team focused on creating and maintaining ...
Customer Profile	1	Feature team focused on securing account data
Email	2	Feature team delivering email apps
Fabrikam Team	7	The default project team. Was Fabrikam Fiber Team
Internet	5	Feature team developing web apps
Phone	1	Feature team delivering phone apps
Service Delivery	7	Management team responsible for ensure high performa...
Service Status	1	Feature team focused on monitoring and addressing servi...
Shopping Cart	1	
Voice	1	Feature team focused on voice communications

1. From the web portal, choose **Project settings** and open **Teams**.

The screenshot shows the 'Project Settings' interface for a project named 'Fabrikam Fiber'. On the left, there's a sidebar with various project management sections: Overview, Boards, Repos, Pipelines, Test Plans, Artifacts, and 'Project settings'. The 'Project settings' button is highlighted with a red box. The main area shows 'Project Settings > Teams'. Under 'General', there's a 'Teams' section with a table listing existing teams. One team, 'Fabrikam Fiber Team', is highlighted with a red box. Below the table are links for Security, Notifications, Service hooks, and Dashboards. To the right, there are navigation links for Boards, Build and release, Code, Test, and Extensions.

Team Name ↑	Members	Description
Fabrikam Fiber Team	7	The default pr...

2. Choose **New team**. Give the team a name, and optionally a description.

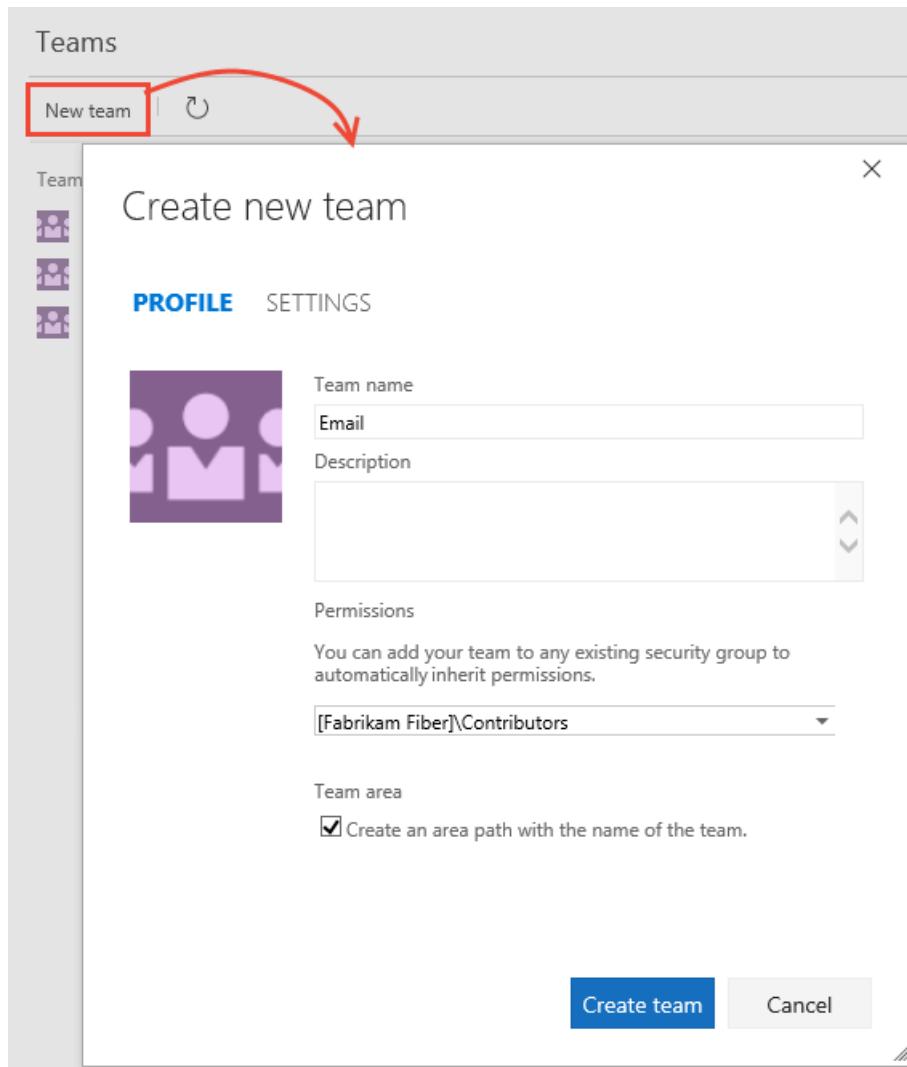


Repeat this step for all feature and management teams you want to create.

1. From the web portal, choose the gear settings icon to open the **Project settings** page for the project.

A screenshot of the Project settings page for 'Fabrikam Fiber'. The top navigation bar includes 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work', 'Build & Release', 'Test', and a gear icon. The gear icon is highlighted with a yellow circle. Below the navigation is a section titled 'Fabrikam Fiber ☆' with a placeholder text 'Briefly describe your project...'. At the bottom, a large button says 'Get started with your new project!'

2. Choose **New team**. Give the team a name, and make sure to select **Create an area path with the name of the team**. If you do not select this option, you will have to set the default area path for the team once you create it. You can choose an existing area path or create a new one at that time. Team tools aren't available until the team's default area path is set.



Repeat this step for all feature and management teams you want to create.

1. From the web portal, choose the gear settings icon to open **Project Settings**.



2. Create a new team. Give the team a name, and make sure to select **Create an area path with the name of the team**.

If you do not select this option, you will have to set the default area path for the team once you create it. You can choose an existing area path or create a new one at that time. Team tools aren't available until the team's default area path is set.

Control panel > DefaultCollection > **Fabrikam Fiber**

Overview Iterations Areas Security Alerts Version Control Service Hooks Serv

Project profile Teams

New team

Team Name Members Description

 **Fabrikam Fiber Team** 1 member The default project team.

CREATE NEW TEAM

PROFILE SETTINGS



Team name: Email

Description:

Permissions: You can add your team to any existing security group to automatically inherit permissions. [Fabrikam Fiber]\Contributors

Team area: Create an area path with the name of the team.

Create team Cancel



Repeat this step for all feature and management teams you want to create.

Move area paths into a hierarchical structure

In this next step, you want to move the areas paths associated with feature teams from a flat structure to a hierarchical structure.

FLAT AREA STRUCTURE

Areas
▼ Fabrikam Fiber
Account Management
Customer Profile
Customer Service
Email
Service Status
Shopping Cart
TV
Voice
Web

HIERARCHICAL AREA STRUCTURE

Areas
▼ Fabrikam Fiber
▼ Account Management
Customer Profile
Shopping Cart
▼ Service Delivery
Email
Internet
Service Status
TV
Voice

FLAT AREA STRUCTURE

Areas
Select the areas your team owns. Select your team's backlog and what work item
New New child
Areas
<input checked="" type="checkbox"/> ▲ Fabrikam
<input type="checkbox"/> Account Management
<input type="checkbox"/> Customer Profile
<input type="checkbox"/> Shopping Cart
<input type="checkbox"/> Service Delivery
<input type="checkbox"/> Email
<input type="checkbox"/> Internet
<input type="checkbox"/> Service Status
<input type="checkbox"/> TV
<input type="checkbox"/> Voice

HIERARCHICAL AREA STRUCTURE

Areas
Select the areas your team owns. Select your team's backlog and what work item
New New child
Areas
<input checked="" type="checkbox"/> ▲ Fabrikam
<input type="checkbox"/> ▲ Account Management
<input type="checkbox"/> Customer Profile
<input type="checkbox"/> Shopping Cart
<input type="checkbox"/> ▲ Service Delivery
<input type="checkbox"/> Email
<input type="checkbox"/> Internet
<input type="checkbox"/> Service Status
<input type="checkbox"/> TV
<input type="checkbox"/> Voice

You do this by opening each area path associated with a feature team and changing its location to be under the management area path.

1. Choose (1) **Project Settings**, expand **Work** if needed, and choose (2) **Project configuration** and then (3) **Areas**.

Project Settings > Project configuration

General

- Overview
- Services
- Teams
- Security
- Notifications
- Service hooks
- Dashboards

Boards

- Project configuration** (highlighted)
- Team configuration

Work

Iterations **Areas** (highlighted) **3**

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
Fabrikam Fiber	Fabrikam Fiber Team, Management team
Customer Service	Customer Service, Fabrikam Fiber Team
Email	Email, Fabrikam Fiber Team
Phone	Fabrikam Fiber Team, Phone
Voice	Fabrikam Fiber Team, Voice
Web	Fabrikam Fiber Team, Web

- Next, choose the *** actions icon for one of the area paths associated with a feature team and select **Edit**. Then change the **Location** to move it under its corresponding management team area path.

For example, here we move the Customer Profile to under Account Management.

Edit area

Customer Profile

Area name
Customer Profile

Location
Fabrikam Fiber\Account Management

Save and close **Cancel**

Repeat this step for all feature team area paths.

- From the web portal for the project, choose the gear icon.

Fabrikam Fiber

Work Items Backlogs Queries* Plans

If you're currently working from a team context, then hover over the gear icon and choose **Project settings**.

The screenshot shows the Azure DevOps interface. At the top, there's a navigation bar with icons for Home, Dashboards, Code, Work, Build and release, and a three-dot menu. Below the navigation bar is a header for the 'Fabrikam Fiber / Fabrika...' project. The main area is titled 'Files' and shows a list of files: 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md'. To the right of the file list is a sidebar with tabs for 'Contents', 'History', and 'README'. A red arrow points from the gear icon in the top right corner down to the 'Project settings' option in a dropdown menu.

2. Choose **Work**.
3. Next, choose the *** actions icon for one of the area paths associated with a feature team and select **Edit**. Then change the **Location** to move it under its corresponding management team area path.

For example, here we move the Customer Profile to under Account Management.

The screenshot shows the 'Edit area' dialog. It has fields for 'Area name' (containing 'Customer Profile') and 'Location' (set to 'Fabrikam Fiber\Account Management'). At the bottom are 'Save and close' and 'Cancel' buttons. A red arrow points from the 'Save and close' button to the 'Customer Profile' text input field.

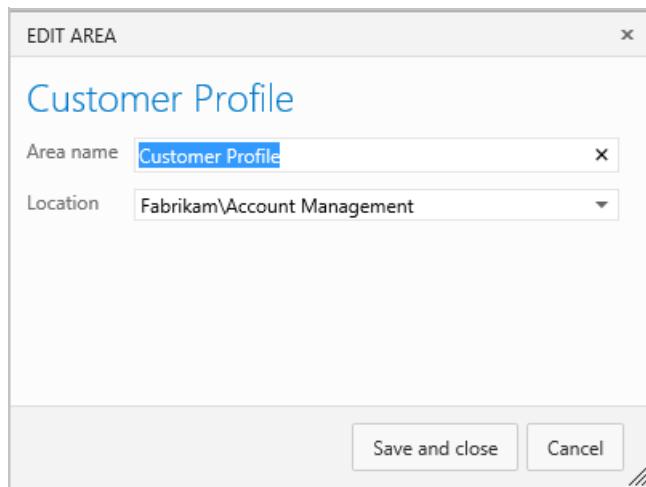
Repeat this step for all feature team area paths.

1. From the web portal, choose the gear icon to open project administration pages. Then choose **Areas**.

The screenshot shows the Visual Studio Team Foundation Server 2015 web portal. At the top, there's a navigation bar with links for HOME, CODE, WORK, BUILD, and TEST. The 'WORK' link is underlined. To the right of the navigation bar are links for 'Helena Peterson', a gear icon (highlighted with a red box), and a question mark icon. A red arrow points from the gear icon to the 'Areas' link in the top navigation bar.

2. Next, choose the context icon for one of the area paths associated with a feature team and select **Edit**. Then change the Location to move it under its corresponding management team area path.

For example, here we move the Customer Profile to under Account Management.



Repeat this step for all feature team area paths.

Include sub-area paths for management teams

By including sub-area paths for the management teams, you automatically include the backlog items of their feature teams onto the management team's backlog. The default setting for all teams is to exclude sub-area paths.

You define both areas and iterations from **Project Settings>Boards>Team configuration**. You can quickly navigate to it from **Teams**.

1. From **Project Settings**, choose **Teams**, and then choose the team whose settings you want to modify.

Here we open the Account Management team.

Team Name	Members	Description
Account Management	1	Management team focused on creating a...
Customer Profile	1	Feature team focused on securing account...
Email	2	Feature team delivering email apps
Fabrikam Team	7	The default project team. Was Fabrikam Fi...
Internet	5	Feature team developing web apps
Phone	1	Feature team delivering phone apps
Service Delivery	7	Management team responsible for ensure...
Service Status	1	Feature team focused on monitoring and ...
Shopping Cart	1	Feature team managing shopping cart app
TV	1	Feature team developing TV apps
Voice	1	Feature team focused on voice communic...

2. Choose **Iterations and areas** and then **Areas**.

Team Profile



Name

Account Management

Description

Management team focused on creating and maintaining customer services

Administrators

Jamal Hartnett

Raisa Pokrovskaya

[+ Add](#)

Manage other settings for this team

[Notifications](#)

[Dashboards](#)

[Iterations and areas](#)

Account Management

Members

[Add...](#) |

Display Name	Username Or Scope	
Jamal Hartnett	fabrikamfiber4@hotmail.com	Remove
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

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

3. Choose **Select area(s)**, and select the area path for **Account Management** and check the **Include sub areas** checkbox.

Select area(s)

Work items in the selected area path(s) will show up on your team's backlog

[Area](#)

Fabrikam Fiber\Account Management

[Include sub areas](#)

[Save and close](#)

[Cancel](#)

Verify that only this area path is selected for the team and is the default area path. Remove any other area paths that may have been previously selected.

Default area

Fabrikam Fiber\Account Management [Change](#)

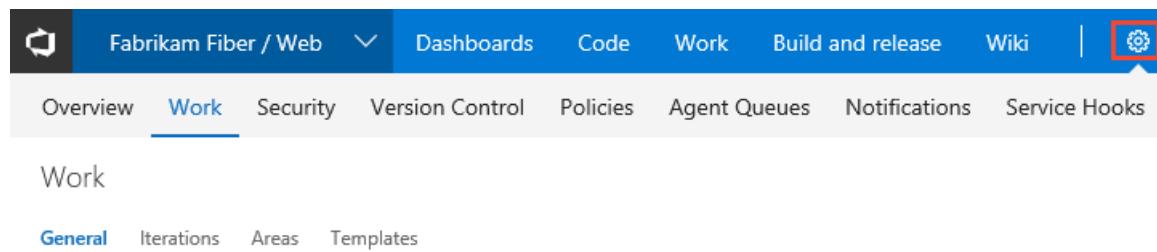
[+ Select area\(s\)](#) [Remove](#) | [New](#) [New child](#)

Area

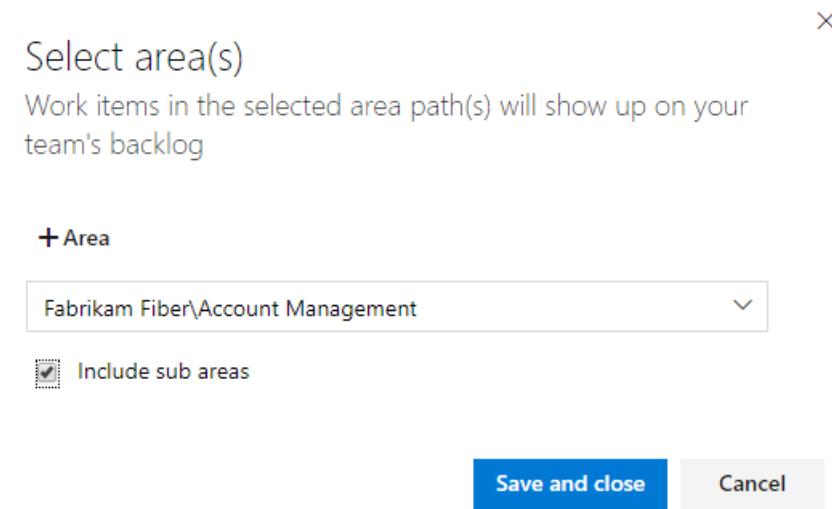
Fabrikam Fiber\Account Management	default area	sub-areas are included
-----------------------------------	--------------	------------------------

Repeat this step for all your management areas. Also, if you want to enable rollup across all feature teams and management areas to the top level area, repeat this step for the default team. In our example, that corresponds to Fabrikam Fiber.

1. You open team settings from the top navigation bar. Select the team you want and then choose the gear icon. To learn more about switching your team focus, see [Switch project, repository, team](#)



2. Choose **Work**, and then **Areas**.
3. Choose **Select area(s)**, and select the area path for **Account Management** and check the **Include sub areas** checkbox.



Verify that only this area path is selected for the team and is the default area path. Remove any other area paths that may have been previously selected.

Default area

Fabrikam Fiber\Account Management [Change](#)

[Select area\(s\)](#) [Remove](#) | [New](#) [New child](#)

Area

Fabrikam Fiber\Account Management

default area

sub-areas are included

Repeat this step for all your management areas. Also, if you want to enable rollup across all feature teams and management areas to the top level area, repeat this step for the default team. In our example, that corresponds to Fabrikam Fiber.

From **Areas**, open the **-** context menu and select **Include sub-areas**.

Here we choose to include sub-area paths for the Account Management area.

Control panel > DefaultCollection > Fabrikam > **Account Management**

Overview Iterations Areas Security Alerts Build Version Control

Areas

Areas

Select the areas your team owns. Selected areas will determine what shows up on your team's backlog and what work items your team is responsible for.

New New child

Areas

▲ Fabrikam

▲ Account Management default area sub-areas not included

New
 New child
 Open
 Delete
 Security
 Set as default area for team
 Include sub-areas

Repeat this step for all your management areas. Also, if you want to enable rollup across all feature teams and management areas to the top level area, repeat this step for the default team. In our example, that corresponds to Fabrikam.

Define a single sprint cadence for all teams

If your feature teams use Scrum or use sprints to assign their work, you'll want to set up a series of sprints that all teams can use. By default, you'll see a set of predefined sprints. Add more sprints and set their sprint dates from **Project Settings** as described in [Add iterations and set iteration dates](#). You can rename and edit the default sprints as needed.

NOTE

While maintaining a single sprint cadence simplifies project administration, you can create different cadences as needed. For example, some teams may follow a monthly cadence while others follow a 3-week cadence. Simply define a node under the top project node for each cadence, and then define the sprints under those nodes. For example:

- Fabrikam Fiber/CY2019
- Fabrikam Fiber/3Week Sprints

Here we define the start and end dates of the first 6 sprints corresponding to a 3-week cadence.

New	New child	+	-
Iterations	Start Date	End Date	
▼ Fabrikam Fiber			
▼ Release 1			
Sprint 1	3/27/2017	4/14/2017	
Sprint 2	4/17/2017	5/5/2017	
Sprint 3	5/8/2017	5/26/2017	
Sprint 4	5/29/2017	6/16/2017	
Sprint 5	6/19/2017	7/7/2017	
Sprint 6	7/10/2017	7/28/2017	
Release 2			
Release 3			
Release 4			

Iterations			
Iterations			
Select the iterations you want to use for iteration planning (sprint planning). Selected iterations will appear in your backlog view as iterations available for planning.			
New New child			
Iterations	Start Date	End Date	
▲ Fabrikam			Backlog iteration for this team
<input checked="" type="checkbox"/> Sprint 1	10/5/2015	10/23/2015	
<input checked="" type="checkbox"/> Sprint 2	10/26/2015	11/13/2015	
<input checked="" type="checkbox"/> Sprint 3	11/16/2015	12/4/2015	
<input checked="" type="checkbox"/> Sprint 4	12/7/2015	12/25/2015	
<input checked="" type="checkbox"/> Sprint 5	12/28/2015	1/15/2016	
<input checked="" type="checkbox"/> Sprint 6	1/18/2016	2/5/2016	

Configure additional team settings

For all teams to be well defined, you'll want to add team administrator(s) and have them verify or configure additional team settings. These include:

- [Add team members](#)
- [Define iteration paths \(aka sprints\) and configure team iterations](#)
- [Select backlog levels](#)

- Show bugs on backlogs and boards
- Configure Kanban boards

For additional details, see [Manage and configure team tools](#)

Review area paths assigned to teams

From **Project Settings>Project configuration>Areas**, you can review which **Area Paths** have been assigned to which teams. To modify the assignments, choose the team and change the team's area path assignments.

[Iterations](#) [Areas](#)

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
▼ Fabrikam Fiber	Fabrikam Team
▼ Account Management	Account Management
Customer Profile	Account Management, Customer Profile
Shopping Cart	Account Management, Shopping Cart
▼ Service Delivery	Service Delivery
Email	Email, Service Delivery
Internet	Internet, Service Delivery
Service Status	Service Delivery, Service Status
TV	Service Delivery, TV
Voice	Service Delivery, Voice

From **Project Settings>Work>Areas**, you can review which **Area Paths** have been assigned to which teams. To modify the assignments, choose the team and change the team's area path assignments.

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
▼ Fabrikam Fiber	Fabrikam Team
▼ Account Management	Account Management
Customer Profile	Account Management, Customer Profile
Shopping Cart	Account Management, Shopping Cart
▼ Service Delivery	Service Delivery
Email	Email, Service Delivery
Internet	Internet, Service Delivery
Service Status	Service Delivery, Service Status
TV	Service Delivery, TV
Voice	Service Delivery, Voice

This feature isn't supported for TFS 2015 and earlier versions.

Related articles

With the hierarchical set of teams in place, you're well positioned to start planning and using the Agile tools available. To take the next steps in planning your portfolio of projects, see these articles:

- [Create your backlog](#)
- [Kanban quickstart](#)
- [Organize your backlog](#)
- [Work with multi-team ownership of backlog items](#)
- [Limitations of multi-team Kanban board views](#)

About area and iteration paths (aka sprints)

6/14/2019 • 7 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Area paths allow you to group work items by team, product, or feature area. Whereas, iteration paths allow you to group work into sprints, milestones, or other event-specific or time-related period. Both these fields allow you to define a hierarchy of paths.

You define area and iteration paths for a project. Teams can then choose which paths are used to support their backlog and other Agile tools. To understand how Agile tools use area and iteration paths, see [Agile tools that rely on areas and iterations](#).

The areas and iterations you see depend on the process you used to create your project. Here we show the defaults defined for the Scrum process. No dates are set. You set dates to correspond to your sprint or release schedules.

ITERATIONS	AREAS																																													
<p>Iterations Areas</p> <p>Create and manage the iterations for this project. These it for iteration planning (sprint planning). Edit Team</p> <p>To access the default team's iteration settings, Edit Team.</p> <p>New New child + -</p> <table><thead><tr><th>Iterations</th><th>Start Date</th><th>End Date</th></tr></thead><tbody><tr><td>▲ Fabrikam Fiber</td><td></td><td></td></tr><tr><td> ▲ Release 1</td><td></td><td></td></tr><tr><td> Sprint 1</td><td>6/11/2018</td><td>6/29/2018</td></tr><tr><td> Sprint 2</td><td>7/2/2018</td><td>7/20/2018</td></tr><tr><td> Sprint 3</td><td>7/16/2018</td><td>8/3/2018</td></tr><tr><td> Sprint 4</td><td>7/23/2018</td><td>8/10/2018</td></tr><tr><td> Sprint 5</td><td>9/17/2018</td><td>10/5/2018</td></tr><tr><td> Sprint 6</td><td>10/29/2018</td><td>11/16/2018</td></tr><tr><td> Release 2</td><td></td><td></td></tr><tr><td> Release 3</td><td></td><td></td></tr></tbody></table>	Iterations	Start Date	End Date	▲ Fabrikam Fiber			▲ Release 1			Sprint 1	6/11/2018	6/29/2018	Sprint 2	7/2/2018	7/20/2018	Sprint 3	7/16/2018	8/3/2018	Sprint 4	7/23/2018	8/10/2018	Sprint 5	9/17/2018	10/5/2018	Sprint 6	10/29/2018	11/16/2018	Release 2			Release 3			<p>Iterations Areas</p> <p>Create and manage the areas for this project. These a the team's backlog and what work items the team is r</p> <p>To access the default team's area settings, Edit Team.</p> <p>New New child + -</p> <table><thead><tr><th>Areas</th><th>Teams</th></tr></thead><tbody><tr><td>▲ Fabrikam Fiber</td><td>Fabrikam Fiber Team</td></tr><tr><td> Customer Service</td><td>Customer Service Team</td></tr><tr><td> Phone</td><td>Fabrikam Fiber Team, Phone</td></tr><tr><td> Voice</td><td>Voice</td></tr><tr><td> Web</td><td>Fabrikam Fiber Team, Web</td></tr></tbody></table>	Areas	Teams	▲ Fabrikam Fiber	Fabrikam Fiber Team	Customer Service	Customer Service Team	Phone	Fabrikam Fiber Team, Phone	Voice	Voice	Web	Fabrikam Fiber Team, Web
Iterations	Start Date	End Date																																												
▲ Fabrikam Fiber																																														
▲ Release 1																																														
Sprint 1	6/11/2018	6/29/2018																																												
Sprint 2	7/2/2018	7/20/2018																																												
Sprint 3	7/16/2018	8/3/2018																																												
Sprint 4	7/23/2018	8/10/2018																																												
Sprint 5	9/17/2018	10/5/2018																																												
Sprint 6	10/29/2018	11/16/2018																																												
Release 2																																														
Release 3																																														
Areas	Teams																																													
▲ Fabrikam Fiber	Fabrikam Fiber Team																																													
Customer Service	Customer Service Team																																													
Phone	Fabrikam Fiber Team, Phone																																													
Voice	Voice																																													
Web	Fabrikam Fiber Team, Web																																													

End-to-end sequence to define and assign Area Paths

If you are new to managing projects and teams, the most straight forward sequence for configuring your project and teams is as follows:

1. Determine the number and names of Area Paths that you want to support to categorize your work. At a minimum, you'll want to add one Area Path for each team that you'll define.
2. Determine the number and names of teams you want to support. For guidance, review [About teams and Agile tools](#).

3. Open **Project settings>Project configuration** and define the Area Paths to support steps 1 and 2 at the project level. Follow the steps provided later in this article: [Open Project Settings, Project configuration](#) and [Add area paths](#).
4. Define the teams you need to support step 2. For guidance, see [Add a team, move from one default team to several teams](#).
5. Open the team configuration and assign the default and additional Area Path(s) to each team. Follow the steps provided later in this article: [Open team settings](#) and [Set team default area path\(s\)](#).
6. Assign the Area Path of work items to an area path you defined. Use [bulk modify](#) to modify several work items at once.

NOTE

While you can assign the same area path to more than one team, this can cause problems if two teams claim ownership over the same set of work items. To learn more, see [About boards and Kanban, Limitations of multi-team Kanban board views](#).

As needed, you can perform the following actions at any time:

- Add additional child nodes
- Rename an Area Path (except the root area path)
- Move a child node under another node
- Delete a child node
- Rename a team
- Change the Area Path assignments made to a team

How many areas should a team define?

You add areas to support your team's traceability and security requirements. Use areas to represent logical or physical components, and then create child areas to represent specific features.

Add areas when you have these requirements:

- Filter queries based on a product or feature area
- Organize or group work items by team or sub-teams
- Restrict access to work items based on their area.

Each team can create a hierarchy of areas under which the team can organize their backlog items, user stories, requirements, tasks, and bugs.

Avoid creating an area structure that is too complex. You can create areas to partition permissions on work items, but complex trees require significant overhead for permission management. You might find that it is too much work to duplicate the structure and permissions in other projects.

End-to-end sequence to define and assign Iteration Paths

Use the following guidance to configure Iteration Paths (aka sprints) for your project and teams:

1. First, define the Area Paths and teams following the guidance provided in [Define area paths and assign to a team](#).
2. Determine the length of the iteration you want to support. Recommended practice is to have all teams use the same sprint cadence.
3. Determine if you want a flat structure or hierarchy of sprints and releases.
4. Open **Project settings>Project configuration** and define the Iteration Paths to support steps 2 and 3 at the

project level. Follow the steps provided later in this article: [Open Project Settings](#), [Project configuration](#) and [Add iterations and set iteration dates](#).

5. Open the team configuration and assign the default and additional Area Path(s) to each team. Follow the steps provided later in this article: [Open team settings](#) and [Set team default iteration path\(s\)](#).
6. Each team should assign the default Iteration Path they selected to their work items. This is needed in order for those work items to show up on their product backlogs and boards. Use [bulk modify](#) to modify several work items at once. See also [Assign backlog items to a sprint](#).

As needed, you can perform the following actions at any time:

- Add additional child iteration nodes
- Rename an Iteration Path (except the root path)
- Move a child Iteration Path under another node
- Delete a child Iteration Path
- Change the default and selected Iteration Paths assigned to a team

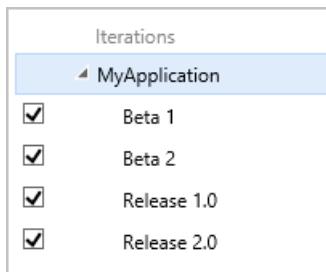
How many iterations should a team define?

You define as many child iterations as you need to reflect your project lifecycle. These paths represent a series of events, such as sprints, pre-beta and beta deliverables, and other release milestones. Teams typically leave work items assigned to the team's default iteration if they are not yet scheduled for work or for a release.

Add iterations to support these requirements:

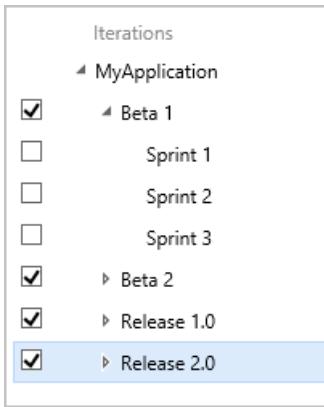
- Define sprints your Scrum teams use to [plan and execute their sprints](#)
- Set up more complex multi-release and sprint cycles
- Filter queries based on sprints, milestones, or cycle time for your project
- Support future work that you're not ready to assign to a target release cycle.

In the following example, Beta 1, Beta 2, Release 1.0, and Release 2.0 are defined for the MyApplication project.



As you create the backlog of product features and tasks, you can start to assign them to the milestones by which you expect the team to finish the features and tasks. As your needs change, you can add events under each major milestone that reflect how your team schedules and manages its work.

As the following example shows, the Beta 1 iteration now contains three child nodes, one for each sprint in the Beta 1 time period.



Iterations do not enforce any rules. For example, you can assign a task to an iteration but not close or complete it during that iteration. At the end of an iteration, you should find all work items that remain active or have not been closed for that iteration and take appropriate action. You can, for example, move them to a different iteration or return them to the backlog.

Naming restrictions

The **Area Path** and **Iteration Path** fields, [data type=TreePath](#), consist of multiple node items which are separated by the backslash (\) character. We recommend that you minimize the names of nodes, and make sure that you conform to the following restrictions when adding child nodes:

RESTRICTION TYPE	RESTRICTION
Node length	Must not contain more than 255 characters
Special characters for nodes	Must not contain Unicode control characters Must not contain any of the following characters: \ / \$? * : " & < # % + Must not contain characters that the local file system prohibits .
Reserved names	Must contain more than a period (.) or two periods (..) Must not be a system-reserved name such as PRN, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, COM10, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, CON, or AUX
Path length	Must contain fewer than 4,000 Unicode characters
Path hierarchy depth	Must be fewer than 14 levels deep

Related articles

As you can see, areas and iterations play a major role in supporting Agile tools and managing work items. You can learn more about working with these fields from these topics:

- [Define area paths and assign to a team](#)
- [Define iteration paths \(aka sprints\) and configure team iterations](#)
- [Agile tools and sprint definitions](#)
- [Query by date or current iteration](#)

Export tree structures

You can't export the structure of tree paths for one project to use with another project.

Supported field rules

You can [specify only a small subset of rules](#), such as `HELPTEXT` and `READONLY` to System.XXX fields.

Team field versus team area path

If your organization has several teams that work from a common backlog and across many product areas, you might want to change how teams are configured. By [adding a custom field to represent teams](#) in your organization, you can reconfigure the agile planning tools and pages to support your teams and decouple assignment to teams and area paths.

Manage and configure team tools

6/13/2019 • 7 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

In this article, learn how to configure team tools and manage teams in Azure DevOps.

Most permissions are governed by security groups or defined at the object level. Team settings are managed by the team administrator role. Users assigned as a team administrator can configure and manage all team tools. Specifically, when a team is added to a project, a project admin should [add one or more team administrators](#).

Then, those team admins should look at doing the following specific tasks:

- Add team members
- Configure area and iteration paths
- Configure backlogs and other common team settings
- Configure Kanban boards

Optional tasks to consider include:

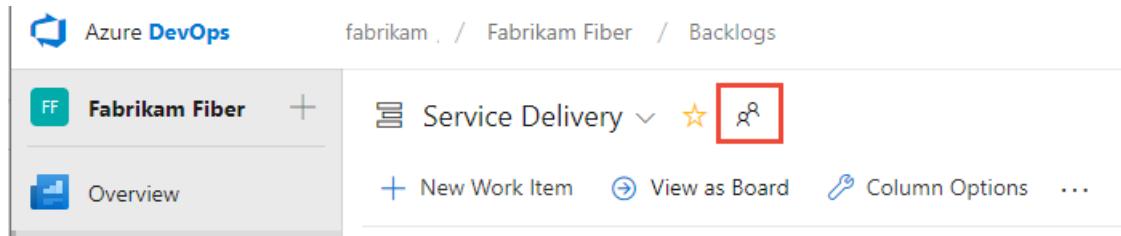
- Configure and manage team dashboards
- Configure team notifications

NOTE

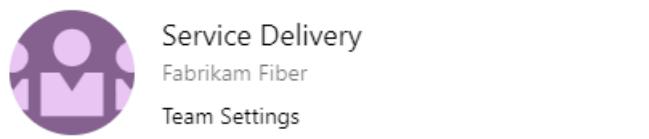
In addition to team administrators, all members of the Project Administrators and Project Collection Administrators groups can manage settings for all teams. To add a team, see [Add teams](#).

Open the team profile and access team tools

- Open a team profile to quickly access items defined for a team. The team profile is available from the **Overview>Dashboards, Boards>Boards, Boards>Backlogs**, and **Boards>Sprints** pages.



A panel opens that shows all items defined for the team.



Items Members (7)

- All Items
- Service Delivery Boards ★
- Service Delivery Backlogs ★
- Sprint 2 Sprints ★
- Overview Dashboards ★

- You can filter the list to show only **Dashboards**, **Boards**, **Backlogs**, or **Sprints** by choosing from the menu.

A screenshot of the same Microsoft Teams service delivery page, but with the "Members" tab selected. The "All Items" dropdown menu is still open, but the background of the page has changed to a light gray. The "Members (7)" link is now underlined in blue. The rest of the interface remains the same, including the team name, icons, and list of items.

- To view the team admins and members of the team, choose **Members**.

The screenshot shows the 'Service Delivery' team settings in Microsoft Teams. The 'Members' tab is selected, highlighted with a red box. The team has 7 members:

- Admins: Cristina Potra
- Members: Christie Church, Chuck Reinhart, Jamal Hartnett, Johnnie McLeod, Raisa Pokrovskaya

- To view or change the team configuration, choose **Team Settings**.

You can then complete the following tasks:

- Add [team members](#)
- Add [team admins](#)
- Navigate to [team notifications](#)
- Navigate to team [iterations](#) and [area paths](#).
- Update the [team description](#) or [profile picture](#).

Add users to a team

Several tools, such as capacity planning, team alerts, and dashboard widgets, are team-scoped. These tools automatically reference the users that are as members of a team to support planning activities or sending alerts.

To add users to a team, see [Add users to a project or specific team](#).

All members of a team can favorite team artifacts and define work item templates. For details, 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, check that they have [the permissions needed for those features](#).

Configure team areas and iterations

Many Agile tools depend on the area and iteration paths that are configured for the team. To learn more

about configuring team areas and iterations, see [About teams and Agile tools](#).

Once project administrators have [added Area Paths](#) and [Iteration Paths](#) for a project, team administrators can select the area and iteration paths associated with their team. These settings affect a number of Agile tools available to the team.

These include making the following associations for each team:

- **Select team area paths**

Can select the default area path(s) associated with the team. These settings affect a number of Agile tools available to the team.

- **Select team iteration paths or sprints** Can select the default area path(s) associated with the team.

These settings affect a number of Agile tools available to the team.

To learn more, see [Define area paths and assign to a team](#) and [Define iteration paths and configure team iterations](#).

Configure team backlogs and other common settings

Team administrators can choose which backlog levels are active for a team. For example, a feature team may choose to show only the product backlog and a management team may choose to show only the feature and epic backlogs. Also, admins can choose whether bugs are treated similar to user stories and requirements or as tasks.

Team admins can also choose which days are non-working days for the team. Sprint planning and tracking tools automatically consider days off when calculating capacity and sprint burndown.

You can configure most of your team settings from the common configuration dialog.

NOTE

The common configuration Settings dialog is available for TFS 2015.1 and later versions.

NOTE

To understand the differences between backlogs, boards, taskboards, and Delivery plans, see [Backlogs, boards, and plans](#). If your backlog or board doesn't show the work items that you expect or want, see [Set up your backlogs and boards](#).

NOTE

To understand the differences between backlogs, boards, and taskboards, see [Backlogs, and boards](#). If your backlog or board doesn't show the work items that you expect or want, see [Set up your backlogs and boards](#).

1. (1) Check that you selected the right project, (2) choose **Boards > Boards**, and then (3) select the correct team from the team selector menu.

The screenshot shows the Azure DevOps interface. At the top left is the 'Azure DevOps' logo. In the top center, there's a breadcrumb navigation bar with 'fabrikam / Fabrikam Fiber'. To its right is a red circle with the number '1'. Below this is a secondary breadcrumb bar with 'Fabrikam Fiber Team' and a red circle with '3' to its right. The main content area has tabs for 'Backlog', 'Analyze', and 'Develop'. On the left, a sidebar menu includes 'Overview', 'Boards' (which is selected and highlighted with a red box and the number '2'), 'Work Items', 'Backlogs', and 'Sprints'. The 'Boards' item is also highlighted with a red box. The central 'Backlog' section shows a card for 'Add an information form' by 'Raisa Pokrovskaya' in 'Iteration ... Sprint 3'. To the right, there's a summary for 'Welcome back page' by 'Johnnie McLeod' in 'Iteration ... Sprint 3', showing 0/4 tasks and 1 bug. A 'Slow form' board for 'Jam' is partially visible on the far right.

2. Make sure that you select the team backlog or board that you want to configure using the team selector. To learn more, see [Use breadcrumbs and selectors to navigate and open artifacts](#).
3. Choose the product or portfolio backlog from the board-selection menu.

This screenshot shows the 'Backlog items' selection menu. It includes options for 'Epics', 'Features', and 'Backlog items'. The 'Backlog items' option is highlighted with a red box. The menu is part of a larger interface with a 'Web' dropdown, a search icon, and other navigation elements.

4. Choose the gear icon to configure the board and set general team settings.

This screenshot shows the same board configuration menu as the previous one, but the gear icon in the top right corner is highlighted with a red box. This icon represents the settings for the board.

5. 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.

Settings

X

Cards

- Fields**
- Styles
- Tag colors

Board

- Columns
- Swimlanes
- Card reordering

Charts

- Cumulative flow

General

- Backlogs
- Working days
- Working with bugs

Fields

Show the important information to your team. Fields are editable directly on the card.

User Story
Bug

Core fields

- Show ID
- Show Assigned To as:

Avatar and full name (default)

▼
- Show Story Points
- Show Tags

Additional fields

Add up to 10 fields in the order that you want them to appear on the card.

+ Field

Show empty fields

- Check if you want to display fields, even when they are empty.

Save
Cancel

1. Make sure that you select the team from the project/team selector. You can switch your team focus to one that you've recently viewed from the project/team selector. If you don't see the team or project you want, choose **Browse...** or choose the Azure DevOps logo to access the [Projects page](#).

The screenshot shows the Azure DevOps navigation bar. The 'Fabrikam Fiber' project is selected. The 'Dashboards' tab is highlighted with a red box. Other tabs include 'Code', 'Work', 'Build & Release', and 'Test'. A gear icon for settings is also present. The left sidebar shows recent projects/teams: 'Fabrikam Fiber Home', 'Recent projects/teams', 'Agile 11', 'FabrikamFiber', 'Fabrikam Fiber A' (which is currently selected), 'Fabrikam Fiber PB', and 'Browse...'. A 'New team' option is also listed. At the bottom of the sidebar, there is a note about the README.md file and a link to learn more about Markdown.

2. Open **Work>Backlogs>Board**.

3. Choose the board you want to configure and then choose the gear icon to configure the board and set general team settings.

For example, from the Kanban board ...

4. Choose a tab under **Cards** or **Board** to configure the cards and Kanban board columns and swimlanes.

![Common configuration dialog team settings]../../../../boards/boards/_img/customize-cards/common-config-141.png)

1. Make sure that you select the team from the project/team selector. You can switch your team focus to one that you've recently viewed from the project/team selector. If you don't see the team or project you want, choose **Browse...** or choose the Azure DevOps logo to access the **Projects** page.

2. Open **Work>Backlogs>Board**.

The screenshot shows the Microsoft Azure DevOps interface for managing work items. The top navigation bar includes 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work', and a search bar. The 'Work' tab is active. Below the navigation is a secondary menu with tabs: 'Work Items*', 'Backlogs', 'Queries', and 'Plans'. The 'Backlogs' tab is selected. On the left, a sidebar lists 'Epics', 'Features', 'Stories' (selected), 'Past', 'Current', and 'Sprint 5'. The main area displays a 'Stories' board for 'Sprint 5'. The 'Board' tab is highlighted with a red box. The board has two columns: 'Backlog' and 'Active'. The 'Backlog' column contains three items: 'Slow response on form' (8 points), 'Add animated emoticons' (3 points), and 'Welcome back page' (3 points). The 'Active' column shows 6 items, with 5 resolved (6/5). To the right, a 'Resolved' column shows 5 items: 'Implement a factory abstracts' (13 points), 'Bug 6' (Raisa Pokrovskaya), and another 'Welcome back page' (3 points). A gear icon in the top right corner of the board area indicates configuration options.

3. Choose the board you want to configure and then choose the gear icon to configure the board and set general team settings.

For example, from the Kanban board ...

The screenshot shows the Microsoft Azure DevOps interface for managing work items using a Kanban board. The top navigation bar includes 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work', and a search bar. The 'Work' tab is active. Below the navigation is a secondary menu with tabs: 'Work Items*', 'Backlogs', 'Queries', and 'Plans'. The 'Backlogs' tab is selected. On the left, a sidebar lists 'Epics', 'Features', 'Stories' (selected), 'Past', 'Current', and 'Sprint 5'. The main area displays a 'Stories' board. The 'Board' tab is highlighted with a red box. The board has four columns: 'Backlog', 'Analyze', 'Develop', and 'Test'. The 'Backlog' column contains one card: 'Change the initial view'. The 'Analyze' column contains two cards: 'Interim save on long forms' and 'Change the initial view'. The 'Develop' column contains one card: 'Change the initial view'. The 'Test' column contains one card: 'Welcome back page'. A gear icon in the top right corner of the board area indicates configuration options.

4. Choose a tab under **Cards** or **Board** to configure the cards and Kanban board columns and swimlanes.

Settings

X

Cards

Fields

Styles

Tag colors

Board

Columns

Swimlanes

Card reordering

Charts

Cumulative flow

General

Backlogs

Working days

Working with bugs

Fields

Show the important information to your team. Fields are editable directly on the card.

User Story

Bug

Core fields

Show ID

Show Assigned To as:

Avatar and full name (default)

Show Story Points

Show Tags

Additional fields

Add up to 10 fields in the order that you want them to appear on the card.

+ Field

Show empty fields

Check if you want to display fields, even when they are empty.

Save

Cancel

For details on each configuration option, see one of the following articles:

AREA	CONFIGURATION TASK
Cards	<ul style="list-style-type: none">• Add fields• Define styles• Add tag colors• Enable annotations• Configure inline tests
Boards	<ul style="list-style-type: none">• Add columns• Add swimlanes• Card reordering• Configure status badges
Chart	<ul style="list-style-type: none">• Configure cumulative flow chart
General	<ul style="list-style-type: none">• Backlogs• Working days• Working with bugs
AREA	CONFIGURATION TASK

Cards	<ul style="list-style-type: none"> • Add fields • Define styles • Add tag colors • Enable annotations • Configure inline tests
Boards	<ul style="list-style-type: none"> • Add columns • Add swimlanes • Card reordering
Chart	<ul style="list-style-type: none"> • Configure cumulative flow chart
General	<ul style="list-style-type: none"> • Backlogs • Working days • Working with bugs

For details on each configuration option, see one of the following articles:

AREA	CONFIGURATION TASK
Cards	<ul style="list-style-type: none"> • Add fields • Define styles • Add tag colors
Boards	<ul style="list-style-type: none"> • Add columns
Chart	<ul style="list-style-type: none"> • Configure cumulative flow chart
General	<ul style="list-style-type: none"> • Backlogs • Working days • Working with bugs

Configure Kanban boards

Team administrators can fully customize the team's Kanban boards associate with the product and portfolio backlogs. You configure a Kanban board by first defining the columns and WIP limits from the common configuration dialog. For guidance, see [Kanban basics](#).

- [Columns](#)
- [WIP limits](#)
- [Definition of Done](#)

Additional elements you can configure include:

- [Split columns](#)
- [Swimlanes](#)
- [Card fields, styles, tag colors, annotations, and card reordering](#)

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 details, see [Add and manage dashboards](#).

Team administrators can add, configure, and manage permissions for team dashboards. For details, see [Add and manage dashboards](#).

Update team description and picture

Team settings also include the team name, description, and team profile image. To add a team picture. Open the Team Profile and choose the picture icon. The maximum file size is 4 MB.

Manage team notifications

Team administrators can add and modify alerts so that the team can receive email notifications as changes occur to work items, code reviews, source control files, and builds. A number of alerts are defined for each team. For details, see [Manage team alerts](#).

Manage team rooms

Team administrators can add users and events to team rooms, and add team rooms. Team rooms are chat rooms limited to team members. For details, see [Collaborate in a team room](#).

NOTE

Team rooms are deprecated for TFS 2018 and later versions as described in [Deprecation of team rooms](#) blog post. Several good solutions are available that integrate well with TFS that support notifications and chat, such as [Microsoft Teams](#) and [Slack](#).

Related articles

- [About projects and scaling your organization](#)
- [About teams and Agile tools](#)
- [Add teams](#)
- [Add a team administrator](#)

Select backlog navigation levels for your team

6/13/2019 • 2 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

Each team can determine the backlog levels that they use. For example, feature teams may want to only focus on their product backlog, while a management team may choose to only show feature and epics (the two default portfolio backlogs). You configure which backlog levels appear from your team settings dialog.

If you want additional portfolio backlogs, see the following topics based on the process model you use:

- **Inheritance:** [Customize your backlogs or boards for a process](#)
- **Hosted XML:** [Add portfolio backlogs](#).

For an overview of process models, see [Customize your work tracking experience](#).

If you want additional portfolio backlogs, see [Add portfolio backlogs](#).

NOTE

Feature availability: The team setting for choosing which backlog levels is available for TFS 2015 and later versions. For TFS 2013, the Feature portfolio backlog level is enabled for all teams.

Prerequisites

- To configure team settings, you must be [added as a team administrator](#) or be a member of the **Project Administrators** or **Project Collection Administrators** group. See [Set permissions at the project- or collection-level](#).

Set your team's preferences for backlog levels

Because this setting affects all team members' view of the team backlogs and boards, you must be a team administrator to change the setting. Changing the setting is disabled if you're not a team administrator. Go [here](#) to get added as a team administrator.

You can change the setting from a backlog or board view. Here we show how to change it from the board view.

1. [Open your Kanban board](#). If you're not a team admin, [get added as one](#). Only team and project admins can customize the Kanban board.
2. Choose the  gear icon to configure the board and set general team settings.



3. Choose **Backlogs** and check the boxes of those backlog levels you want your team to manage.

Settings

Cards
Backlogs

Fields
See only the backlogs your team manages.

Styles
Backlog navigation levels

Tag colors
 Epics

Annotations
 Features

Tests
 Backlog items

Board
Columns

Swimlanes
Card reordering

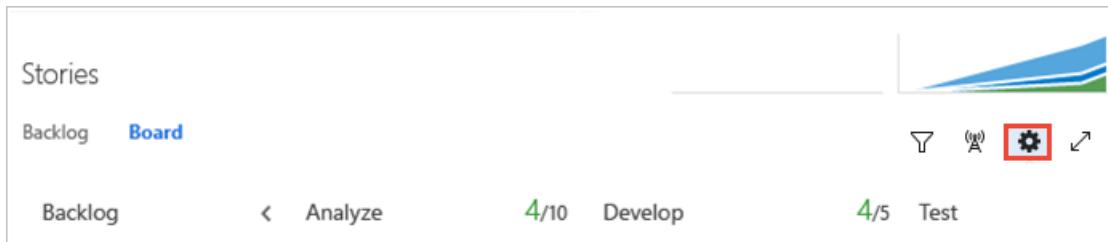
Charts
Cumulative flow

General
Working days

Backlogs *
Working with bugs

Save
Cancel

4. When done with your changes, choose **Save**.
5. To see the changes, open or refresh your team's [backlog](#).
1. Open your Kanban board. If you're not a team admin, [get added as one](#). Only team and project admins can customize the Kanban board.
2. Choose the  gear icon to open the settings dialog.



The screenshot shows a Microsoft Kanban board interface. At the top left, there's a "Stories" section. Below it, a navigation bar has "Backlog" and "Board" tabs, with "Board" being active. On the far right of the navigation bar is a gear icon, which is highlighted with a red box. Below the navigation bar, there are four columns: "Backlog", "Analyze", "Develop", and "Test". Each column has a progress bar and some numerical values: "Backlog" has "4/10", "Analyze" has "4/5", "Develop" has "4/10", and "Test" has "4/5".

3. Choose **Backlogs** and check the boxes of those backlog levels you want your team to manage.

Settings

Cards

- Fields
- Styles
- Tag colors
- Annotations
- Tests

Board

- Columns
- Swimlanes
- Card reordering

Charts

- Cumulative flow

General

Backlogs *

- Working days
- Working with bugs

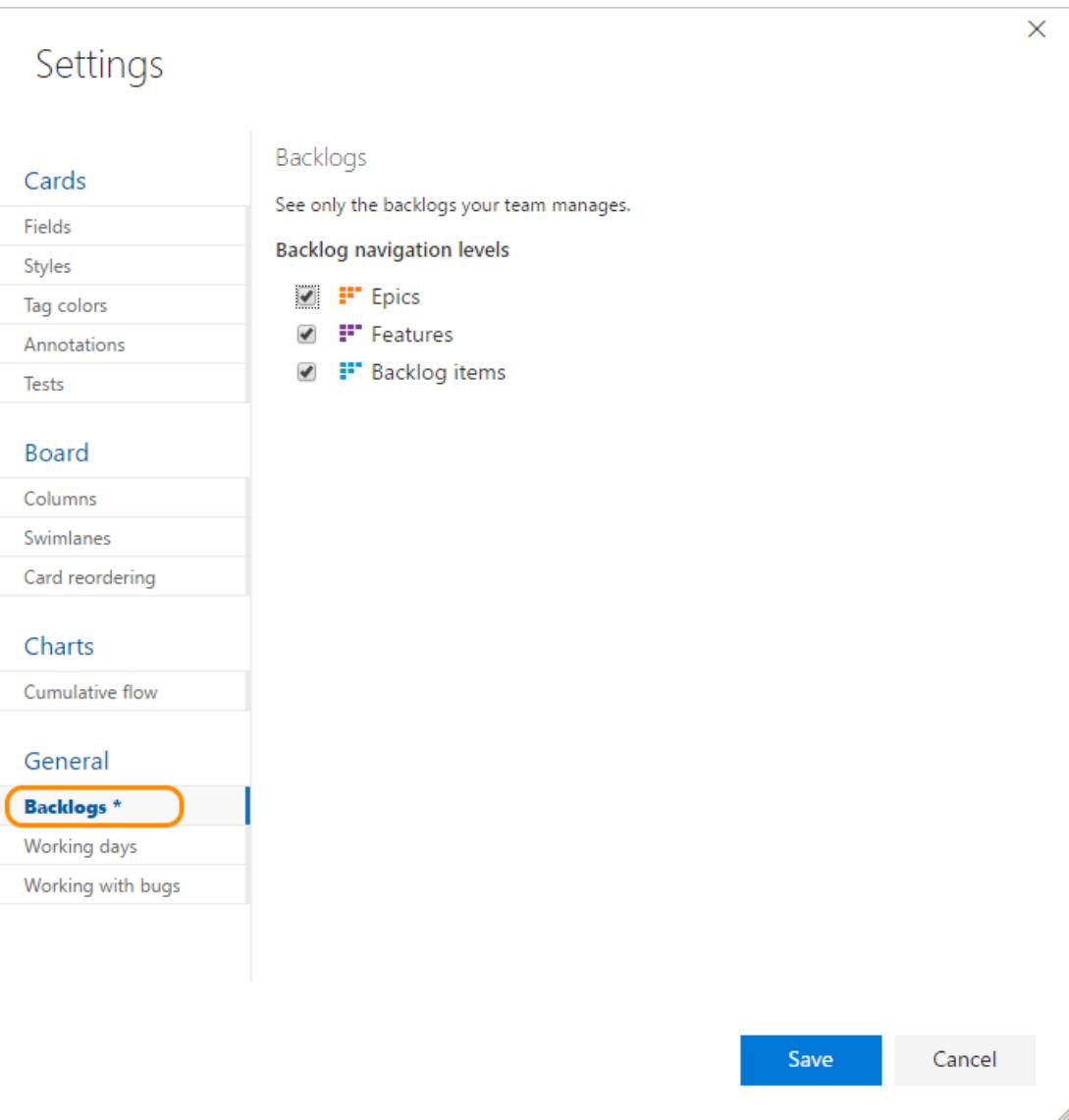
Backlogs

See only the backlogs your team manages.

Backlog navigation levels

- Epics
- Features
- Backlog items

Save **Cancel**



- When done with your changes, choose **Save**.
- To see the changes, open or refresh your team's [backlog](#).

Requires TFS 2015.1 or later version.

- From your web portal, choose the gear icon to open the administration page.



- From **Overview**, choose the team whose settings you want to configure, and then choose **Settings**.
- Check the boxes of those backlog levels you want your team to manage.

Overview Security Alerts Build Version Control Service Hooks Services

Team Profile

Fabrikam Fiber Team

Members **Settings**

Backlogs

Select the backlog levels that your team will manage.

Epics

Features

Backlog items

Name
Fabrikam Fiber Team

4. To see the changes, open or refresh your team's [backlog](#).

Related articles

- [Get started with Agile tools to plan and track work](#)
- [Backlogs, boards, and plans](#)
- [Create your backlog](#)
- [Define features and epics](#)
- [Organize your backlog](#)

Show bugs on backlogs and boards

6/14/2019 • 4 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

As your team identifies code defects or bugs, they can add them to the backlog and track them similar to requirements. Or, they can schedule them to be fixed within a sprint along with other tasks.

NOTE

You can define this team setting for the [Agile](#), [Scrum](#), and [CMMI](#) processes. The Bug work item type isn't defined for the [Basic](#) process, so there isn't a team setting for Basic. Instead, you should track bugs and code defects using the Issue work item type.

When you track bugs as requirements, they'll show up on the product backlog and Kanban board. When you track bugs similar to tasks, they'll show up on the sprint backlogs and task boards. If you want to track additional work item types (WITs) or custom WITs on your backlogs or boards, you can. See [Add other work item types to backlogs or boards](#) later in this topic.

Prerequisites

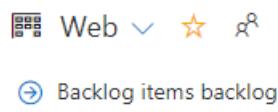
- To configure team settings, you must be [added as a team administrator](#) or be a member of the **Project Administrators** or **Project Collection Administrators** group. See [Set permissions at the project- or collection-level](#).

Set your team's preferences for tracking bugs

You can change the setting from a backlog or board view. Here we show how to change it from the board view.

In the **Working with bugs** dialog, you can select from the following three options.

- Choose the first option when your team wants to manage bugs similar to requirements. Bugs can be estimated and tracked against team velocity and cumulative flow. Bugs are associated with the Requirements category.
 - Choose the second option when your team wants to manage bugs similar to tasks. Remaining work can be tracked for bugs and tracked against the sprint capacity and burndown. Bugs are associated with the Task category.
 - Choose the last option if your team manages bugs separate from requirements or tasks. Bugs are associated with the Bugs category and won't appear on either backlogs or boards.
- [Open your Kanban board](#). If you're not a team admin, [get added as one](#). Only team and project admins can customize the Kanban board.
 - Choose the gear icon to configure the board and set general team settings.



3. Choose **Working with bugs** and then choose the option that best meets your team's way of working.

The screenshot shows the 'Settings' dialog box. On the left, a sidebar lists various settings categories: Cards, Fields, Styles, Tag colors, Annotations, Tests, Board, Columns, Swimlanes, Card reordering, Charts, Cumulative flow, General, Backlogs, Working days, and Working with bugs. The 'Working with bugs' item is highlighted with a red box. The main content area is titled 'Working with bugs' and contains the following text: 'Set your team's preference for how they manage bugs. Your selection determines where bugs appear in the hierarchy and on backlogs and boards.' Below this is a list of three options, each with a radio button:

- Bugs are managed with requirements. [\(i\)](#)
- Bugs are managed with tasks. [\(i\)](#)
- Bugs are not managed on backlogs and boards. [\(i\)](#)

At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

4. When done with your changes, choose **Save**.

5. To see the changes, open or refresh the team's [backlog](#) or [Kanban board](#).

1. [Open your Kanban board](#). If you're not a team admin, [get added as one](#). Only team and project admins can customize the Kanban board.

2. Choose the  gear icon to open the settings dialog.

The screenshot shows the Kanban board settings dialog. At the top left is the word 'Stories'. Below it are two tabs: 'Backlog' and 'Board', with 'Board' being the active tab. On the far right are four icons: a downward arrow, a person icon, a gear icon (which is highlighted with a red box), and a refresh arrow. Below these are four status indicators: 'Backlog' (green), 'Analyze' (light blue), 'Develop' (blue), and 'Test' (light green). Each indicator shows a count: '4/10' for Analyze, '4/5' for Develop, and '4/5' for Test.

3. Choose **Working with bugs** and then choose the option that best meets your team's way of working.

X

Settings

Cards Working with bugs

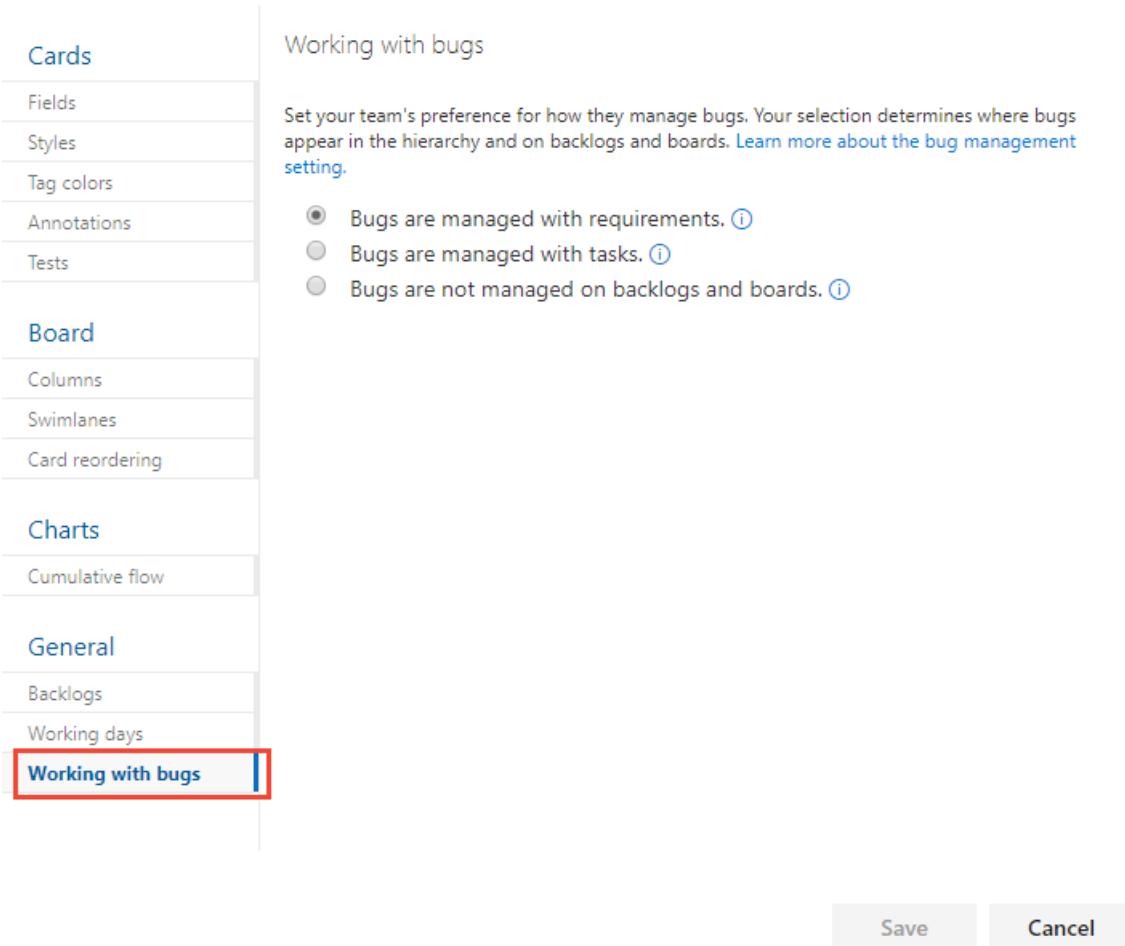
Fields Styles Tag colors Annotations Tests

Board Columns Swimlanes Card reordering

Charts Cumulative flow

General Backlogs Working days Working with bugs

Save Cancel



4. When done with your changes, choose **Save**.
5. To see the changes, open or refresh your team's [backlog](#) or [Kanban board](#).

Requires TFS 2013.4 or later version.

1. Open your team settings from the **Overview** tab of your team's admin context. Your changes are automatically saved.
2. Choose the  (gear icon) to open the administration page.



3. From the **Overview** tab, choose the team whose settings you want to configure, and then choose **Settings**. Select the option you want. Your changes are automatically saved.

Overview Security Alerts Version Control

Team Profile



Fabrikam Fiber Team

Members [Settings](#)

Working Days

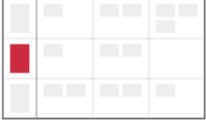
Select the working days in the week for your team. Selected days are shown on t...

Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

Bugs

Choose the behavior of bugs (shown as ■) on your backlogs and boards. [Learn...](#)

Bugs appear on the backlogs and boards with requirements.


Bugs appear on the backlogs and boards with tasks.


Bugs do not appear on backlog or boards.

- To see the changes, open or refresh the team's [backlog](#) or [Kanban board](#).

Nested items

TIP

If, after refreshing a backlog or board, and you don't see bugs where you expect them, review [How backlogs and boards display hierarchical \(nested\) items](#). Only leaf nodes of nested items appear on the Kanban or task boards.

When you manage bugs with requirements or with tasks, they'll show up on one or more of your Agile tool backlogs and boards. However, if you nest items—create parent-child links of items that belong in either the Requirements or Task categories—then not all items may appear on your backlogs and boards. To learn more about how nested items are treated, see [How backlogs and boards display hierarchical \(nested\) items](#).

Add other work item types to your backlogs or boards

Bugs are a common item that teams want to track, and choose how they track it. See [Manage bugs](#) for more guidance.

However, what if you want to track other work item types (WITs) on your backlogs and boards?

You can add other WITs—such as change requests, issues, or impediments—by customizing your process or project, based on the process model you use. For details,

- For the Inheritance process model, see [Customize your backlogs or boards for a process](#).
- For Hosted XML and On-premises XML process models, see [Add a work item type to a backlog and board](#).

You can add other WITs—such as change requests, issues, or impediments—by customizing your process or project, based on the process model you use. For details, see [Add a work item type to a backlog and board](#).

For an overview of process models, see [Customize your work tracking experience](#).

Create, list, and manage bugs

When bugs are managed along with requirements, you can add them through the [product backlog](#) or [Kanban board](#). When bugs are managed along with tasks, you can add them to a [sprint backlog](#) or [taskboard](#). Or, you can capture them using other tools as indicated in [Define, triage, and manage bugs](#).

You can review bugs defined for your project by creating a query and specifying the **Work Item Type=Bug**. Or, open a predefined query, **Active Bugs** (Agile and CMMI) or **Work in Progress** (Scrum). For other bug related tasks, see the following articles:

- [View, run, or email a work item query](#)
- [View and add work items using the Work Items page](#)
- [Triage work items](#)
- [Query by assignment or workflow changes](#)
- [View, run, or email a work item query](#)
- [Triage work items](#)
- [Query by assignment or workflow changes](#)

Related articles

- [Enable backlog levels of interest to your team](#)
- [Manage teams and configure team tools](#)

Set working days

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

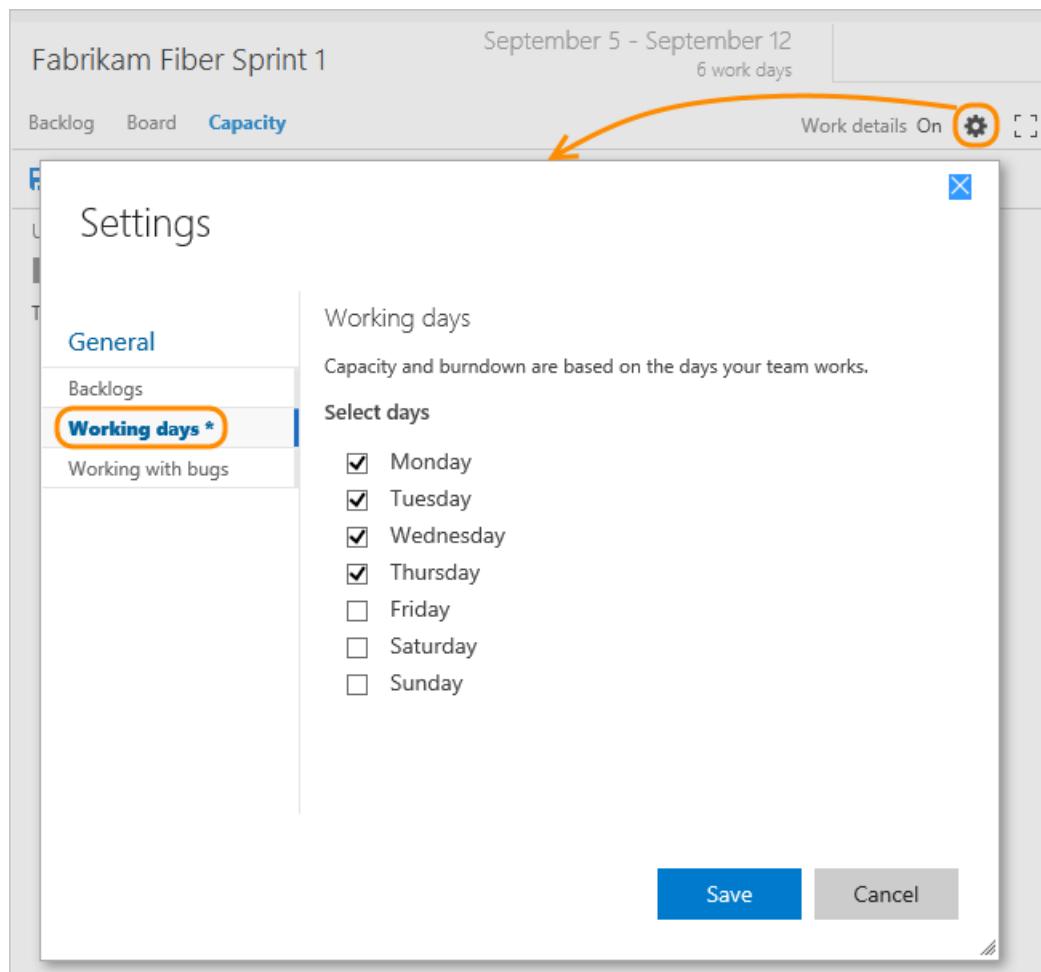
Each team's sprint planning and tracking tools automatically consider days off when calculating capacity and sprint burndown. Leave those days of the week that your team doesn't work unchecked in your team's Settings, Working days page.

Prerequisites

- To configure team settings, you must be [added as a team administrator](#) or be a member of the **Project Administrators** or **Project Collection Administrators** group. See [Set permissions at the project- or collection-level](#).

Configure working days

Open the [Capacity page](#), and then choose the gear icon to open the settings dialog.



Open your team settings from the **Overview** tab of your team's admin context. Check or uncheck one or more days. Your changes are automatically saved.

Overview

Security

Alerts

Version Control

Services

Team Profile



Name

Fabrikam Fiber Team

Description

The default project team.

Administrators

Fabrikam Fiber Team

Members

Settings

Working Days

Select the working days in the week for your team. Selected days are shown in orange. You can also set non-working days for your team based on team capacity.

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

To set non-working days, modify the **ProcessConfiguration** file. For details, see [Process configuration XML element reference](#), [Set non-working days](#).

Related articles

- [About Sprints, Scrum and project management](#)
- [Scrum and sprint planning tools](#)
- [Manage teams and configure team tools](#)

Tutorial: Set personal or team favorites

6/13/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

Favorite  those views that you frequently access. You can favorite all sorts of Azure DevOps features and tools—such as a project, repository, build pipeline, dashboard, backlog, board, or query. You can set favorites for yourself or your team.

As your code base, work tracking efforts, developer operations, and organization grows, you'll want to be able to quickly navigate to those view of interest to you and your team. Setting favorites allows you to do just that.

Team favorites are a quick way for members of your team to quickly access shared resources of interest. You favorite an item for yourself by choosing the  star icon. The favorited item will then show up easily from one or more directory lists. You set favorites for a team through the context menu for the definition, view, or artifact.

In this tutorial you'll learn how to view your personal favorites and to favorite or unfavorite the following views:

- Project or team
- Dashboard
- Team backlog, board, shared query, or other Azure Boards view
- Repository
- Build and release definition
- Test plans

- Project
- Shared query
- Repository
- Build and release definition
- Test plans

Prerequisites

- You must connect to a project through the web portal. If you don't have a project yet, [create one](#). To connect to the web portal, see [Connect to a project](#).
- You must be a member of the **Contributors** or an administrators security group of the project. To get added, [Add users to a project or team](#).
- To favorite projects, backlogs, boards, queries, dashboards, or pipeline views, you must have **Stakeholder** access or higher.
- To favorite repositories, or delivery plans, you must have **Basic** access or higher.
- To favorite test plans, you must have **Basic + Test Plans** access level or equivalent.

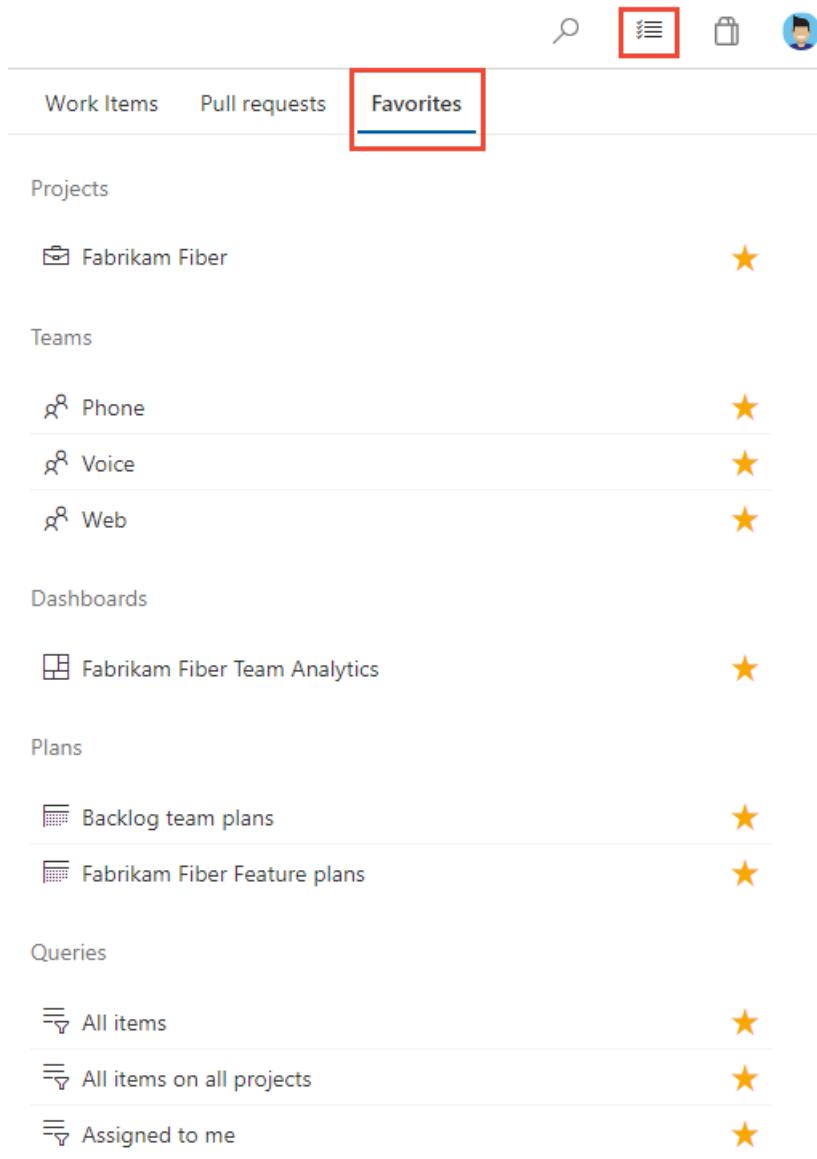
- You must connect to a project through the web portal. If you don't have a project yet, [create one](#). To connect to the web portal, see [Connect to a project](#).
- You must be a member of the **Contributors** or an administrators security group of the project. To get added, [Add users to a project or team](#).
- To favorite projects, backlogs, boards, queries, dashboards, or pipeline views, you must have **Stakeholder** access or higher.
- To favorite repositories, or delivery plans, you must have **Basic** access or higher.

- To favorite test plans, you must have **Basic + Test Plans** access level or equivalent.

For details about the different access levels, see [About access levels](#).

View personal favorites

Access views that you have favorited by choosing the  inbox icon, and then choosing **Favorites**.

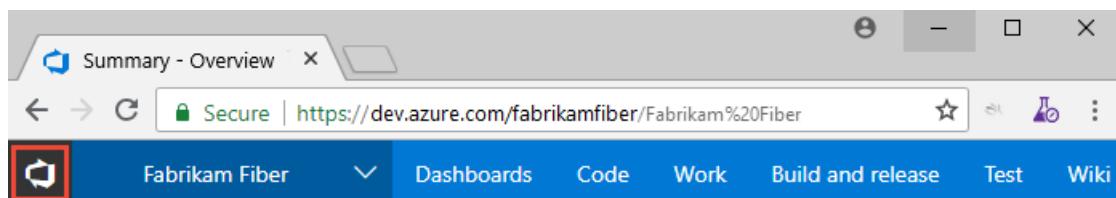


Category	Item	Favorite Status
Projects	Fabrikam Fiber	★
	Phone	★
	Voice	★
Teams	Web	★
	Fabrikam Fiber Team Analytics	★
	Backlog team plans	★
Fabrikam Fiber Feature plans	★	
Queries	All items	★
	All items on all projects	★
	Assigned to me	★

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](#).

1. Access views that you have favorited by choosing the  Azure DevOps logo to open **Projects**.



2. Choose **My Favorites** to quickly access any view or item that you've marked as a favorite.

Favorites

Filter favorites



Queries

Bug Triage	Fabrikam Fiber	.../Shared Queries/Current Iteration	
My Bugs	Contoso	Shared Queries	
Open User Stories	Contoso	.../Shared Queries/Current Iteration	
Product Planning	Fabrikam Fiber	Shared Queries	
Product Planning	Contoso	Shared Queries	

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 'Fabrikam Fiber', 'Overview', 'Summary' (which is 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 'Add tags' and a 'README.md' file entry with the text: 'minor modification to test development section in mobile form', 'Update this README.md file.', and 'A README.md file is intended to quickly orient readers to what your project'. The URL in the browser bar is https://dev.azure.com/fabrikamfiber/Fabrikam%20Fiber.

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 > Backlog items backlog' page. At the top, there are two tabs: 'Phone' (selected) and 'Backlog items backlog' (highlighted with a red box). Below the tabs, there are several icons for filtering and managing the backlog, including a star icon. The main area displays a horizontal bar chart representing the backlog status.

3. To favorite other team artifacts, choose the team icon, and then choose the star icon next to one of the listed artifacts.

Phone

Fabrikam Fiber

Team Settings

Items Members (1)

All Items

Phone Boards

Phone Backlogs

Phone Sprints

Favorite a project

To favorite a project, open the project **Summary** page and choose the star icon.

FabrikamFiber

Customer-focused apps under development based on Agile process.

Members

K

Activity

Code

Build & Rel

Setup Build

Learn more about continuous integration

Or, you can favorite a project from the **Projects** page by choosing the star icon next to the project.

Favorite a dashboard

- From **Overview>Dashboards**, open the selector and choose the **Browse all dashboards** option.

The screenshot shows the Microsoft Power BI 'Mine' dashboard. On the left, there's a sidebar with a search bar at the top labeled 'Search dashboards'. Below it is a section titled 'Favorites' containing 'Fabrikam Team Analytics' with a yellow star icon. Under 'Account Management', there's 'Account Management Overview'. Under 'Customer Profile', there's 'Customer Profile Overview'. Under 'Fabrikam Team', there's 'Fabrikam Team Analytics' with a yellow star icon. At the bottom of the sidebar is a red-bordered button labeled 'Browse all dashboards'. The main area displays several cards: a green card for 'Fabrikam Team' showing '6 Items', a purple card for 'Fabrikam Fiber' showing '0 Commits in last 7 days', and a grey card for 'Work items by State' showing '11' items updated on '23 - November 10'.

2. The **Mine** page shows your favorited dashboards, and all dashboards of teams that you belong to. The **All** page (shown below) lists all dashboards defined for the project in alphabetical order. You can filter the list by team or by keyword.

The screenshot shows the Microsoft Power BI 'All' dashboard list. At the top, there are tabs for 'Mine' (highlighted with a red box) and 'All' (highlighted with a red box), a '+ New dashboard' button, and a filter icon. Below the tabs is a 'Filter dashboards' button and a 'Filter by team' dropdown menu with a search bar and a list of teams: Account Management, Customer Profile, Email, Fabrikam Team, Internet, Phone, Service Delivery, and Service Status. A 'Clear' button is at the bottom of the filter menu. The main list shows various dashboards with columns for Name, Team, and a star icon indicating favoriting. The dashboards listed include '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), and 'Work in Progress' (Internet). An 'Active work items' button is at the bottom right.

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.



Favoriting a dashboard will cause it to appear on your **Favorites** page and towards the top in the **Dashboards** selection menu.

Favorite a team's backlog, Kanban 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**.

A screenshot of the Boards page in Azure DevOps for the 'Fabrikam Fiber' project. The left sidebar shows navigation options: Overview, Boards, Work Items, Boards, Backlogs (which is highlighted with a red box), Sprints, and Queries. The main area shows a list of backlog items for the 'Fabrikam Fiber Team'. The first item, 'Hello World Web Site', has a yellow star icon next to it, indicating it is favorited. The list includes:

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 dropdown menu titled "Fabrikam Fiber Team". At the top left of the menu, there is a red box highlighting the team name. Below the title, there is a search bar labeled "Search team backlogs". The menu lists several backlog items under "My Team Backlogs": "Account Management", "Customer Profile", "Fabrikam Team" (which is selected and highlighted), "Phone", "Service Delivery", "Service Status", and "Shopping Cart". At the bottom of the menu, there is a link "Browse all backlogs".

2. Choose the star icon to favorite a team backlog. Favorited artifacts (favorited 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.

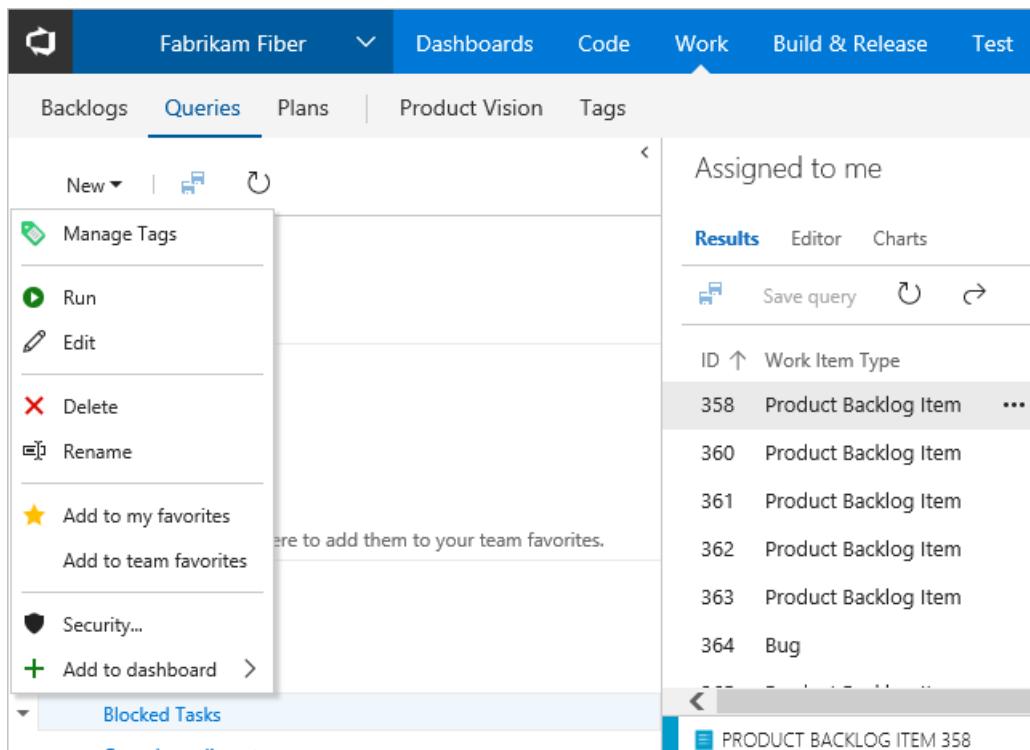
Or, open the context menu of the query, and then select **Add to Team Favorites**, and then select from the list of teams.

Queries

The screenshot shows the "Queries" page with the "All" tab selected. On the left, there is a sidebar with sections "Title", "My Queries", "Shared Queries", and "Current Sprint". Under "Shared Queries", there is a list of queries: "Blocked Tasks" (selected and highlighted with a red box), "Open Impediments", "Test Cases", "Unfinished Work", "Work in Progress", "Triage folder", "All items", "All items in a tree query", and "Feedback". To the right of the sidebar, there is a list of queries. A context menu is open over the "Blocked Tasks" query, showing options: "Run query", "Edit", "Rename", "Delete", "Add to Team Favorites" (highlighted with a red box), "Security...", and "Manage Tags". A second red box highlights the "Phone" team selection in the "Add to Team Favorites" dropdown menu. At the top right, there is a "Filter by keywords" search bar and a refresh icon.

You can also set a query as a personal favorite by opening the query and choosing the star icon.

Open **Work>Queries**. Next, open the *** actions icon menu of the shared query you want to favorite, and then select **Add to my favorites** or **Add to team favorites**.



The screenshot shows the 'Queries' page in the 'Work' section of Azure DevOps. The left sidebar has options like 'Manage Tags', 'Run', 'Edit', 'Delete', 'Rename', 'Add to my favorites', 'Add to team favorites', 'Security...', and 'Add to dashboard'. The main area shows a list of results under 'Assigned to me'. The first item in the list is selected, and its details are shown in the bottom right corner: 'PRODUCT BACKLOG ITEM 358'.

Favorite a delivery plan

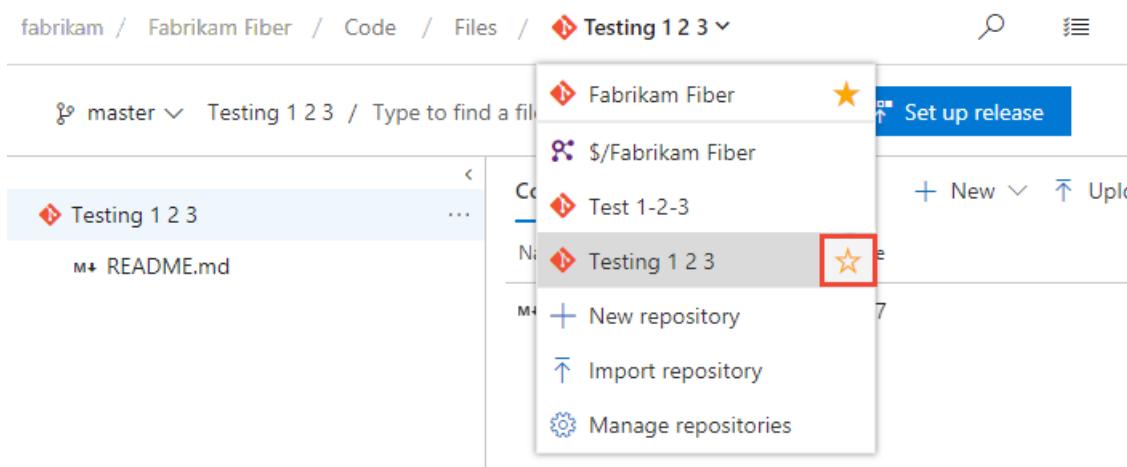
To learn more about delivery plans, see [Review team Delivery Plans](#).

To mark a delivery plan as a favorite, open the **Boards>Plans** page and choose the  star icon next to the Delivery Plan.

To mark a delivery plan as a favorite, open the **Work>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.



The screenshot shows the 'Code' page in the 'Fabrikam Fiber' project. The repository selector on the right shows several repositories: 'Fabrikam Fiber' (selected), '\$/Fabrikam Fiber', 'Test 1-2-3', 'Testing 1 2 3' (highlighted with a red box), 'New repository', 'Import repository', and 'Manage repositories'. The 'Testing 1 2 3' repository is currently selected.

From any **Code** page, open the repository selector and choose the star icon next to the repository you want to favorite.

The screenshot shows the 'Fabrikam Fiber' repository selected in the repository selector. The star icon next to 'Fabrikam Fiber' is highlighted with a red box. The main pane displays the contents of the repository, including files like 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md' with their respective last change dates and commit IDs.

Favorite a build pipeline

Open **Pipelines>Builds** and choose either **Mine** or **Definitions** page. 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 with the 'Mine' tab selected. A context menu is open for the 'fabrikam build' definition, with the 'Add to my favorites' option highlighted with a red box. Other options in the menu include 'Queue new build...', 'Edit definition', 'Pause', 'View builds', 'Add to team favorites >', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', and 'Security...'. The 'fabrikam build' definition has a status of 'No builds have run...'.

Open **Build and Release>Builds** and choose either **Mine** or **Definitions** page. 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', 'All Definitions', 'Queued', and 'XAML'. A search bar at the top right contains the placeholder 'Build ID or build number' with a magnifying glass icon. Below the tabs, a table header includes columns for 'Recently built', 'Status', and 'Triggered by'. A single row is visible, representing a build definition named 'fabrikam build'. To the left of the definition name is a user icon with a checkmark. To the right are a star icon, three dots for more options, and a note stating 'No builds have r...'. A context menu is open over the definition name, listing several options: 'Queue new build...', 'Edit...', 'View definition summary', 'Add to my favorites' (which is highlighted with a red box), 'Add to team favorites', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', and 'Security...'.

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.

To mark a test plan as a favorite, open the **Test>Test Plans** page and choose the star icon next to a test plan from the menu that shows All test plans.

Unfavorite a view you've favorited

You can unfavorite an artifact from your **Favorites** page. Choose the inbox icon, and then choose **Favorites**. Choose the favorited icon of a currently favorited artifact.

The screenshot shows the 'Favorites' section of the Microsoft Project interface. At the top, there are navigation links: 'Work Items', 'Pull requests', and 'Favorites'. The 'Favorites' link is underlined and has a red box drawn around it. Below the navigation, there are sections for 'Projects', 'Teams', 'Dashboards', 'Plans', and 'Queries'. Each section contains a list of items with their icons and star ratings. For example, under 'Projects', there is 'Fabrikam Fiber' with a yellow star. Under 'Teams', there are 'Phone', 'Voice', and 'Web' with yellow stars. Under 'Dashboards', there is 'Fabrikam Fiber Team Analytics' with a yellow star. Under 'Plans', there are 'Backlog team plans' and 'Fabrikam Fiber Feature plans' with yellow stars. Under 'Queries', there are 'All items', 'All items on all projects', and 'Assigned to me' with yellow stars.

Category	Artifact	Rating
Projects	Fabrikam Fiber	★
	Phone	★
	Voice	★
Teams	Web	★
	Fabrikam Fiber Team Analytics	★
	Backlog team plans	★
Fabrikam Fiber Feature plans	★	
Queries	All items	★
	All items on all projects	★
	Assigned to me	★

Similarly, you can unfavorite an artifact from the same page where you favorited it.

You can unfavorite an artifact from the **Projects>Favorites** page and choose the ★ favorited icon of a currently favorited artifact.

Similarly, you can unfavorite an artifact from the same page where you favorited it.

Try this next

[Follow a user story, bug, issue, or other work item or pull request](#)

Related articles

- [Manage personal notifications](#)
- [Set your preferences](#)

Manage Projects

5/7/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Structure your projects by adding area paths, iteration paths, and teams.

5-minute quickstarts

- [Get started as an administrator](#)
- [Share your project vision](#)
- [Define area paths](#)
- [Define iteration paths or sprints](#)
- [Add a team](#)
- [Add users to a project or team](#)
- [Add administrators or set permissions at the project or collection level](#)

Step-by-step tutorials

- [Change individual permissions, grant select access to specific functions](#)
- [Grant or restrict permissions to select tasks](#)
- [Customize a project \(Azure DevOps Services\)](#)

Concepts

- [Customize a project](#)
- [About areas and iterations](#)
- [About teams and Agile tools](#)
- [Resources granted to project members](#)

How-to guides

- [Create a project](#)
 - [Rename a project](#)
 - [Delete a project](#)
 - [Restore a project](#)
 - [Change service visibility](#)
 - [Connect to projects](#)
-
- [Create a project](#)
 - [Rename a project](#)
 - [Delete a project](#)
 - [Change service visibility](#)
 - [Connect to projects](#)

Reference

- [Default permissions and access](#)

- [Permission lookup guide \(Security\)](#)
- [Azure DevOps data protection overview](#)

Resources

- [Get Started using Azure DevOps](#)
- [Marketplace & Extensibility](#)
- [Public Projects](#)
- [Migrate from Azure DevOps Server to Azure DevOps Services](#)

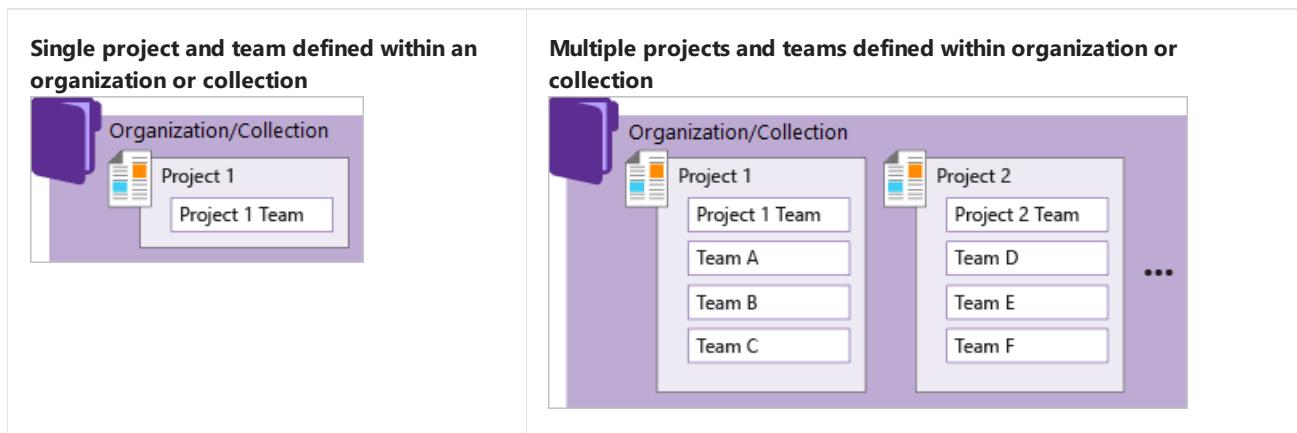
About projects and scaling your organization

6/3/2019 • 8 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

A project provides a repository for source code and a place for a group of people to plan, track progress, and collaborate on building software solutions. It represents a fundamental container where data is stored when added to Azure DevOps.

When you create your project, a team of the same name is automatically created. For small teams, this is sufficient. However, for enterprise-level organizations, it may be necessary to scale up, to create additional teams and/or projects. These can be created within the single account or collection.



The collection-project-team structure provides teams a high-level of autonomy to configure their tools in ways that work for them. It also supports administrative tasks to occur at the appropriate level. As your organization grows, your tools can grow to support a [culture of team autonomy as well as organizational alignment](#).

How do you manage work across the enterprise?

How do you scale your DevOps and Agile tools to support your growing enterprise?

When you connect to Azure DevOps, you connect to an organization or project collection. Within that container, one or more projects may be defined. At a minimum, at least one project must be created in order to use the system.

You can scale your organization in the following ways:

- To support different business units, you can add projects
- Within a project, you can add teams
- Add repositories and branches
- To support continuous integration and deployment, you can add agents, agent pools, and deployment pools
- To manage a large number of users, you can manage access through Azure Active Directory

You can scale your on-premises TFS deployment in the following ways:

- To increase performance, you can add server instances
- To support different business units, you can add project collections and projects
- Within a project, you can add teams
- Add repositories and branches
- To support continuous integration and deployment, you can add agents, agent pools, and deployment pools

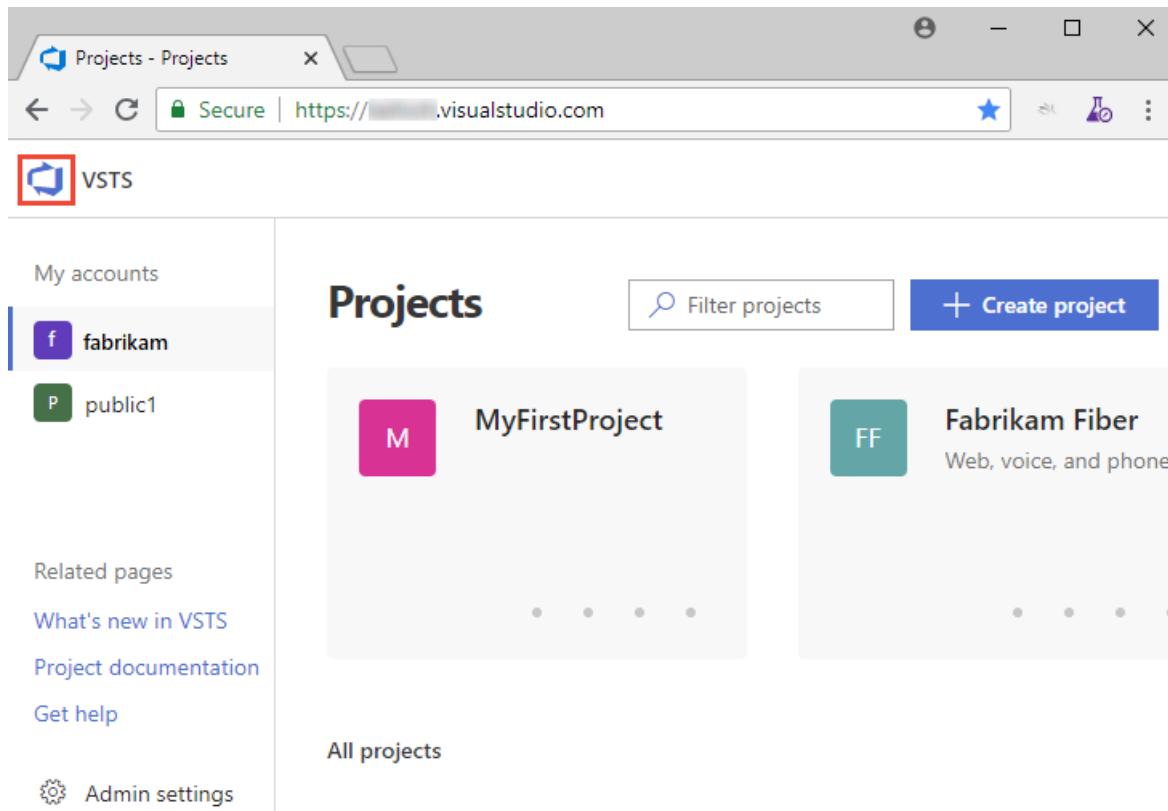
- To manage a large number of users, you can manage access through Active Directory

Both Azure DevOps Services and Azure DevOps Server are enterprise-ready platforms that support teams of any size, from tens to thousands. Azure DevOps Services, our cloud service, provides a scalable, reliable, and globally available hosted service. It is backed by a 99.9% SLA, monitored by our 24x7 operations team, and available in local data centers around the world.

How to view projects defined for your organization or collection

You can view the projects defined for your organization by opening the **Projects** page.

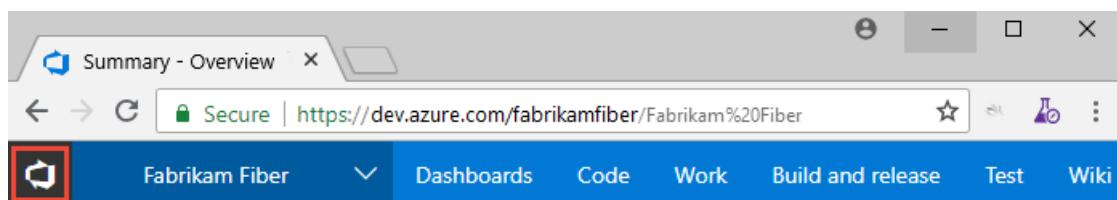
1. Choose the  Azure DevOps logo to open **Projects**.



The screenshot shows the 'Projects' page in VSTS. On the left, there's a sidebar with 'My accounts' (fabrikam) and 'Related pages' (What's new in VSTS, Project documentation, Get help, Admin settings). The main area is titled 'Projects' with a 'Filter projects' search bar and a '+ Create project' button. It lists two projects: 'MyFirstProject' (M icon) and 'Fabrikam Fiber' (FF icon). Below the projects is a link 'All projects'.

2. From there, you can choose a project from the set of projects listed.

1. Choose the  Azure DevOps logo to open **Projects**.



The screenshot shows the 'Summary - Overview' page for the 'Fabrikam Fiber' project. At the top, there's a header with the project name 'Fabrikam Fiber'. Below it is a navigation bar with tabs: Dashboards, Code, Work, Build and release, Test, and Wiki. The 'Work' tab is highlighted with a red box.

2. From there, you can choose a project from the set of projects listed.

FabrikamFiber

Search work items in this collection

Good evening, Jamal Hartnett

Projects My favorites My work items My pull requests ...

Filter projects and teams

New Project

Projects

Filter projects and teams



New Project

Recent

FabrikamFiber

FabrikamFiberTest

1. Choose the name of the server.

2. From there, you can choose a project from the set of projects listed.

When to add another project

In general, we recommend that you use a single project to support your organization or enterprise. A single project minimizes the maintenance of administrative tasks and supports the most optimized / full-flexibility [cross-link object](#) experience.

Even if you have many teams working on hundreds of different applications and software projects, you can most easily manage them within a single project. A project serves to isolate data stored within it; you can't easily move data from one project to another. When you move data from one project to another, you typically lose the history associated with that data.

Reasons to add another project

Instances where you may want to add another project include the following:

- To prohibit or manage access to the information contained within a project to select groups
- 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 prior to rolling out changes to the working project
- To support an Open Source Software (OSS) project

Instances where you may want to add another project include the following:

- To prohibit or manage access to the information contained 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 prior to rolling out changes to the working project

Private and public projects

You can add either public or private projects to your organization. You can also [change the visibility of a project from private to public](#).

Private projects require that you add and manage user access. Users must sign-in to gain access to a project, even if it is read-only access. All users added to a project gain access to information contained with the project and organization. For details, see [Resources granted to project members](#).

A public project, on the other hand, doesn't require users to sign in to gain read-only access to many of the services. Public projects provide support to share code with others and to support continuous integration/continuous deployment (CI/CD) of open source software. To learn more about public projects, see [What is a public project?](#).

Structure your project

When you add a project, look at using the following elements to structure it to support your business needs:

- [Create a Git repository](#) for each sub-project or application, or [create root folders within a TFVC repository](#) for each sub-project.
- [Define area paths](#) to support different sub-projects, products, features, or teams.
- [Define iteration paths \(aka sprints\)](#) that can be shared across teams.
- [Add a team](#) for each product team that develops a set of features for a product. Note that each team you create automatically creates a security group for that team which you can use to manage permissions for a team. See also, [Portfolio management](#).
- [Grant or restrict access to select 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.

Customizing and configuring projects

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 perform the following tasks. For a comprehensive view of what 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 their 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 details, see [Customize an inheritance process](#).
- **Build and Release:** You can fully customize your build and release pipelines, define build steps, release environments, and deployment schedule. For details, see [Build and Release](#).
- **Test:** You can define and configure test plans, test suites, and test cases as well as configure test environments; additionally you can add test steps within your build pipelines. For details, see [Exploratory & Manual Testing](#) and [continuous testing for your builds](#).
- **Dashboards:** Each team can [configure their set of dashboards](#) to share information and monitor their 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 details, see [Customize the On-premises XML process model](#).

- **Build and Release:** You can fully customize your build and release pipelines, define build steps, release environments, and deployment schedule. For details, see [Build and Release](#).
- **Test:** You can define and configure test plans, test suites, and test cases as well as configure test environments; additionally you can add test steps within your build pipelines. For details, see [Exploratory & Manual Testing](#) and [continuous testing for your builds](#).

When to add a team, scaling Agile tools across the enterprise

As your organization grows, you'll want to add teams to provide them the Agile tools that each team can configure to meet their workflow. To learn more, see the following articles.

- [Scale Agile to large teams](#)
- [About teams and Agile tools](#)
- Manage a [portfolio of backlogs](#) and gain insight into each team's progress as well as the progress of all programs.
- Use [Delivery plans](#) to review the schedule of stories or features your teams plan to deliver. Delivery plans show the 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](#).

To review stories and short videos on how Microsoft transitioned from waterfall to Agile, see [Scaling Agile Across the Enterprise](#).

Clients that support connection to a project

In addition to connecting through 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](#)
- [Eclipse: Team Explorer Everywhere](#)
- [Office Excel](#)
- [Office Project](#)
- [PowerPoint Storyboarding](#)
- [Azure Test Plans \(formerly Test Manager\)](#)
- [Microsoft Feedback Client](#)

See also, [Compatibility with Azure DevOps Server versions](#).

Related articles

- [Get started as an administrator](#)
- [Web portal navigation](#)
- [What do I get with a project?](#)
- [Understand differences between Azure DevOps](#)

What features and services do I get with Azure DevOps?

5/10/2019 • 8 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

With Azure DevOps, you gain an integrated set of services and tools to manage your software projects, from planning and development through testing and deployment. Services are delivered through a client/server model. Many of them are delivered through an easy-to-use web interface that you can access from all major browsers. Some services, such as source control, build pipelines, and work tracking, can also be managed through a client.

Access web services through the following areas, as shown in the following image.

The screenshot shows the Azure DevOps web interface. At the top, there's a header bar with a back arrow, forward arrow, refresh button, and a secure connection indicator. Below the header is a navigation bar with the 'Azure DevOps' logo and a 'FabrikamFiber' project name. The main area is a sidebar menu with the following items:

- Overview
- Summary
- Dashboards
- Wiki
- Boards
- Repos
- Pipelines
- Test Plans
- Artifacts

At the bottom of the page, there's a navigation bar with tabs for 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work', 'Build & Release', 'Test', and 'Wiki*'. The 'Dashboards' tab is currently selected. Below the navigation bar, there are two links: 'Overview' and 'Calendar', with 'Overview' being underlined to indicate it is the active page.

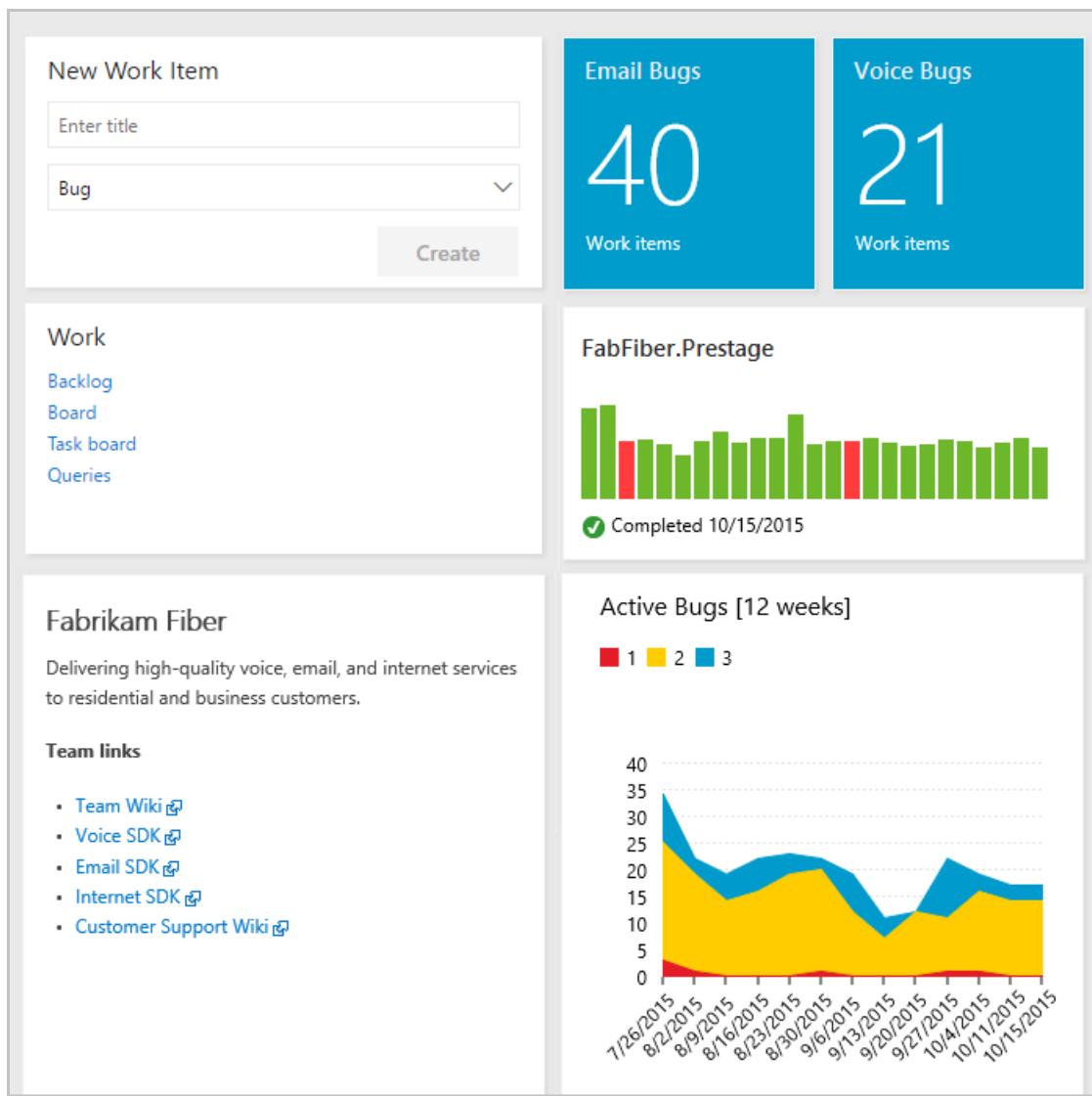
Many of our services are either free for small teams or available through a subscription model or per-use model. You can do a hybrid approach where you use an on-premises deployment to manage your code and work. Then, you purchase cloud build or testing services on an as-needed basis.

For information about client tools, see [Tools](#).

Dashboards

From **Dashboards**, you gain access to user-configurable dashboards.

The screenshot shows the 'Overview dashboard - Vis' page in a web browser. The URL is https://dev.azure.com/Fabrikam/_dashboards/_/FabrikamFiber%20Team/11c. The page title is 'Fabrikam / FabrikamFiber / Overview / Dashboards'. The left sidebar has a 'FabrikamFiber' header and links to 'Overview', 'Summary', 'Dashboards' (which is selected), 'Wiki', 'Boards', 'Repos', 'Pipelines', 'Test Plans', and 'Artifacts'. The main content area is titled 'FabrikamFiber Team Overview'. It features a 'Welcome' section with a message: 'Get started using Azure DevOps to make the most of your team dashboard.' Below it are four cards: 'Manage Work' (Add work to your board), 'Collaborate on code' (Add code to your repository), 'Continuously integrate' (Automate your builds), and 'Visualize progress' (Learn how to add charts). A 'Code Tile' section on the right is partially visible. At the bottom, there's a 'Team Members' section with icons for 'CC', a person, and a plus sign.



You can do the following tasks in **Dashboards**:

- Add, configure, and manage dashboards
- Configure widgets that you add to dashboards
- Quickly navigate to different areas of your project

To learn more, see [Dashboards](#).

Source control

Source or version control systems allow developers to collaborate on code and track changes made to the code base. Source control is an essential tool for multi-developer projects.

Our systems support two types of source control: Git (distributed) or Team Foundation Version Control (TFVC), a centralized, client-server system. Both systems enable you to check in files and organize files within folders, branches, and repositories.

With Git, each developer has a copy on their dev machine of the source repository, including all branch and history information. Each developer works directly with their own local repository and changes are shared between repositories as a separate step.

Developers commit each set of changes and do version control operations like history and compare without a network connection. Branches are lightweight. When developers need to switch contexts, they create a private local branch and can switch from one branch to another to pivot among different variations of the codebase. Later, they merge, publish, or dispose of the branch.

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.

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 created on the server.

From **Repos**, you gain access to your source control Git-based or Team Foundation Version Control (TFVC) repositories to support version control of your software projects. These repositories are private.

The screenshot shows the Azure DevOps interface for a repository named 'DotNetSample'. The left sidebar has a 'Files' section selected. The main area shows a list of files and folders in the 'master' branch:

- docs
- dotnetcore-sample
- dotnetcore-tests
- .gitignore
- .vsts-ci.acr.yml
- .vsts-ci.docker.yml
- .vsts-ci.yml
- Dockerfile
- dotnetcore-sample.sln
- LICENSE
- LICENSE-CODE
- README.md

From **Code**, you gain access to your source control Git-based or TFVC repositories to support version control of your software projects. These repositories are private.

	Contents	History	README	+ New file	Upload file(s)	
	↑ Name		Last change		Commits	
M+ page-1.md	M+ page-1.md	10/15/2015	3458a6c7	Added file page-1.md		
M+ page-2.md	M+ page-2.md	10/15/2015	01a447ca	Added file page-2.md		
M+ page-3.md	M+ page-3.md	9/21/2016	68385e28	Added file page-3.md		
M+ README.md	M+ README.md	5/19/2017	fb9177d8	Merged PR 2: Updated		

From Azure Repos for Git, you can do the following tasks:

- Review, download, and edit files, and review the change history for a file
- Review and manage commits that have been pushed
- Review, create, approve, comment on, and complete pull requests
- Add and manage Git tags

To learn more, see the overviews for [Git](#) or [TFVC](#).

Plan and track work

Software development projects require ways to easily share information and track the status of work, tasks, issues, or code defects. In the past, perhaps you used one or more tools. For example, Microsoft Excel, Microsoft Project, a bug tracking system, or a combination of tools. Now, many teams have adopted Agile methods and practices to support planning and development.

Our systems provide several types of work items that you use to track features, requirements, user stories, tasks, bugs, and issues. Each work item is associated with a work item type and a set of fields that can be updated, as progress is made.

For planning purposes, you have access to several types of backlogs and boards to support the main Agile methods—Scrum, Kanban, or Scrumban.

- Product backlog: Used to create and rank stories or requirements.
- Kanban: Used to visualize and manage the flow of work as it moves from beginning, to in-progress, to done.
- Sprint backlogs: Used to plan work to complete during a sprint cycle, a regular two to four-week cadence that teams use when implementing Scrum.
- Task board: Used during daily Scrum meetings to review work that's completed, remaining, or blocked.

Project managers and developers share information by tracking work items on the backlogs and boards. Useful charts and dashboards complete the picture and help teams monitor progress and trends.

From **Boards**, you gain access to Agile tools to support planning and tracking work.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. The left sidebar has 'Boards' selected. The main area displays the 'FabrikamFiber Team' backlog. It includes a 'New' item button, a search bar, and two items listed:

- Technician can report busy/late on Windows Phone (3)
- Technician can see service tickets on Windows Phone (0/2)

On the right, there's a sidebar for 'Active' work items with 3/5 items:

- Add an information form
- Welcome back page
- Secure sign in (Unassigned, 1)
- Add Test
- Test for secure sign in

From **Work**, you gain access to Agile tools to support planning and tracking work.

The screenshot shows the 'Backlogs' page for the 'Fabrikam Fiber' project. The left sidebar shows a hierarchy of backlog items: Epics, Features, Stories, Past Sprints (Sprint 1, Sprint 2), and Current Sprints (Sprint 3, Sprint 4, Sprint 5). The main area displays the 'Stories' backlog with the following settings:

- Forecast Off
- Parents Hide
- In progress items Show
- Mapping On

A modal window is open for adding a new story, with 'User Story' selected as the type and an empty 'Title' field. Below the modal, the backlog table shows five stories:

Order	State	Story Points	Title
1	New	5	Add an information form
2	New	3	Welcome back page
3	New	8	Interim save on long forms
4	Active	5	Secure Sign-in
5	Active	5	Canadian addresses don't display

Specifically, you can do the following tasks:

- Add and update work items
- Define work item queries, and create status and trend charts based on those queries

- Manage your product backlog
- Plan sprints by using sprint backlogs
- Review sprint tasks and update tasks through the task boards
- Visualize the workflow and update the status by using Kanban boards
- Manage portfolios by grouping stories under features and grouping features under epics

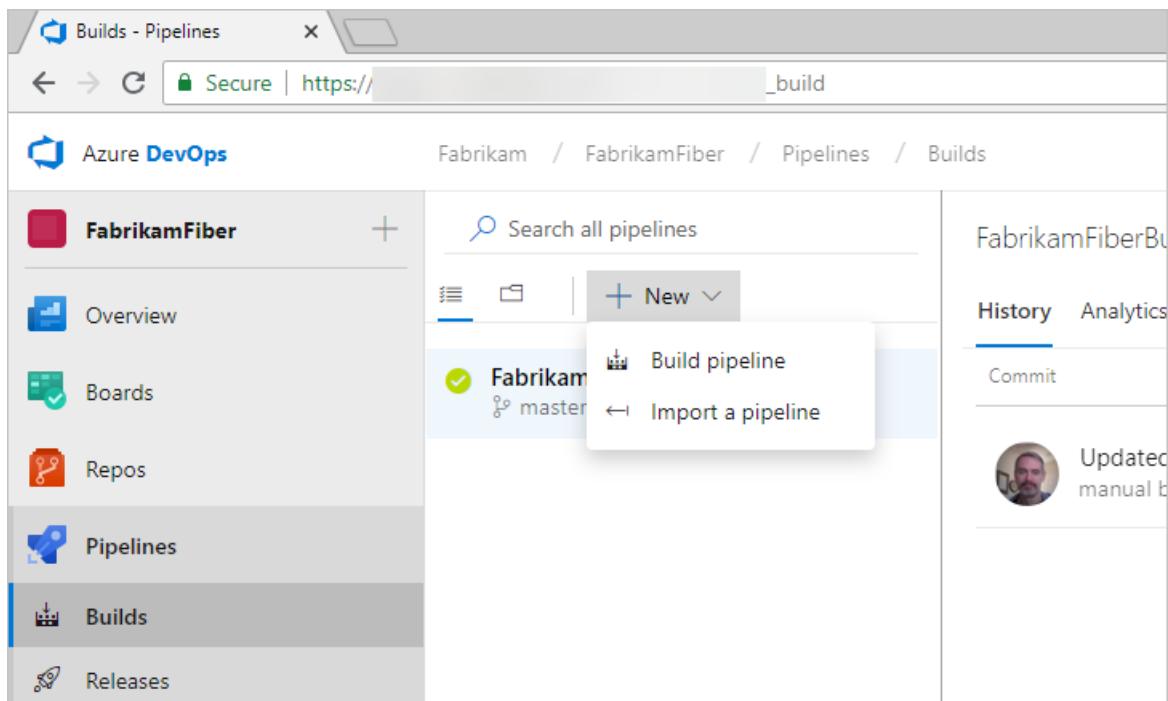
See [Backlogs, boards, and plans](#) for an overview of each.

Continuous integration and deployment

The rapid and reliable release of software comes from automating as many processes as possible. Our systems support build, test, and release automation.

- You can define builds to automatically run whenever a team member checks in code changes.
- Your build pipelines can include instructions to run tests after the build runs.
- Release pipelines support managing deployment of your software builds to staging or production environments.

Azure Pipelines provides an integrated set of features to support building and deploying your applications.



Azure Pipelines provides an integrated set of features to support building and deploying your applications.

The screenshot shows the Microsoft DevOps interface for 'Fabrikam Fiber'. The top navigation bar includes 'Builds', 'Releases', 'Library', 'Task Groups', 'Deployment Groups*', 'Dashboards', 'Code', 'Work', 'Build & Release', 'Test', and a '...' button. Below the navigation is a search bar labeled 'Build ID or build number' with a magnifying glass icon, and buttons for '+ New' and '+ Import'. A filter bar at the top allows switching between 'Mine', 'All Definitions', 'Queued', and 'XAML'. The main area displays a table of build definitions:

		Status	Triggered by	7-day pass rate
	Content.VS Build : #Content.VS Build_20160609.1 requested a year ago	★ ✓ passing	Updated the overview s... ↳ 80496e4 in ↳ 80 users/...	0% →
	Content.VS.PR : #Content.VS.PR_20161019.14 requested 10 months ago	★ ✓ passing	Merge pull request 152... ↳ 2be71b1 in ↳ 152638	0% →
	MSDN.GatedCheck.ALM-master : #20170313.2 requested 5 months ago	★ ✓ passing	Merge pull request 194... ↳ 8f7955d in ↳ 194899	0% →
	MSDN.GatedCheck.VS-master : #20160725.1 requested a year ago	★ ✓ passing	Merge pull request 126... ↳ 2d56c79 in ↳ 126293	0% →

Use pipelines to implement continuous integration and continuous delivery.

- **Build automation:** Define the steps to take during build and the triggers that start a build.
- **Release management:** Supports a rapid release cadence and management of simultaneous releases. You can configure release pipelines that represent your environments from development to production. Run automation to deploy your app to each environment. Add approvers to confirm that the app has been successfully deployed in an environment. Create your release manually or automatically from a build. Then track your releases as they're deployed to various environments.

To learn more, see [Continuous integration on any platform](#).

Manual and exploratory testing

Test features support manual and exploratory testing, and continuous testing.

Test Plans supports creating and managing manual tests.

The screenshot shows the Microsoft Test Plans interface for 'FabrikamFiber'. The left sidebar shows a tree view with 'Test Plans' expanded, 'FabrikamFiber' selected, and 'FabrikamFiber (2)' under it. There is also a 'New suite' option. The main area displays a 'Test suite: FabrikamFiber (Suite ID: 367)' with a 'Tests' tab selected. The table below lists the tests:

Outcome	Order	ID	Title
Active	1	368	Fabrikam Test
Active	2	369	Test sign in flow

Test supports creating and managing manual tests.

The screenshot shows the Microsoft DevOps Test Plans interface. At the top, there's a navigation bar with links for 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work', 'Build & Release', 'Test', 'Wiki*', and a gear icon. Below the navigation bar, there's a sub-navigation menu with 'Test Plans' selected, along with other options like 'Parameters', 'Configurations', 'Runs', 'Machines', and 'Load test'. A dropdown menu shows 'Fabrikam Fiber: Fabrikam Fiber Team_Sto...'. On the left, there's a toolbar with icons for creating new items and a sidebar showing a tree structure for 'Fabrikam Fiber Team_Stories_Fabrikam Fiber' with a node '379 : Phone sign in (2)'. The main area displays a grid titled 'Test suite: 379 : Phone sign in (Suite ID: 477)'. The grid has columns for 'Tests', 'Charts', 'Outcome All', 'Tester All', and 'Configuration All'. It lists two active tests: one for Windows 8 with ID 474 and another for Windows 8 with ID 478.

With test features, you gain access to the following features:

- Customization of workflows with test plan, test suite, and test case work items
- End-to-end traceability from requirements to test cases and bugs with requirement-based test suites
- Criteria-based test selection with query-based test suites
- Excel-like interface with the grid for easy creation of test cases
- Reusable test steps and test data with shared steps and shared parameters
- Sharable test plans, test suites, and test cases for reviewing with Stakeholders
- Browser-based test execution on any platform
- Real-time charts for tracking test activity

To learn more, see [Testing overview](#).

Collaboration services

The following services work across the previously mentioned services to support:

- Team dashboards
- Project wiki
- Discussion within work item forms
- Linking of work items, commits, pull requests, and other artifacts to support traceability
- Alerts and change notifications managed per user, team, project, or organization
- Ability to request and manage feedback
- Analytics service, analytic views, and Power BI reporting
- Dashboards
- Project wiki
- Discussion within work item forms
- Linking of work items, commits, pull requests, and other artifacts to support traceability
- Alerts and change notifications managed per user, team, project, or project collection
- Ability to request and manage feedback
- SQL Server Reporting
- Dashboards
- Discussion within work item forms
- Linking of work items, commits, pull requests and other artifacts to support traceability
- Alerts and change notifications managed per user, team, project, or project collection
- Ability to request and manage feedback

- Team (chat) rooms
- SQL Server Reporting

NOTE

Team rooms are deprecated for TFS 2017.2. Instead, we recommend that you [use service hooks to integrate with Microsoft Teams](#).

- Dashboards
- Linking of work items, commits, pull requests, and other artifacts to support traceability
- Alerts and change notifications managed per user or for teams
- Ability to request and manage feedback
- Team (chat) rooms
- SQL Server Reporting
- Team home page
- Linking of work items, commits, pull requests, and other artifacts to support traceability
- Alerts and change notifications managed per user or for teams
- Ability to request and manage feedback
- Team (chat) rooms
- SQL Server Reporting

Service hooks

Service hooks enable you to complete tasks on other services when events happen within your project hosted on Azure DevOps. For example, you can send a push notification to your team's mobile devices when a build fails. You can also use service hooks in custom apps and services as a more efficient way to drive activities in your projects.

The following services are available as the target of service hooks. To learn about other apps and services that integrate with Azure DevOps, visit the [Visual Studio Marketplace](#), Azure DevOps tab.

For the latest set of supported services, see [Integrate with service hooks](#).

Cloud-hosted services based on usage

The following services support your DevOps operations:

- Cloud-based, Microsoft-hosted build and deployment agents
- On-premises self-hosted agents to support build and deployment

To learn more, see [Pricing](#).

Azure cloud-hosted services

Azure provides cloud-hosted services to support application development and deployment. You can make use of these services solely or in combination with Azure DevOps.

To browse the directory of integrated services, features, and bundled suites, see [Azure products](#).

For continuous delivery to Azure from Azure DevOps Services, see [Automatically build and deploy to Azure web apps or cloud services](#).

Administrative services

There are features and tasks associated with administering a collaborative software development environment. You complete most of these tasks through the web portal. To learn more, see [About user, team, project, and organization-level settings](#).

The screenshot shows the 'Project Settings > Overview' page for the 'FabrikamFiberTest' project in Azure DevOps. The left sidebar lists project management areas: Overview, Boards, Repos, Pipelines, Test Plans, and Artifacts. The 'Project settings' option at the bottom is highlighted with a red box. The main content area displays 'Project details' with fields for Name (FabrikamFiberTest), Description (Fabrikam Fiber test project), Process (Scrum), and Visibility (Private). A 'Save' button is present. Below this, the 'Azure DevOps services' section lists Boards, Repos, Pipelines, and Packages, each with a brief description and icon.

Project Settings > Overview

Project details

Name
FabrikamFiberTest

Description
Fabrikam Fiber test project

Process
Scrum

Visibility
Private

Save

Azure DevOps services

- Boards**
Flexible agile planning v
- Repos**
Repos, pull requests, ad
- Pipelines**
Build, manage, and scale
- Packages**

Screenshot of the Azure DevOps Services interface showing the 'Fabrikam Fiber' project profile and team management.

The top navigation bar includes links for Dashboards, Code, Work, Build & Release, Test, Wiki*, and a gear icon for settings.

The left sidebar shows the project profile with details:

- Name: Fabrikam Fiber
- Process: Scrum
- Description: Web, voice, and phone apps

The main content area is titled "Teams" and displays a list of teams:

Team Name ↑	Members	Description
Customer Service	7	
Fabrikam Fiber Team	7	The default project team.
Management team	1	
Phone	1	
Voice	1	
Web	2	

A "New team" button and a refresh icon are located at the top of the teams list.

Related articles

- [Understand differences between Azure DevOps Services and Azure DevOps Server](#)
- [Client-server tools](#)
- [Software development roles](#)
- [Azure DevOps pricing](#)
- [Azure DevOps data protection overview](#)

Quickstart: Share your project vision, view project activity

6/25/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

In this quickstart, you learn how to share your project with your team, add project members, and check the latest project activity. Share your project and objective, and ways for team members to contribute to the project through a project README file or through a project wiki.

If you want to use a project wiki, then first [create a Wiki for your project](#). You can then [change the project summary page to point to the wiki](#).

From the project home page, share your project with your team, add project members, and check the latest project activity. Share your project and objective, and ways for team members to contribute to the project through a project README file.

NOTE

The features and functions available from your project page depend on the source control, Git, or Team Foundation Version Control (TFVC) that you selected when you [created your team project](#).

Prerequisites

- You must be a member of the [Project Administrators group](#) or have your **Edit project-level information** permission set to **Allow** to do the following:
 - Edit information on the project page
 - Change the repository that you use to share your project mission
 - Manage project membership
- To edit a page, you must be a contributor to the repository or branch or have the **Contribute** permissions set to **Allow**.
- To view the project page, you must be a valid member of the project. For more information, see [Permissions and groups](#), [Valid user groups](#).

Open project summary

From your web browser, choose **Overview > Summary**. If you don't have a project yet, [create a project](#).

If you haven't set up your project summary yet, you'll see this welcome page:

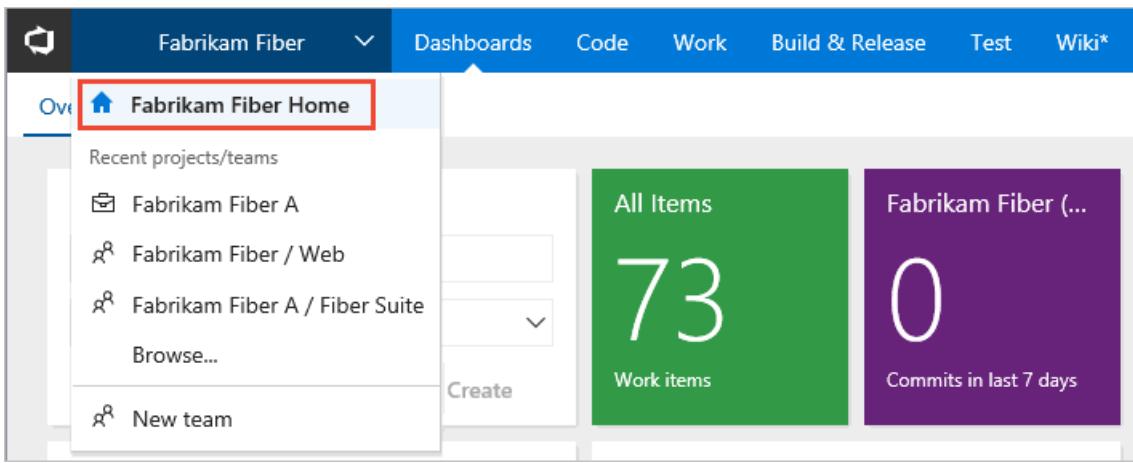
The screenshot shows the Azure DevOps interface for the 'Fabrikam Test' project. At the top, there's a navigation bar with icons for file operations, a back arrow, forward arrow, refresh, and home. The title 'Summary - Overview' is displayed, along with a '+' and a dropdown arrow. Below the title is a secure connection indicator and the URL 'https://dev.azure.com/fabrikam/Fabrikam%20Test'. On the left, a sidebar menu lists 'Fabrikam Test' (with a green 'FT' icon), 'Overview' (selected), 'Summary' (selected), 'Dashboards', 'Wiki', 'Boards', 'Repos', 'Pipelines', 'Test Plans', and 'Artifacts'. A 'Project settings' link is at the bottom of the sidebar. The main content area features a large 'Fabrikam Test' header with a green 'FT' icon, a 'Private' button, and an 'Invite' button. Below the header is a cartoon illustration of a person sitting at a desk with a laptop, and a dog standing nearby. The text 'Welcome to the project!' is prominently displayed. Underneath, it says 'What service would you like to start with?' followed by buttons for 'Boards', 'Repos', 'Pipelines', 'Test Plans', and 'Artifacts'. At the bottom, there's a link to 'or manage your services'.

Select one of the following tasks to get started:

- **Invite** to begin [adding others to your project](#). Note, you can only invite users who have already been [added to your organization](#).
- **Boards** to begin [adding work items](#).
- **Repos** to open [Repos > Files](#) page where you can clone or import a repository, or [initialize a README file](#) for your project summary page.
- **Pipelines** to start [defining a pipeline](#).
- **Test Plans** to start [defining test plans and test suites](#).
- [Manage your services](#) to disable the visibility of one or more services.

To support your project mission, choose a README file that you maintain in a project repository, or the [project Wiki](#). To choose between a README file or a Wiki, see [Change the repository](#). To define a README file for your project, see [Initialize a README file for your Git repo](#) or [Initialize a README file for your TFVC repo](#).

From your web browser, open the team project drop down menu and select the home page. If you don't have a project, [create a team project](#).



To define a README file for your project, see [Initialize a README file for your Git repo](#) or [Initialize a README file for your TFVC repo](#).

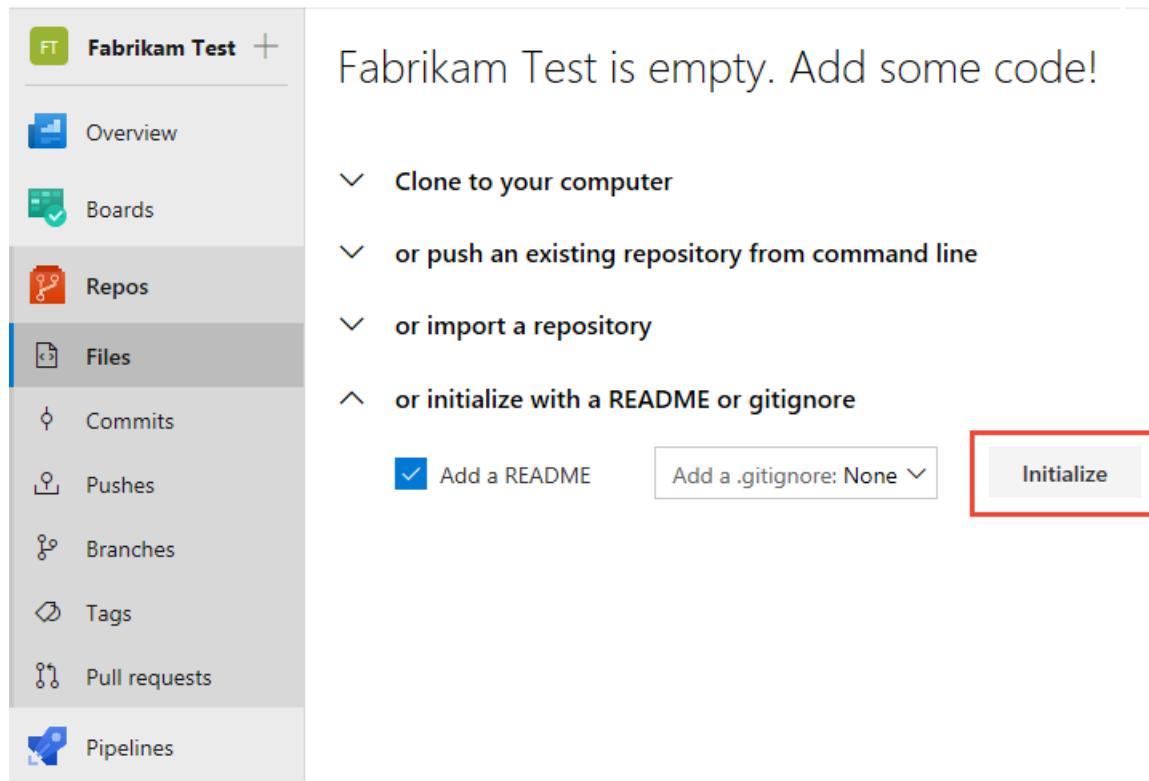
NOTE

The project page described in this section is available for TFS 2017.1 and later versions. It replaces the Welcome page used in TFS 2015 and TFS 2017.

Initialize a README file for a Git repo

You can share your project and objective, as well as ways for team members to contribute to the project through a project README file. For Git projects, the README.md file needs to be at the root of each repository in the default branch. For Git based projects the left pane supports navigation to other repositories. A separate Welcome page/README.md file can be created for each repository.

1. Open **Repos>Files**. This page guides you to get started quickly by adding code to your repository when you choose one of the options to clone, push, import, or initialize a repo.
2. With the **Add a README** check box checked, choose **Initialize**.



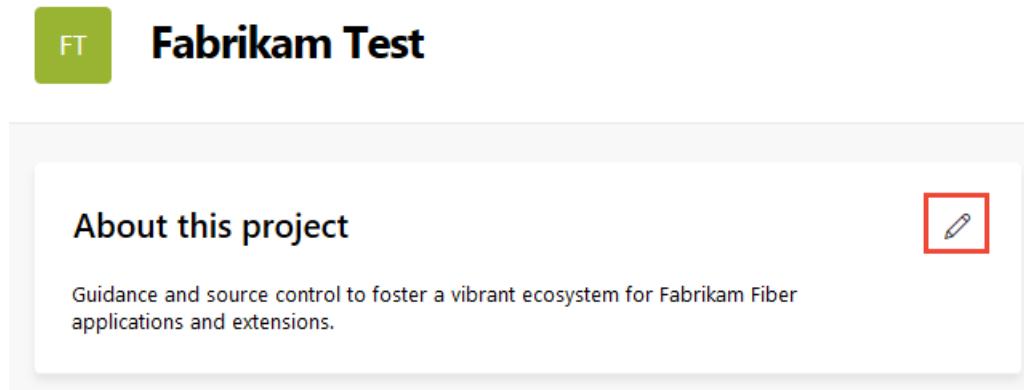
Fabrikam Test is empty. Add some code!

- ▽ Clone to your computer
- ▽ or push an existing repository from command line
- ▽ or import a repository
- △ or initialize with a README or .gitignore

Add a README Add a .gitignore: None ▾ **Initialize**

A default README file is added to the project repository, in this case, the **Fabrikam Test** repo.

3. Return to **Overview>Summary** and choose the README file for the project page. Choose the  edit icon.



Fabrikam Test

About this project

Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

4. Select the project repository where you initialized the README file.

About this project

Description

Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

Tags

Add tags

About

Readme file Wiki

❖ Select a repository

❖ Fabrikam Test

Cancel

Save

5. To edit the README file, choose the README file link.

About this project



Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

❖ [Fabrikam Test / README.md](#)

Introduction

TODO: Give a short introduction of your project. Let this section explain the objectives or the motivation behind this project.

You're directed to the **Repos > Files** page for the README file. You can edit and modify the README Markdown file like you would any other file in a Git repository. You can use Markdown language to format the README file and add images. To learn more about adding a README file, see [Create a README for your repo](#) and [Markdown guidance](#).

1. Open the Project home page.
2. With the **Add a README** check box checked, choose **Initialize**.

FF

Fabrikam Fiber ☆

Briefly describe your project...

Add tags

Get started with your new project!

- ▽ Clone to your computer
- ▽ or push an existing repository from command line
- ▽ or import a repository
- △ or initialize with a README or gitignore



Add a README

Add a .gitignore: None ▾

Initialize

- ▽ or build code from an external repository

A default README file is added to the project repository, in this case, the **Fabrikam Test** repo.

3. To edit the project README.md file, choose **Edit**.

FF

Fabrikam Fiber ☆

Private

Briefly describe your project...

Add tags



Use continuous integration

Improve code quality by detecting breaking changes as soon as they happen.

[Set up a pipeline](#)

[Learn more about continuous integration](#)

Fabrikam Test / README.md

Edit

Change

Introduction

TODO: Give a short introduction of your project. Let this section explain the objectives or the motivation behind this project.

Getting Started

TODO: Guide users through getting your code up and running on their own system. In this section you can talk about:

Use Markdown language to format the README file and add images. To learn more about adding a README file, see [Create a README for your repo](#) and [Markdown guidance](#).

1. You can start editing directly from the Welcome page.

The screenshot shows a GitHub repository page for 'Fabrikam Fiber'. The repository has a teal icon with 'FF' and a yellow star. It's described as 'Web, voice, and phone apps'. A 'Private' lock icon is present. Below the repository name, there's a 'Add tags' button. The README.md file is displayed with the following content:

```
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 can do.
Learn more [about Markdown](#).

[page 1](#)
[page 2](#)
[page 3](#) - verifying this works as advertised

`{{{MONOSPACE}}} text here?`

code block

The 'Edit' button is highlighted with a red box.

NOTE

If you set policies on the Git repository, changes to the welcome page must be done as a pull request.

2. To add another page, enter a link to a new Markdown file that doesn't yet exist, for example:

```
[page-1](./page-1.md)
```

3. After you save the file, select the link. Respond to the prompt to edit the file and commit it to your repository.

Initialize a README file for a TFVC repo

For projects that selected TFVC for version control, the README.md file needs to be at the root of your team project folder (i.e. \$/TeamProject/README.md).

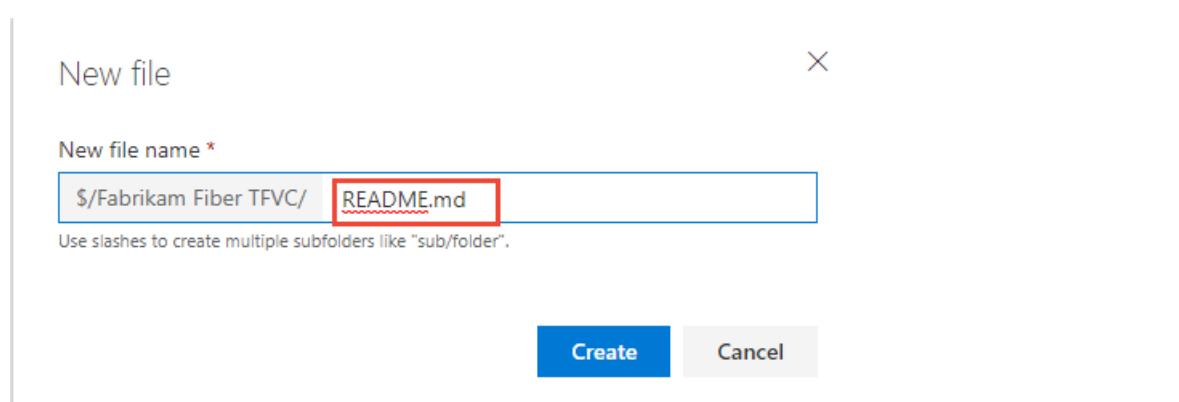
1. Open **Repos>Files**.
2. Select **Add Project Description**.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber TFVC' project. The left sidebar has a dark grey header with the project name 'Fabrikam Fiber TFVC' and a '+' icon. Below it are several items: 'Overview' (blue icon), 'Summary' (selected, grey icon), 'Dashboards' (grey icon), 'Wiki' (grey icon), 'Boards' (green icon), 'Repos' (orange icon), 'Pipelines' (blue icon), and 'Test Plans' (purple icon). The main content area has a purple header with the letters 'FT'. Below it is the title 'Fabrikam Fiber TFVC'. A large box contains the heading 'About this project' and a sub-section 'Help others to get on board!'. It includes a placeholder text 'Describe your project and make it easier for other people to understand it.' and a red-bordered button '+ Add Project Description'. To the right of the text is a cartoon illustration of a man in a suit running on clouds.

3. Select the TFVC repository and choose **Save**. If no README file has been created yet in the repo, you'll see the following message.

The screenshot shows the 'About this project' edit screen. At the top right is a close button 'X'. Below it is a heading 'About this project'. Under 'Description', there is a text box containing 'Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.' with a green circular 'G' icon. In the 'Tags' section, there is a button 'Add tags'. Under 'About', there are two radio buttons: 'Readme file' (selected) and 'Wiki'. Below them is a dropdown menu showing '\$/Fabrikam Fiber TFVC'. A pink message box at the bottom says 'We couldn't find Readme.md' and 'Seems like the file has not been created or was deleted.' At the bottom right are 'Cancel' and 'Save' buttons.

4. To create a README file, choose **Repos>Files** and choose new file to add a file to the project repository.
5. Name the file as **README.md**.



6. Add the contents of your README file in Markdown format, and then choose **Check in....**

```
1 # Requirements integrating for Fabrikam Fiber apps
2
3 Support users to import, map and analyze requirements Fabrikam apps
4
5 ### Features
6 - Import requirements
7 - Manage requirement
8 - Requirement visualization (visual traceability)
9 - Export requirement information
10
11
12 ### Extensibility API Features Used
13 - Extension Data Service
14 - MessageArea Control
15 - Grid Control
16 - Core HttpClient
17
18
```

7. Select **Check in** to complete the check in process of the README file.

Comment

Added file README.md

Work items to link

Search work items by ID or title

Check in Cancel

8. Select **Overview>Summary** to review your project summary page with the README file displayed.

FT

Fabrikam Fiber TFVC

About this project

Like 0



Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

[\\$/Fabrikam Fiber TFVC / README.md](#)

Requirements integrating for Fabrikam Fiber apps

Support users to import, map and analyze requirements Fabrikam apps

Features

- Import requirements
- Manage requirement
- Requirement visualization (visual traceability)
- Export requirement information

Extensibility API Features Used

- Extension Data Service
- MessageArea Control
- Grid Control
- Core HttpClient

1. Open the Project home page.

2. Select **Create README**.



Fabrikam Fiber TFVC

Briefly describe your project...

Add tags

No README.md found in  [\\$/Fabrikam Fiber TFVC](#) 



Add a README

Help others learn about your project

[Create README](#)

[Learn more about README files and what to include](#)

A default README file is added to the project repository, in this case, the **Fabrikam Fiber TFVC** repo.

3. You can immediately edit the README file. When you're done, select **Check in**.

Add tags

Contents Preview Highlight changes **Check in** Discard

1 # Introduction
2 The Fabrikam Fiber TFVC project is used to collaborate on major code features.
3

Any additional Markdown files you have (ones with a *.md extension) in the root of the project folder also appear in the left pane for easy navigation between them so you can provide additional information.

View project activity, add project members

In addition to sharing information, the project summary page pulls data from the applications to give visitors a bird's-eye view of your project activity.

To add users to the project, choose the  **add** button. You can only add users to a project that you have already added to the organization. To learn more, see [Add users to a team project or team](#).

Project stats Last 7 days

Boards

467 Work items created 410 Work items completed

Repos

109 Pull requests opened 1183 Commits by 31 authors

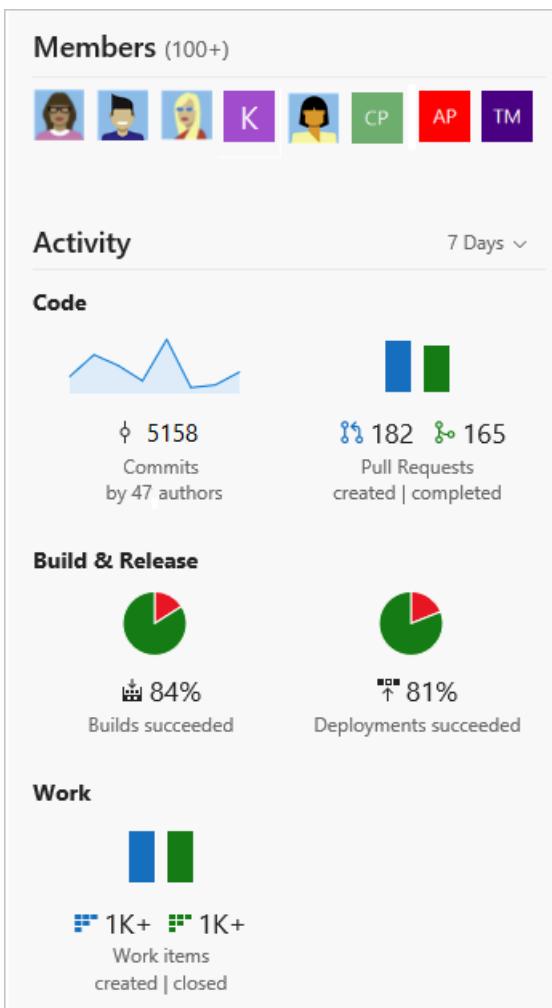
Pipelines

100% Builds succeeded 0% Deployments succeeded

Members 8

K CP

To add users to the project, choose the **add** button. To learn more, see [Add users to a team project or team](#).



Change the repository

You can change the repository used to support your project vision, including pointing it to the home page of your [built-in Wiki](#).

1. Open **Overview > Summary**.
2. Choose the edit icon.

FT Fabrikam Test

About this project

Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

If you don't see the **Edit** icon, then you're not a member of the Project Administrators group. [Get added as an admin](#) to proceed.

3. Select a different repository or choose the Wiki option.

About this project

Description

Public project for sharing code and collaborating on my project

Tags

Add tags

About

Readme file Wiki

 \$/Fabrikam Fiber TFVC

 \$/Fabrikam Fiber TFVC

 Fabrikam Fiber

 Test 1-2-3

 Testing 1 2 3

The Fabrikam Fiber TFVC project is used to collaborate on major code features.

Cancel

Save

TIP

If you choose the Wiki option, only the Wiki home page displays. To access additional Wiki pages, you must navigate to the Wiki.

- From your project home page, choose **Change**.

FF Fabrikam Fiber 

Private

Guidance and source control to foster a vibrant ecosystem for Fabrikam Fiber applications and extensions.

Add tags

 Fabrikam Fiber / README.md  

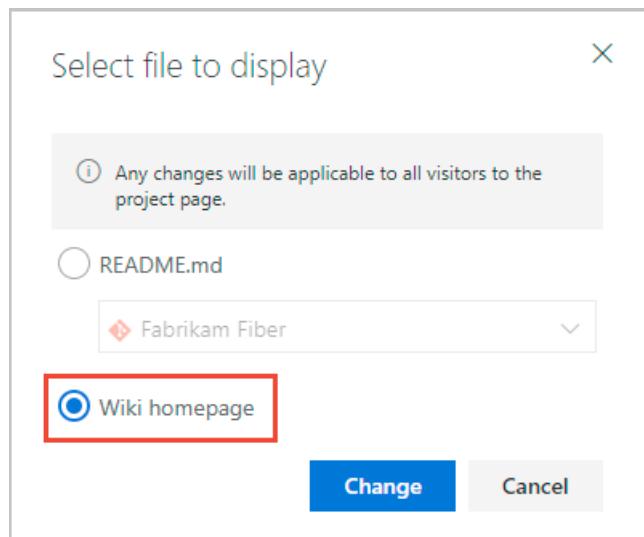
minor modification to test development section in mobile form

Update this README.md file.

A README.md file is intended to quickly orient readers to what your project can do.
[Learn more](#)  about Markdown.

If you don't see **Change** link, then you're not a member of the Project Administrators group. [Get added as an admin](#) to proceed.

2. From the select file dialog, choose an existing repo from the drop-down menu, or choose the Wiki option, shown as follows.



TIP

Only the Wiki home page displays. To access additional Wiki pages, you must navigate to the Wiki.

Next steps

[Create a wiki for your team project](#)

Install and configure the Azure Boards app for GitHub

7/9/2019 • 5 minutes to read • [Edit Online](#)

Azure Boards

By installing the Azure Boards app for GitHub, you can configure and manage the connections of your Azure Boards projects (hosted service only) with your GitHub.com repositories. By connecting your Azure Boards projects with GitHub.com repositories, you support linking between GitHub commits and pull requests to work items. You can use GitHub for software development while using Azure Boards to plan and track your work.

While the steps to make the GitHub-Azure Boards connection are different depending on your starting point, the end result is the same. You can [connect from Azure Boards](#) or use the instructions provided in this article to connect from GitHub.

This article walks you through the following 5 minute installation and configure process:

- **Install and configure**

- Choose the GitHub.com repositories you want to connect
- Choose the Azure DevOps Services organization and Azure Boards project you want to connect
- Authorize connection to Azure Boards
- Confirm the repositories you want to connect

- (Optional) **Get started**

- In Azure Boards, create a work item for adding a badge to your GitHub.com repo README file
- In GitHub.com, add the badge syntax to a repo README file, commit the change, and create a pull request for the commit
- In Azure Boards, add links to the GitHub commit and pull request to the work item; choose the GitHub pull request link to open the pull request in GitHub.com
- In GitHub.com, complete the pull request and view the badge added to your GitHub repo

You can learn more about the Azure Boards app from the [GitHub Marketplace](#), and Azure Boards from [Azure DevOps Services>Azure Boards](#).

Prerequisites

- You must be an administrator or owner of the GitHub repository you'll be connecting to.
- To install the Azure Boards app, you must be an administrator or owner of the GitHub repository or GitHub organization.
- To connect to the Azure Boards project, you must have read permission to the GitHub repository.

IMPORTANT

If your repository is already connected via another authentication type such as OAuth, you'll need to remove that repository from your existing connection before re-connecting it via the GitHub App. Follow the steps in the [remove repositories](#) section before starting the GitHub App configuration.

You can connect an Azure DevOps organization to multiple GitHub repositories so long as you are an administrator for those repositories. However, you can't connect a GitHub repository to more than one Azure Boards project. To understand why, review [Troubleshoot GitHub & Azure Boards connection](#), [Unexpected results when linking to projects defined in two or more Azure DevOps organizations](#).

Install and configure the Azure Boards app

1. Go to the Azure Boards app in the GitHub Marketplace.

[Azure Boards app](#)

2. Choose **Set up a plan**.

The screenshot shows the Azure Boards application page in the GitHub Marketplace. At the top, there's a dark header with the GitHub logo, a search bar, and navigation links for Pull requests, Issues, Marketplace, and Explore. Below the header, the URL 'Marketplace / Apps / Azure Boards' is visible. The main content area has a large circular icon containing a Kanban board with a checkmark. The text 'Application' is above the title 'Azure Boards'. A prominent green button labeled 'Set up a plan' is centered. Below the button, the text 'Plan, track, and discuss work across your teams' is followed by a description: 'Azure Boards offers Kanban boards, backlogs, and team dashboards for flexible work tracking that is fully connected to the code for all your projects – big and small.' Categories listed are Project management and Free.

3. Choose the GitHub organization you want to connect to Azure Boards.

The screenshot shows the 'Install Azure Boards' step in the GitHub Marketplace. It features a large circular icon with a Kanban board and a checkmark. The text 'Install Azure Boards' is centered, followed by the question 'Where do you want to install Azure Boards?'. A dropdown menu lists two GitHub organizations: 'JamalHart' and 'Fabrikam-Test'. Both items have a blue square icon with white letters (blue for JamalHart, teal for Fabrikam-Test) and a right-pointing arrow indicating they can be selected.

4. Choose the repositories you want to connect to Azure Boards.

Here we choose to connect to all repositories.

Install Azure Boards

Install on your personal account JamalHart



All repositories

This applies to all current *and* future repositories.

Only select repositories Select at least one repository

Select repositories ▾

...with these permissions:

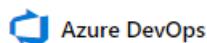
- Write access to code
- Read access to metadata
- Read and write access to commit statuses, content references, deployments, issues, pull requests, and repository projects
- Write access to attach content to the following external domains:
 - dev.azure.com
 - visualstudio.com

Install

[Cancel](#)

Next: you'll be directed to the GitHub App's site to complete setup.

5. Choose the Azure DevOps organization and Azure Boards project you want to connect to GitHub.com.



Setup your Azure Boards project

Select your Azure DevOps organization *

fabrikam



[Create a new organization](#)

Select a project *

Fabrikam Fiber



[Create a new project](#)

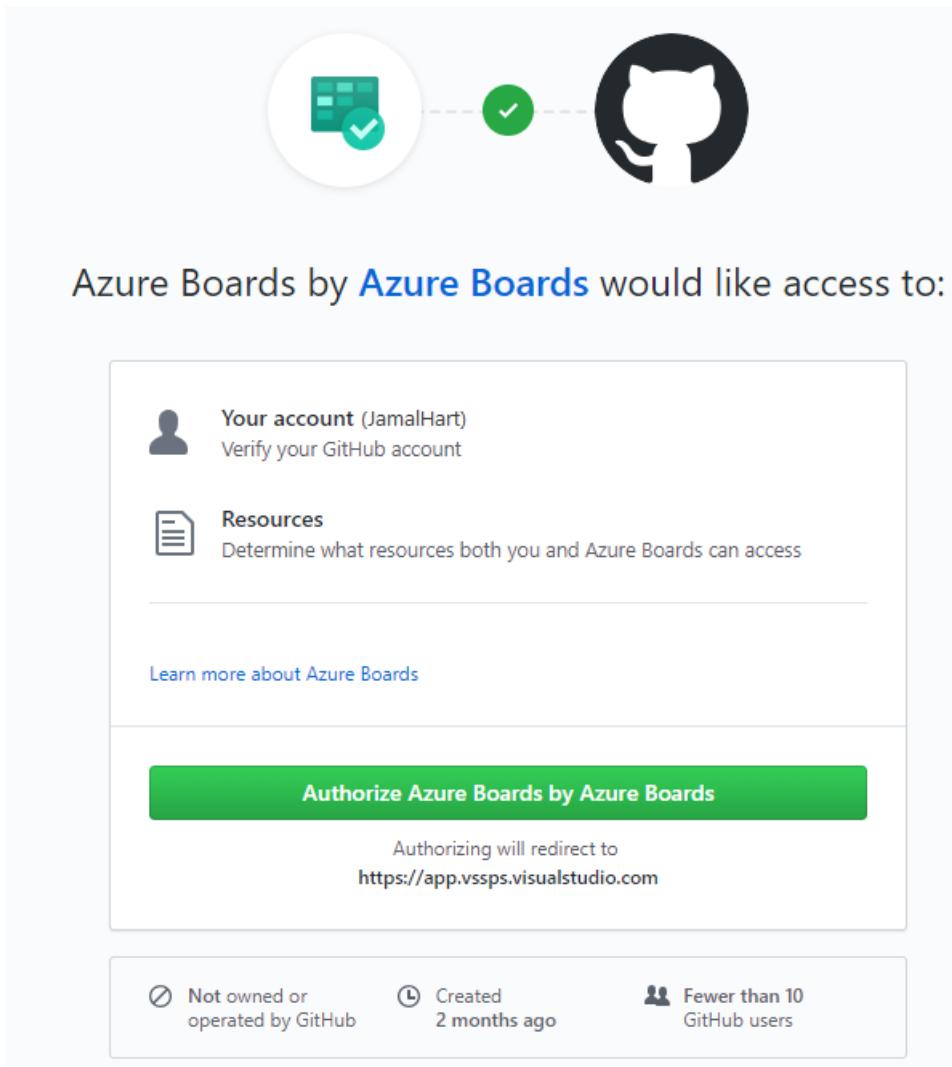
Choosing **Continue** means that you agree to our [Terms of Service](#), [Privacy Statement](#), and [Code of Conduct](#).

Continue

You can only connect one project at a time. If you have other projects you want to connect, you can do that

later as described in [Configure additional projects or repositories](#) later in this article.

6. Authorize your Azure Boards organization to connect with GitHub.com.



7. Confirm the GitHub.com repositories that you want to connect. Select each repository you want to connect to. Unselect any repositories that you don't want to participate in the integration.

Confirm your GitHub repositories



Confirm the GitHub repositories you want to use with this Azure Boards project to [finish the configuration](#). [Learn more](#)

Filter by keywords ×

Viewing 4, 4 selected

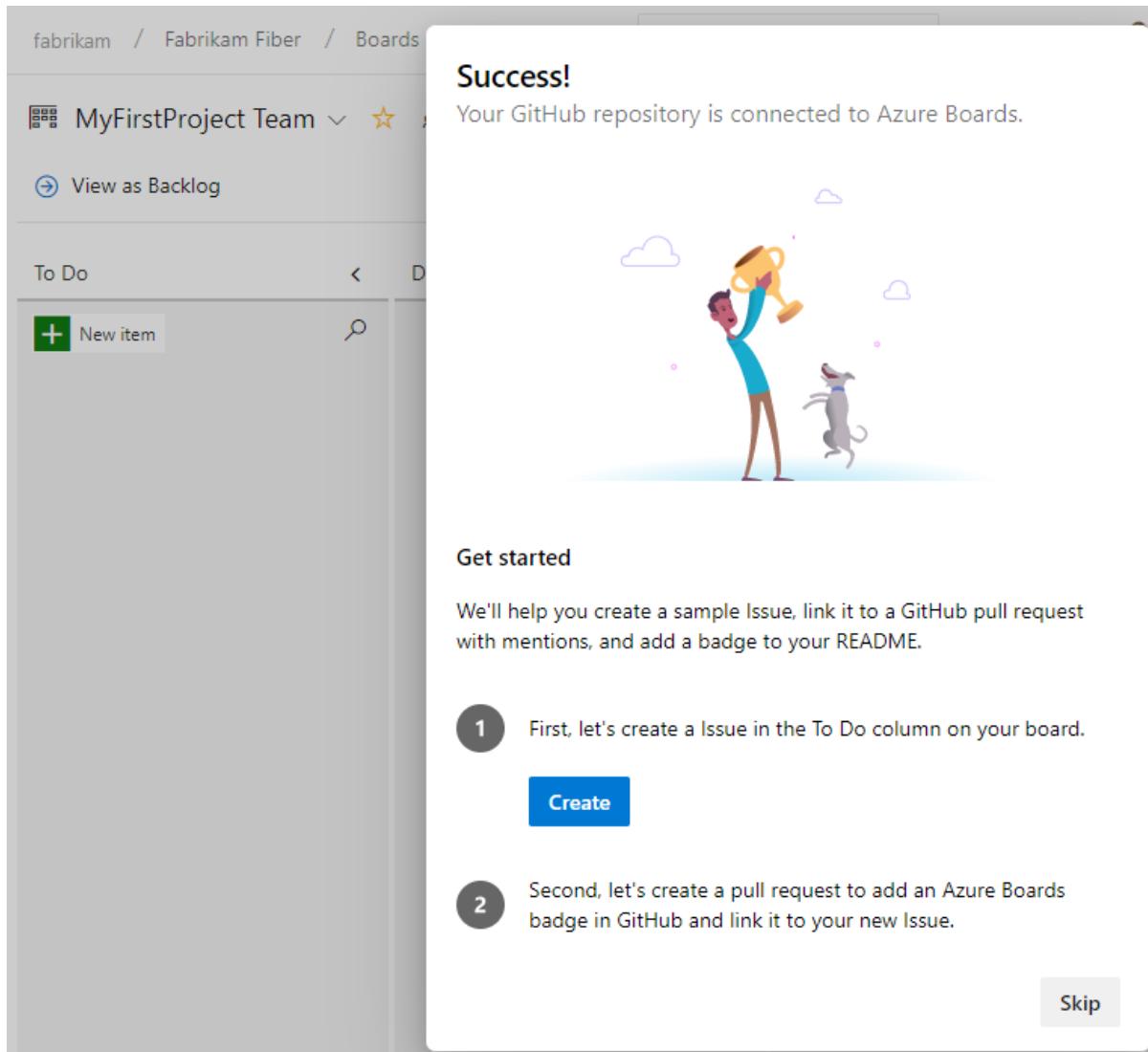
<input checked="" type="checkbox"/>	JamalHart/fabrikam-apps-2
<input checked="" type="checkbox"/>	JamalHart/fabrikam-demo
<input checked="" type="checkbox"/>	JamalHart/fabrikam-open-source
<input checked="" type="checkbox"/>	JamalHart/fabrikam-suite

Cancel Save

Get started with the connection

At this point, your Azure Boards + GitHub connection is complete. You can skip the next steps or run through them to understand the features supported with the connection.

1. Choose **Create** to add a work item—Issue (Basic), User Story (Agile), or Product Backlog Item (Scrum)—depending on the process model used by your Azure Boards project.



A work item titled *Add badge to README* appears on your Azure Boards.

2. Next, choose **Create and link a pull request**.

The screenshot shows the Azure Boards interface. On the left, there's a sidebar for 'MyFirstProject Team' under 'fabrikam / Fabrikam Fiber / Boards'. A 'To Do' column is visible with one item: '1 Add badge to README'. The main area displays a success message: 'Success! Your GitHub repository is connected to Azure Boards.' Below this is a cartoon illustration of a person holding a trophy and a dog jumping. A 'Get started' section provides instructions: 'We'll help you create a sample Issue, link it to a GitHub pull request with mentions, and add a badge to your README.' It includes two steps: 'Issue created and in the To Do column.' (step 1) and 'Second, let's create a pull request to add an Azure Boards badge in GitHub and link it to your new issue.' (step 2). A blue button labeled 'Create and link a pull request' is present. A 'Skip' button is located at the bottom right.

This step performs the following actions in the background:

- Adds a badge to the README file of the first repository in the list of connected GitHub repositories
 - Creates a GitHub commit for the update made by adding the badge to the README file
 - Creates a GitHub pull request to merge the changes made to the README file
 - Links the GitHub commit and pull request to the work item created in step 1.
3. Lastly, choose **View work item** to open the work item created in step 1. Note the links under the **Development** section that correspond to the commit and pull request created in GitHub.com

fabrikam / Fabrikam Fiber / Boards

MyFirstProject Team

[View as Backlog](#)

To Do

New item

1 Add badge to README

UnknownUser

State To Do

Success!
Your GitHub repository is connected to Azure Boards.

Get started

We'll help you create a sample Issue, link it to a GitHub pull request with mentions, and add a badge to your README.

- Issue created and in the To Do column.
- Pull request created with the badge and linked to your Issue.

Quick tip

Mentioning an Azure Boards work item is just like mentioning a GitHub issue or pull request, except you begin with "AB#" before the work item ID.

[Close](#) [View work item](#)

4. Choose the pull request link (first link in the list) to open the pull request in GitHub.

The GitHub pull request opens in a new browser tab.

The screenshot shows an Azure Boards issue card for a project named 'Fabrikam Fiber'. The card has the following details:

- State:** Unassigned
- To Do:** To Do
- Area:** Fabrikam Fiber
- Reason:** Added to backlog
- Iteration:** Fabrikam Fiber

The card was updated just now. On the right side, there are sections for **Planning** (Priority set to 2), **Development** (with two items listed), and **Related Work**.

Description:

Azure Boards + GitHub is ready! Your Azure Boards project is ready and connected to GitHub. See the [GitHub & Azure Boards](#) documentation for more information about the integration. If you chose to create a linked pull request, you'll see that a commit and pull request have already been linked. Click the pull request title to review and merge in the commit to add the badge for this board to your repository's README. See the [status badge configuration](#) documentation for more information about configuring your badge.

Discussion:

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

Planning:

Priority: 2

Development:

- 1 Add the Azure Boards badge to the ... Updated 2 minutes ago, open
- 97954d3 Add the Azure Boards badge... Updated 2 minutes ago

Related Work:

+ Add link

5. Go ahead and complete the pull request.

The screenshot shows a GitHub pull request from 'JamalHart / fabrikam-demo'. The pull request has the following details:

- Open**
- JamalHart wants to merge 1 commit into `master` from `azure-boards`
- Pull requests:** 1
- Actions:** 0
- Projects:** 0
- Insights:** 0
- Settings:** 0

Add the Azure Boards badge to the README #1

Conversation: 0 Commits: 1 Checks: 0 Files changed: 1

JamalHart commented 3 minutes ago • edited by azure-boards bot Owner + ⚡ ...

Add the Azure Boards badge for the board used to track the work for this repository. Fixes AB#1. See the [status badge configuration](#) documentation for more information.

Add the Azure Boards badge to the README. Fixes AB#1 4e81d41

Add more commits by pushing to the `azure-boards` branch on `JamalHart/fabrikam-demo`.

Branch status: This branch has no conflicts with the base branch. Merging can be performed automatically.

Merge pull request You can also [open this in GitHub Desktop](#) or view command line instructions.

6. Navigate to your repository README file and view the badge that has been added.

The screenshot shows a GitHub repository page for 'JamalHart / fabrikam-demo'. At the top, there are buttons for 'Unwatch' (1), 'Unstar' (1), and 'Fork' (0). Below the header, there are tabs for 'Code' (selected), 'Issues 0', 'Pull requests 0', 'Projects 0', 'Wiki', 'Insights', and 'Settings'. A note says 'No description, website, or topics provided.' with an 'Edit' button. A link to 'Manage topics' is also present. Below this, summary statistics are shown: 7 commits, 2 branches, 0 releases, 1 contributor, and a license of 'GPL-3.0'. A dropdown for 'Branch: master' and a 'New pull request' button are available. A 'Clone or download' button is highlighted in green. The main content area shows a list of files: '.gitattributes' (Initial commit, 5 months ago), 'LICENSE' (Initial commit, 5 months ago), 'README.md' (Add the Azure Boards badge to the README. Fixes AB#1, 3 hours ago), and another 'README.md' entry with an edit icon. A red box highlights the 'Azure Boards Doing 0' badge in the 'README.md' file.

To learn more about Azure Boards badges, see [Configure status badges to add to GitHub README files](#).

Configure additional projects or repositories

You can configure additional Azure Boards/Azure DevOps projects, GitHub.com repositories, or change the current configuration from the Azure Boards app page.

NOTE

The Azure Boards app prevents you from connecting a GitHub repo to more than one Azure Boards/Azure DevOps organization. You can, however, connect a repo to two or more projects within the same organization. To learn more, see [Troubleshoot GitHub & Azure Boards connection](#).

1. Open the Azure Boards app page.



2. Choose **Configure**.
3. To add repositories, scroll down the page and choose each repository to add from the **Select repositories** drop-down menu.

Repository access

The screenshot shows the 'Repository access' settings page. It has two radio button options: 'All repositories' (selected) and 'Only select repositories'. Under 'Only select repositories', there is a 'Select repositories' button with a dropdown arrow. Below it, it says 'Selected 2 repositories' and lists two GitHub repositories: 'JeffreyHart/fabrikam-suite' and 'JeffreyHart/fabrikam-open-source', each with a delete 'X' icon. At the bottom are 'Save' and 'Cancel' buttons.

4. Follow steps 5 through 7 provided under the [Install and configure](#) section earlier in this article.

Uninstall the Azure Boards app

1. Open the Azure Boards app page.
2. Choose **Configure**.
3. Scroll down and choose **Uninstall**.

Uninstall Azure Boards

When you uninstall Azure Boards, it will be removed from this account and will lose access to all of its resources.

[Uninstall](#)

4. Confirm that you understand that uninstalling the Azure Boards app will remove all connections you've made to connect to GitHub repositories.

Add or remove repositories from Azure Boards

Once you've integrated Azure Boards with GitHub using the Azure Boards app, you can add or remove repositories from the web portal for Azure Boards.

1. From your Azure Boards project web portal, choose (1) **Project Settings**, expand **Boards** as needed, and then choose (2) **GitHub connections**.

The screenshot shows the 'Project Settings > GitHub connections' page in Azure Boards. The left sidebar has a 'Project settings' button highlighted with a red box and a '1'. The top navigation bar has a 'GitHub connections' tab highlighted with a red box and a '2'. The main area shows a table with one row for a GitHub connection named 'Fabrikam'.

Connection	Authentication type	Repositories
Fabrikam GitHub	OAuth	JamalHart/fabrikam-apps, 3 more

2. To add or remove repositories, open the **...** actions icon for the connection and choose **Add repositories** or **Remove repositories** from the menu.

The screenshot shows the 'GitHub connections' table. A context menu is open over the first row, which contains the repository 'Fabrikam/fabrikam-apps, 3 more' and the creator 'Jamal Hartnett'. The menu options are: Add repositories, Remove repositories, and Remove connection. A red arrow points from the 'Add repositories' option to the '...' icon in the table row.

Repositories	Created by
Fabrikam/fabrikam-apps, 3 more	Jamal Hartnett

3. To remove all repositories and the connection, choose the **Remove connection** option. Then, choose **Remove** to confirm.



Try this next

[Link GitHub commits and pull requests to work items](#)

Related articles

- [What is Azure Boards?](#)
- [Link GitHub commits and pull requests to work items](#)
- [Configure status badges to add to GitHub README files](#)

Resources granted to project members

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013 ↗

The project is a container and security boundary for your software development assets: work items, code, builds, etc. When you add someone as a member of a project, you are also trusting that person with some additional privileges. A project member has access to organization-level resources and additional groups (or scopes) beyond the project. If someone is not already a member of your organization, when you add them to a project, you implicitly grant them this additional access.

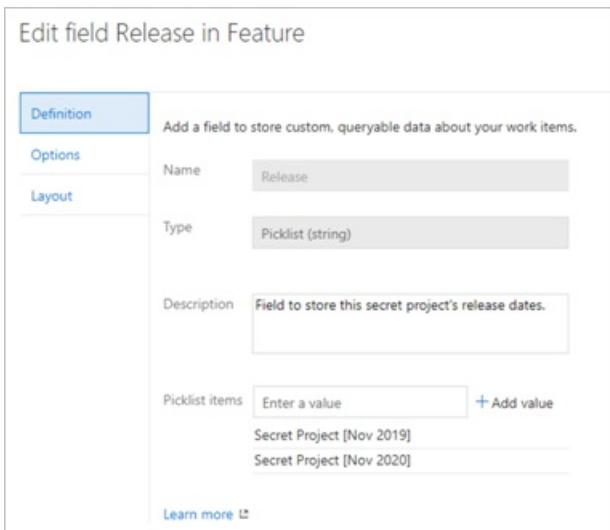
Additional groups and scopes

Under the hood, a project member belongs to one or more [project-related security groups](#) such as "Project Valid Users" and "Project Contributors". That person is also a member of an organization-level group known as "Project Collection Valid Users". Also, that person's identity appears in the [identity service](#) which backs the organization. User accounts backed by [Azure Active Directory](#) can have [native identities](#) or [guest identities](#), which grant different levels of access.

Organization-level resources

Project members have access to resources beyond the specific project. Those resources include those defined at the organization-level (cloud) or project collection level (on-premises):

- Information about other members, including their email address and other contact details, that is hidden from non-members.
- The Settings area, including security groups and permissions.
- All installed extensions, including paid extensions (if you assign a license).
- [Process](#) metadata from all processes in the organization, which includes the work item types, its fields and picklist items. Picklist items could show sensitive information such as release dates, as shown in the image below:



- When the WIT Client OM is used, which includes the usage of Excel and Visual Studio integration, it stores sensitive information in a cache on the local disk. This cache includes the metadata of all processes in the organization and the identities and group memberships of all members of the organization.

- When a user is added to the project-level Build Administrators group, they have the ability to create pipelines which run with project collection (account-wide) scope. A pipeline with project collection scope may access resources in another project, such as Git repositories, that the user cannot. (You can change this by [removing the Read permission from Project Collection Build Service](#)).

The trust decision

These resources and groups are required for the proper functioning of a member of a project. Your collaborators are typically colleagues and others with whom you have an existing relationship. Before you add someone from outside this trusted group, think carefully about whether they should have access to the items mentioned above.

Create a project in Azure DevOps and TFS

5/24/2019 • 8 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Create a project to establish a repository for source code, where a group of developers and teams can plan, track progress, and collaborate on building software solutions. Each project you create provides boundaries to isolate data from other projects and must be managed and structured to support your business needs. To learn more about projects and when or when not to create one, see [About projects and scaling your organization](#).

NOTE

This article is about creating a project in Azure DevOps or a Team Foundation Server. If instead you want to create Azure DevOps Projects, see [Azure DevOps Projects](#).

If you have a project already, and want to start coding an application project, then see one of the following topics: [Set up Git on your dev machine](#) or [Develop your app in Team Foundation version control](#).

NOTE

If you don't want to manage an on-premises server, you can [sign up for Azure DevOps Services](#) and create a project.

Create a project from the web portal

To create a project, you must first have [created an organization in Azure DevOps](#).

IMPORTANT

To create a Public project, or to make a private project public, see [Create a public project](#) or [Change the project visibility, public or private](#). Additional policy settings must be enabled to work with public projects.

IMPORTANT

When you create a project from the web portal, several process template files are ignored. Specifically, the files that would create a Report Manager site aren't supported. If you want SQL Server Reporting Services to be available, then create your project from Visual Studio or Team Explorer. For details, see [Process template and plug-in files, Client support for project creation](#).

IMPORTANT

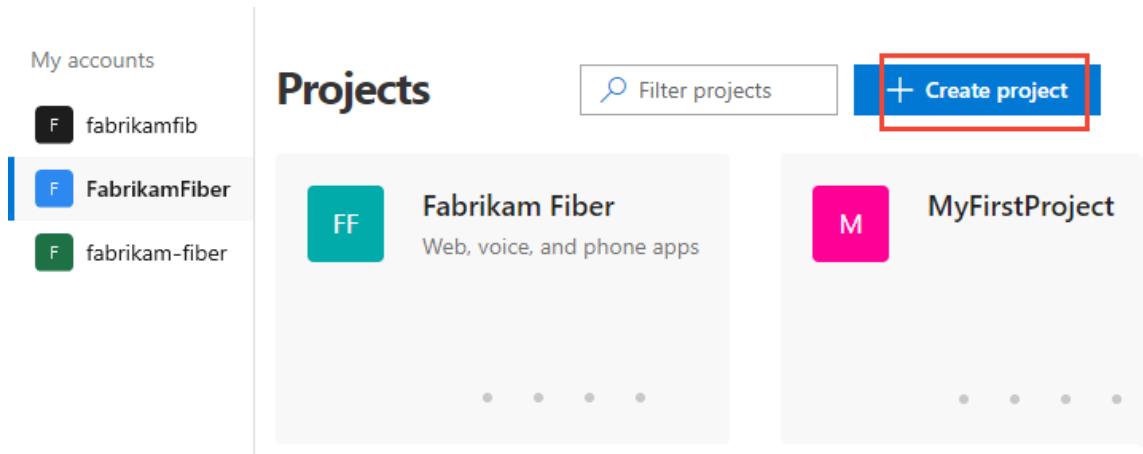
When you create a project from the web portal, several process template files are ignored. Specifically, the files that would create a Report Manager site and a SharePoint project portal aren't supported.

If you want these features to be available on your on-premises TFS, then create your project from Visual Studio or Team Explorer. For details, see [Process template and plug-in files, Client support for project creation](#).

If you're not a member of the Project Collection Administrators Group, [get added as one](#). To create projects

you must have the **Create new projects** permission set to **Allow**.

1. Choose the  Azure DevOps logo to open the **Projects** page, and then choose **Create Project**.



The screenshot shows the 'Projects' page in the Azure DevOps interface. On the left, there's a sidebar titled 'My accounts' with three items: 'fabrikamfib' (dark blue icon), 'FabrikamFiber' (light blue icon), and 'fabrikam-fiber' (green icon). The main area is titled 'Projects' with a search bar labeled 'Filter projects' and a red box around the 'Create project' button. Below the button are two project cards: 'Fabrikam Fiber' (Web, voice, and phone apps) and 'MyFirstProject'. Each card has a small icon (FF for Fabrikam Fiber, M for MyFirstProject) and a horizontal ellipsis below it.

2. Enter information into the form provided. Provide a name for your project, and choose the visibility, initial source control type, work item process. For details on public projects, see [Create a public project](#). If the **Public** option is grayed out, you need to change the policy.

Create new project X

Project name *
 ✓

Description

Visibility

 Public
Anyone on the internet can view the project. Certain features like TFVC are not supported.

 Private
Only people you give access to will be able to view this project.

^ Advanced

Version control ? ▾

Work item process ? ▾

Create Cancel

See [choosing the right version control for your project](#) and [choose a process](#) for guidance.

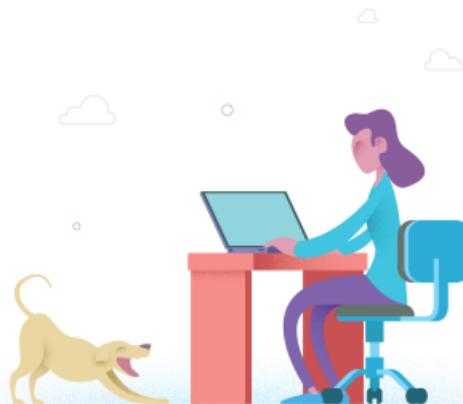
3. When your project has been created, the welcome page appears.

FT

Fabrikam Test

Private

Invite



Welcome to the project!

What service would you like to start with?

Boards

Repos

Pipelines

Test Plans

[or manage your services](#)

Select one of the following tasks to get started:

- **Invite** to begin [adding others to your project](#). Note, you can only invite users who have already been [added to your organization](#).
- **Boards** to begin adding work items.
- **Repos** to open [Repos>Files](#) page where you can clone or import a repository, or initialize a README file for your project summary page.
- **Pipelines** to start [defining a pipeline](#).
- **Test Plans** to start [defining test plans and test suites](#).
- [Manage your services](#) to disable the visibility of one or more services.

1. Choose the Azure DevOps logo to open the **Projects** page, and then choose **New Project**.

The screenshot shows the Azure DevOps interface. At the top, there is a navigation bar with links for 'Projects', 'My favorites', 'My work items', 'My pull requests', and a '...' menu. Below the navigation bar, the main area is titled 'Projects'. On the right side of this title, there is a search bar labeled 'Filter projects and teams' with a dropdown arrow icon. To the right of the search bar is a blue button with white text that says 'New Project', which is outlined with a red border. Below the title, there is a section titled 'Recent' with two items listed: 'FabrikamFiber' and 'FabrikamFiberTest', each represented by a small folder icon.

2. Fill out the form provided. Provide a name for your new project, and choose the visibility, initial source control type, work item process. For details on public projects, see [Create a public project](#). If the **Public** option is grayed out, you need to change the policy.

Create new project

Projects contain your source code, work items, automated builds and more.

Project name *

 ✓

Description

Test project for testing new features prior to roll out.

Visibility

Public Anyone on the internet can view the project. Certain features like TFVC are not supported. [Learn more](#).

Private Only people you give access to will be able to view this project.

Version control

Git ?

Work item process

Agile ?

Create Cancel

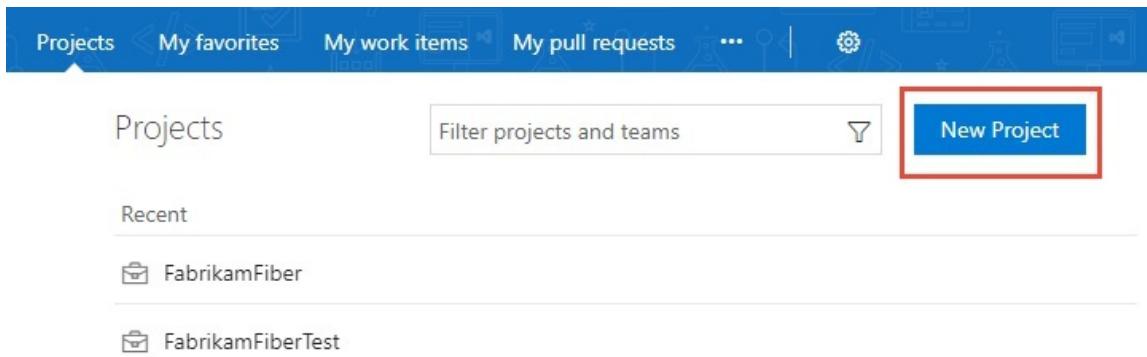
See [choosing the right version control for your project](#) and [choose a process](#) for guidance.

3. Upon successful completion, the project summary displays. To learn more, see [Share your project vision](#).

NOTE

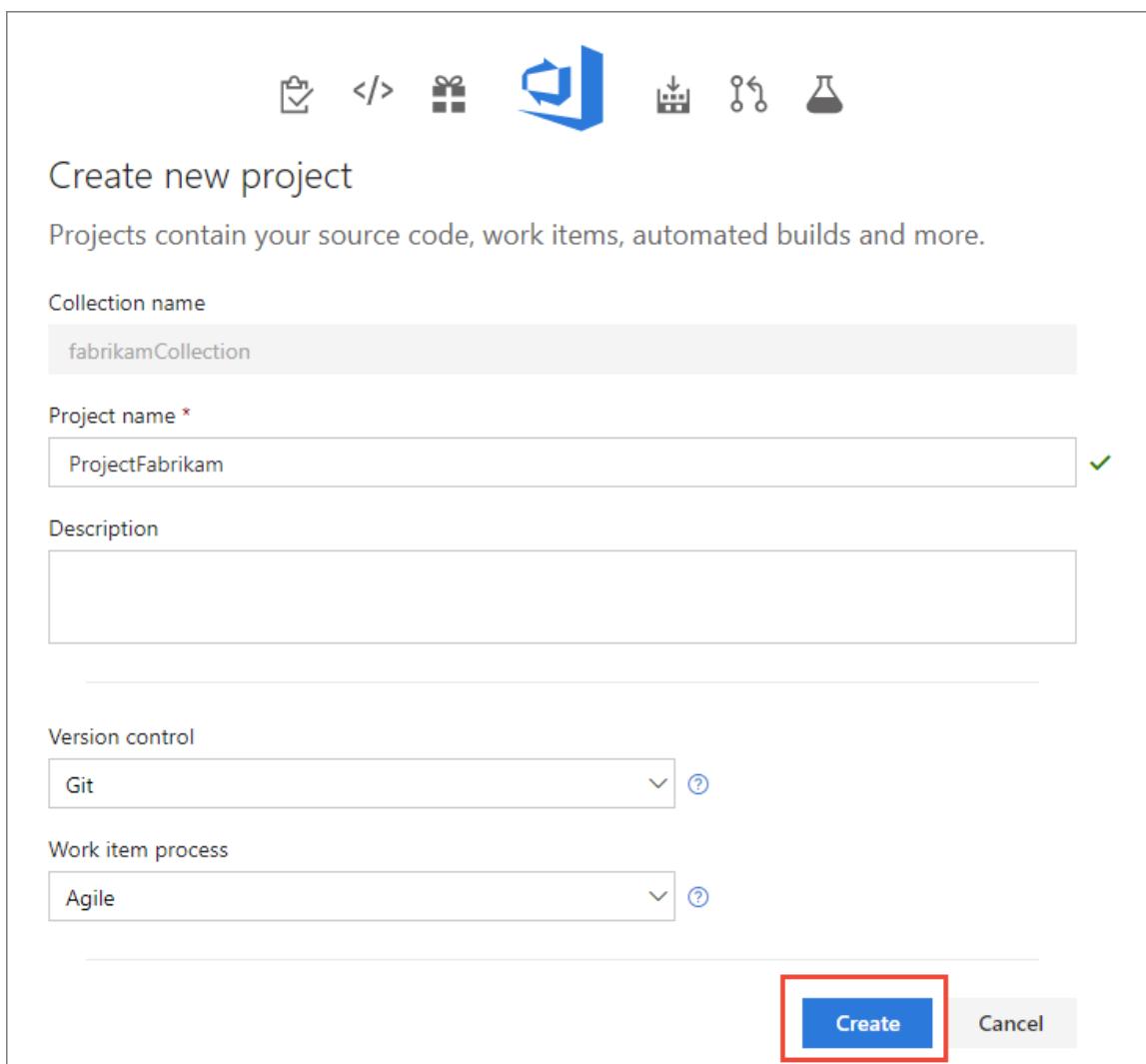
TFS 2018 and later versions no longer support native integration with SharePoint products. If you're planning to upgrade to TFS 2018, read [About SharePoint integration](#) to learn about the options available to you.

1. Choose the  Azure DevOps logo to open the **Projects** page, and then choose **New Project**.



2. Fill out the form provided. Provide a name for your new project, select its initial source control type, select a process, and choose with whom to share the project.

See [choosing the right version control for your project](#) and [choose a process](#) for guidance.



If you're using TFS 2015.2 or later version, then you can create a project from the web as well. It's important to note that for projects created from the web, Reporting and SharePoint integration steps are skipped when creating the project. You can still set up [Reporting](#) and [SharePoint](#) manually after project creation.

1. If you have TFS 2017.1 or a later version, choose the  to open the **Projects** page, and then choose **New Project**.

The screenshot shows the TFS 2015.2 or TFS 2017 interface. At the top, there is a navigation bar with links for 'Projects', 'My favorites', 'My work items', 'My pull requests', '...', and a gear icon. Below the navigation bar, the main area is titled 'Projects'. It features a search bar labeled 'Filter projects and teams' and a 'New Project' button, which is highlighted with a red box. Under the search bar, there is a section titled 'Recent' with two entries: 'FabrikamFiber' and 'FabrikamFiberTest', each preceded by a folder icon.

Otherwise, for TFS 2015.2 or TFS 2017, open the administration overview page by choosing the gear icon at the top of the page and choose **Server settings**. Then choose **New project...**

The screenshot shows the collection administration page for 'Fabrikam-Fiber-Inc'. The top navigation bar includes links for 'Overview', 'Settings', 'Security', 'Users', 'Process', 'Build and Release', 'Agent Pools', and 'Notifications'. The main content area is titled 'Account / Fabrikam-Fiber-Inc' and 'Projects'. On the left, there is a 'Description' section. In the center, there is a button labeled 'New team project...' which is highlighted with a red box. Below this button, there is a table with three columns: 'Project name', 'Process', and 'Status'. It lists two projects: 'Fabrikam' (Scrum, Online) and 'Fabrikam Mobile' (Scrum, Online).

Project name	Process	Status
Fabrikam	Scrum	Online
Fabrikam Mobile	Scrum	Online

Select the collection administration page for the collection you want to create the project in from the left pane, and choose **Create a new project....**

2. Enter information into the form provided. Provide a name for your new project, select its initial source control type, select a process, and choose with whom to share the project.

See [choosing the right version control for your project](#) and [choose a process](#) for guidance.

Create new project

Projects contain your source code, work items, automated builds and more.

Collection name

fabrikamCollection

Project name *

ProjectFabrikam ✓

Description

Version control

Git

Work item process

Agile

Create Cancel

Creating a project from the web portal isn't supported for TFS 2015 and earlier versions. Use [Team Explorer to create a project](#).

Create a project in Team Explorer

You can create a project from Team Explorer after you have connected to an on-premises server.

NOTE

For TFS 2018 and later versions, users are redirected to the web. They no longer are able to create a project from Visual Studio.

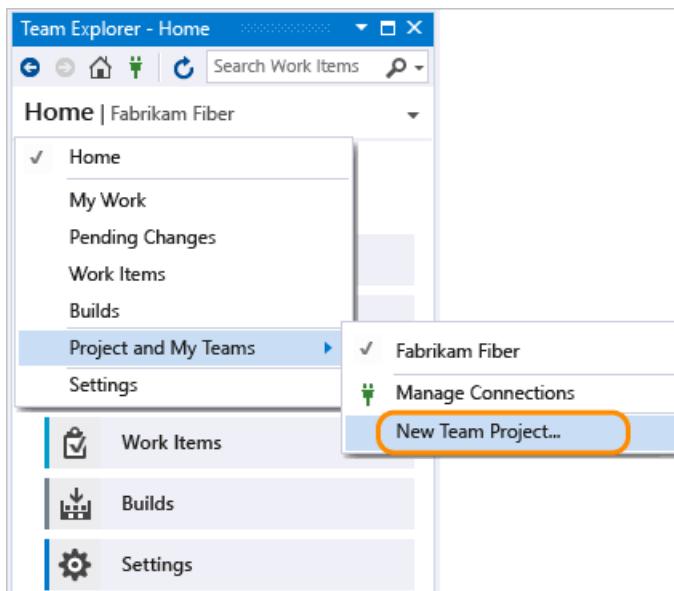
TFS 2018 and later versions no longer support native integration with SharePoint products. If you're planning to upgrade to TFS 2018, read [About SharePoint integration](#) to learn about the options available to you.

1. If you're not a member of the Project Collection Administrators Group, [get added as one](#). To create projects you must have the **Create new projects** permission set to **Allow**.
2. Ask your TFS administrator about the following resources and get additional permissions as needed:
 - Which project collection should you connect to when you create your project? If you installed TFS using the Basic Server Configuration Wizard, you have only one project collection named **DefaultCollection**. Unless you are supporting hundreds of projects, you should create all your projects within a single project collection. If you need to create additional collections, see [Manage project collections](#).

- Has SQL Server Analysis Services and SQL Server Reporting Services been configured for the deployment? If so, ask your administrator to [add you as a member of the Team Foundation Content Managers group](#) on the server that hosts SQL Server Reporting Services. Without these permissions, you are unable to create a project.
 - Has a SharePoint Web application been configured for your deployment? If you want to configure a SharePoint portal when you create your project, ask the SharePoint administrator to give you Full Control permissions on the server that hosts SharePoint Products. Otherwise, you can skip this step and configure a portal at a later time.
3. Open the same version of Visual Studio as the version of TFS that you're connecting to. If you don't see the Team Explorer pane, open **View>Team Explorer** from the menu.

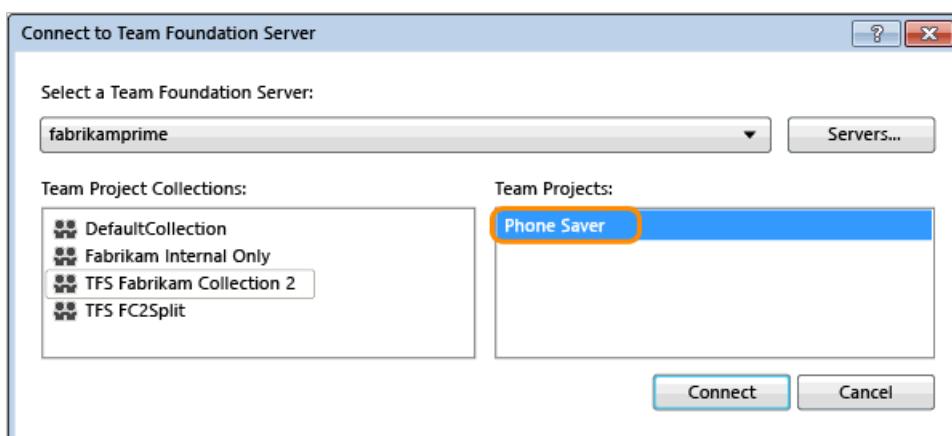
As needed, [Download and install Visual Studio Community](#) to get a free copy of the latest version.

4. Connect to the server and project collection where you want to create your project.



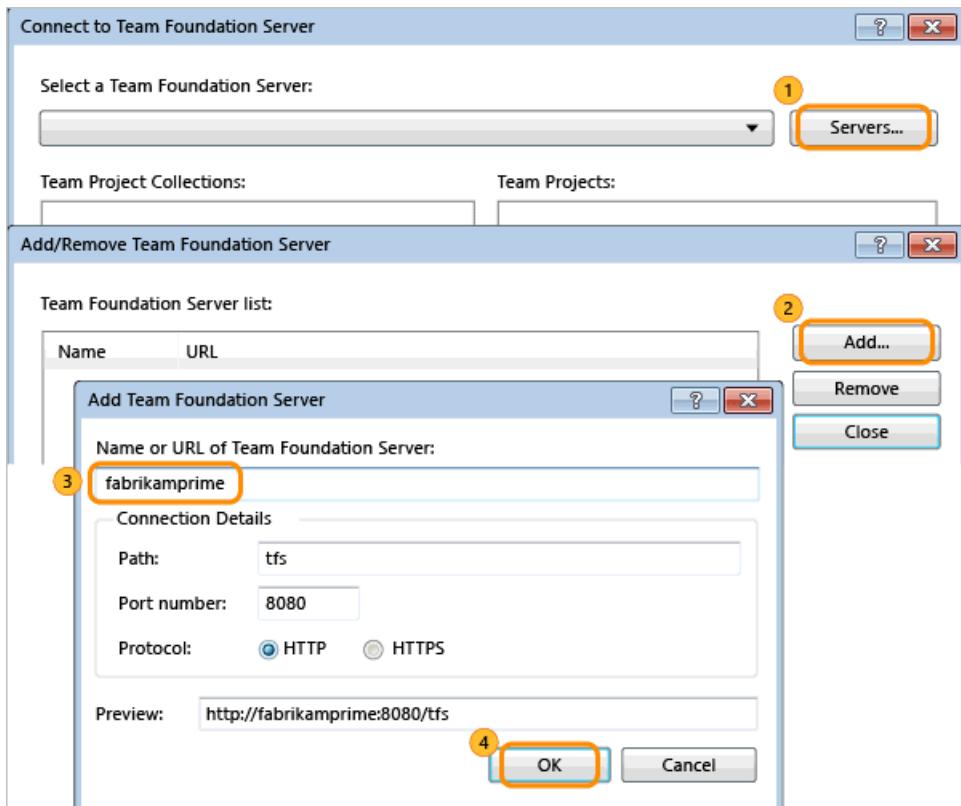
You can access Team Explorer for free by installing [Visual Studio Community](#) or any other Visual Studio version.

You must connect from a client that is at the same version level as TFS. That is, you must connect to TFS 2015 from a version of Visual Studio 2015.

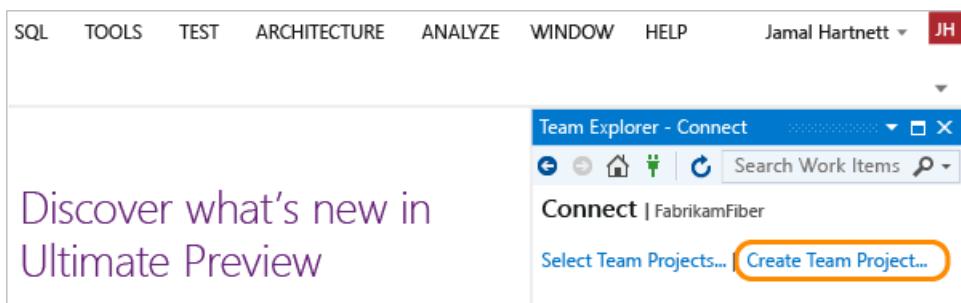


Tip: If you are running Team Explorer from a server that hosts SharePoint Products and SQL Server Reporting Services, you might need to run Visual Studio as an administrator.

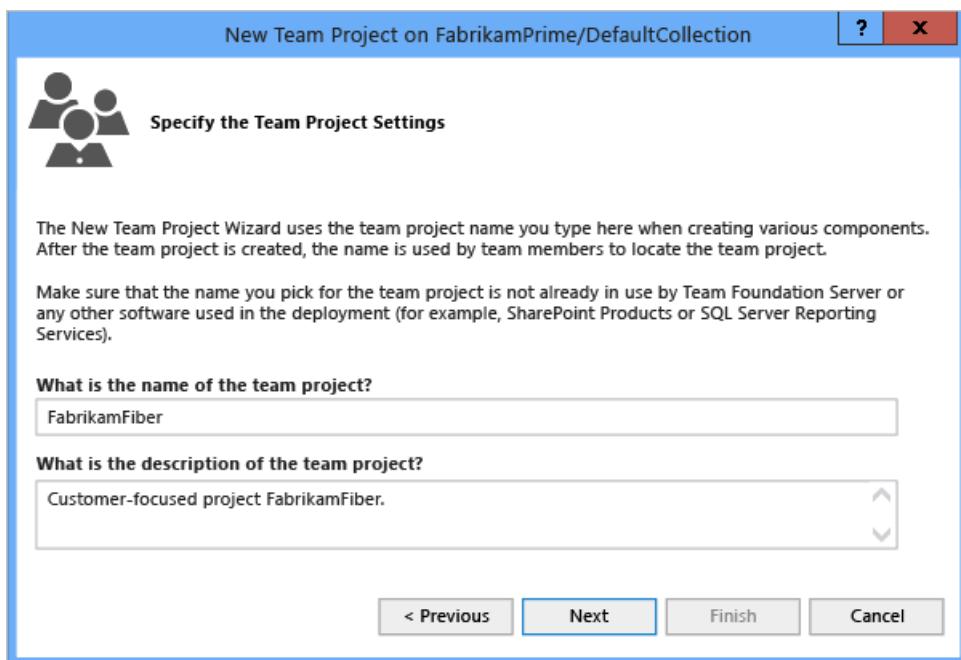
5. If it's your first time connecting to TFS, you need to add TFS to the list of recognized servers.



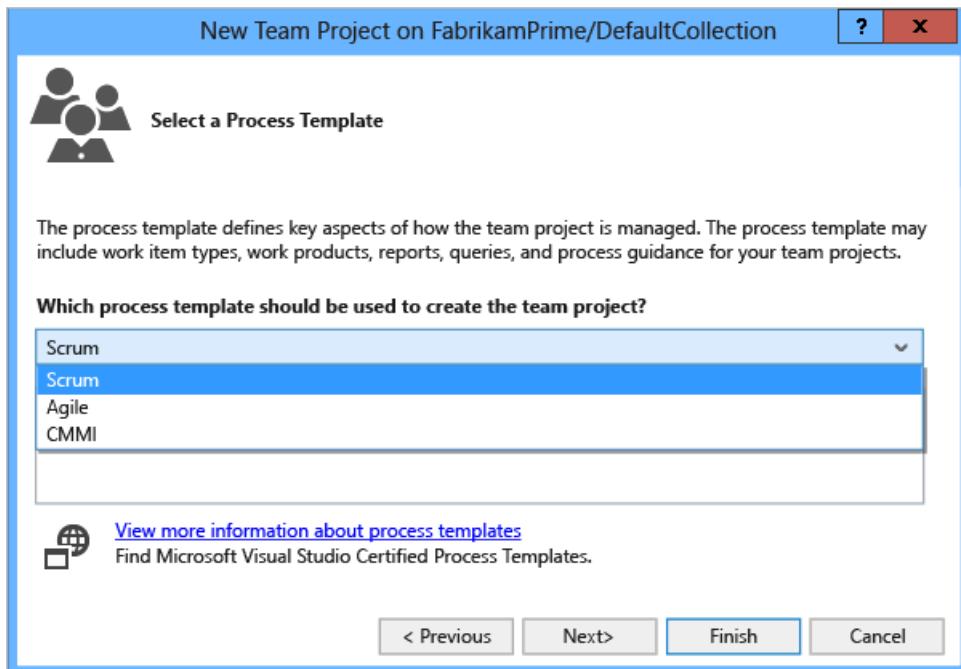
6. Open the New Project Wizard.



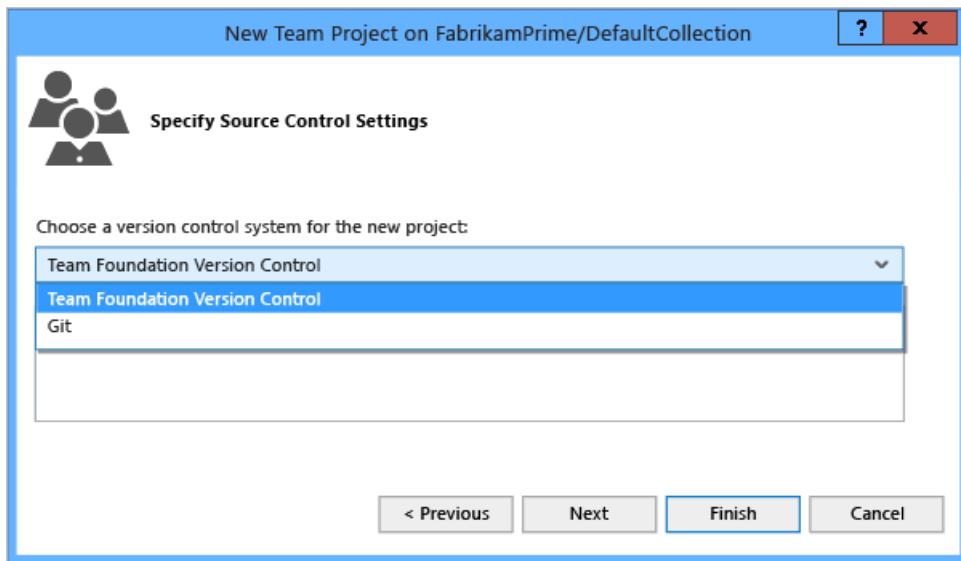
7. Name the project. Don't specify more than 64 characters.



8. Choose a process template. For a comparison of the default process templates, see [Choose a process](#).



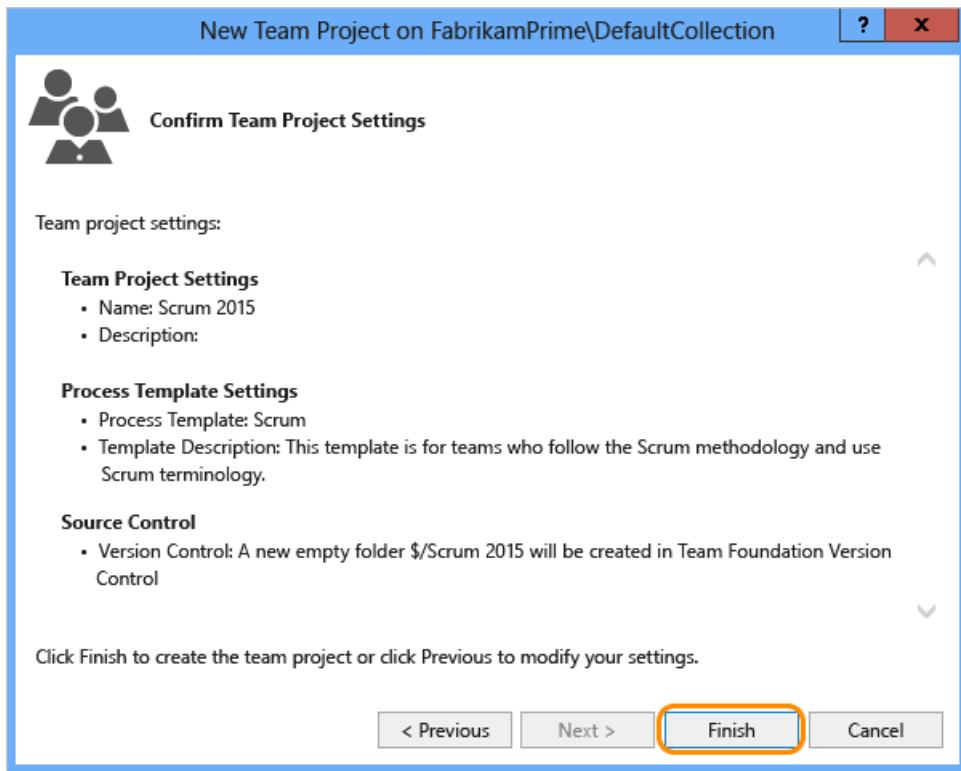
9. Choose your version control, either Git distributed repositories or TFVC, one centralized repository.



Not sure which system to use? Learn more about [Git](#) or [TFVC](#).

After you've created your project, you can [add repositories](#).

10. Unless your project collection is configured to support a SharePoint project portal, you're done.



If the Next button is active, you can configure your project portal.

If the wizard encounters a problem, you receive an error message and a link to the project creation log. Review the [log file](#) for specific errors and exceptions.

- When you're finished, you can see your project in Team Explorer. You can also choose the **Web Access** link to connect to your project from the web portal.

The image contains two side-by-side screenshots of the 'Team Explorer - Home' interface. Both screenshots show a similar layout with a top navigation bar and a main content area. The left screenshot shows a simplified view with items like 'My Work', 'Pending Changes', 'Source Control Explorer', 'Work Items', 'Builds', and 'Settings'. The right screenshot shows a more detailed view with additional items like 'Changes', 'Branches', 'Pull Requests', 'Sync', 'Work Items', 'Builds', and 'Settings'. Both screenshots include a note at the bottom: 'You must [configure your workspace](#) mappings to open solutions for this project.' and 'You must [clone the repository](#) to open solutions for this project.'

Create a project from the command line or scripts

You can create and retrieve projects and other objects from the command line or scripts using the CLI. Check out the [CLI documentation](#) to learn more.

NOTE

The CLI is supported for TFS 2017.2 and later versions.

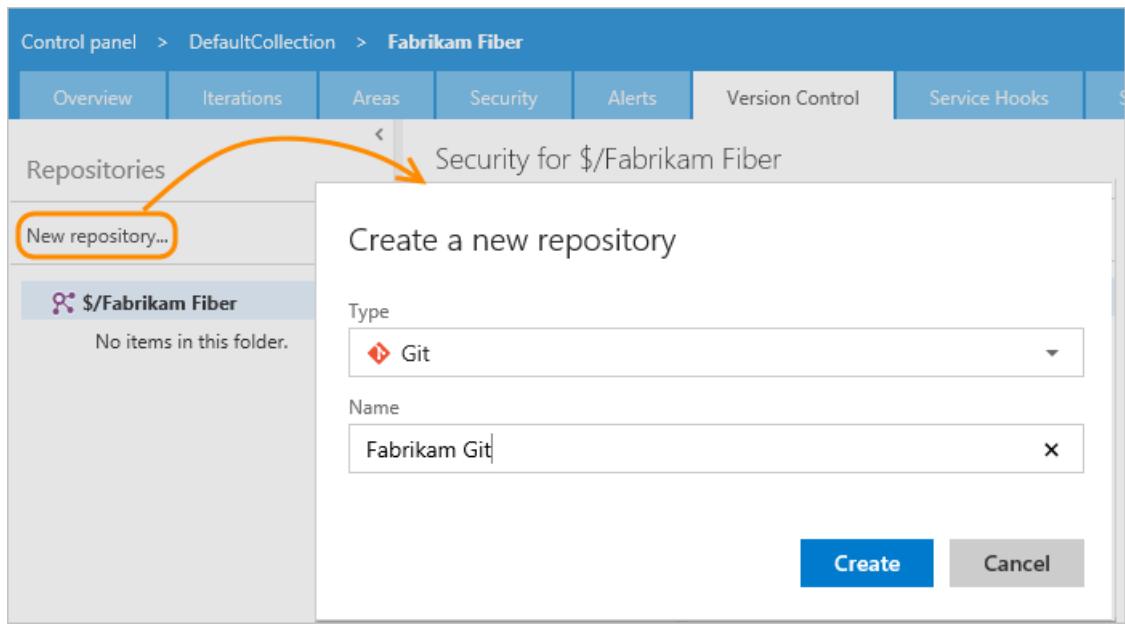
Add a repository

From the admin context of the web portal, you can add additional repositories to a project, either Git (distributed) or TFVC (centralized). While you can create many Git repositories, you can only create a single TFVC repository for a project. Additional steps to address permissions may be required. See [Use Git and TFVC repos in the same project](#).

The screenshot shows the 'Security for all Git repositories' page. On the left, there's a sidebar with 'Repositories' and a 'New repository' button highlighted with a red box. Below it are 'Git repositories' and two other items. The main area has tabs for 'Security' and 'Options'. Under 'Security', there's a 'Search' bar and a 'VSTS Groups' dropdown with 'Build Administrators' selected. To the right is a 'ACCESS CONTROL SUMMARY' section with links like 'Contribute', 'Create branch', etc.

Name the repository and choose **Create**.

The dialog box has a title 'Create a new repository' and a close button 'X'. It contains a 'Type' dropdown set to 'Git', a 'Repository name *' input field containing 'Test 1-2-3', and a checked checkbox 'Add a README to describe your repository'. Below that is a dropdown for '.gitignore' with 'None' selected. At the bottom, a note says 'Reminder: Visual Studio users will need Visual Studio 2015 Update 1 or later to view TFVC and Git repositories in team projects that include both types.' There are 'Learn more' and 'Create' buttons at the bottom.



NOTE

The ability to work from both Git and TFVC repositories from the same project is supported when you connect to TFS 2015.1 and later versions.

Next steps

[Get started as an administrator](#)

Related articles

- [Use Git](#)
- [Develop your app in TFVC](#)
- [Additional project structure activities](#)

Rename a project in Azure DevOps

7/10/2019 • 6 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

In this article, learn how to rename a project. A project rename updates all of your version control paths, work items, queries, and other project artifacts to reflect the new name. Projects can be renamed multiple times and older names can be reused. Post rename, there might be some [actions](#) required from team members. We recommend performing this action during off-hours to minimize any impact.

Open organization settings

Organization settings configure resources for all projects or the entire organization. For an overview of all organization settings, see [Project collection administrator role and managing collections of projects](#).

1. Choose the  Azure DevOps logo to open **Projects**, and then choose **Collection settings**.



2. Select a service from the sidebar. Settings are organized based on the service they support. Expand or collapse the major sections such as **Boards** and **Pipelines** to choose a page.



1. Choose the  Azure DevOps logo to open **Projects**, and then choose **Organization settings**.



2. Select a service from the sidebar. Settings are organized based on the service they support. Expand or collapse the major sections such as **Boards** and **Pipelines** to choose a page.



1. Choose the  gear icon to open **Collection Settings**.



2. From there, you can choose a page. Settings are organized based on the service they support.



Rename a project

1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>), and then open the project that you want to rename.
2. Select **Project settings** > **Overview**, and then enter a new name and select **Save**.

Project Settings <ul style="list-style-type: none"> General Overview Teams Security Notifications Service hooks Dashboards Boards Project configuration Team configuration GitHub connections Pipelines Agent pools Parallel jobs 	<h2>Project details</h2> <p>Name</p> <input style="width: 100%; border: 2px solid red; height: 30px; margin-bottom: 10px;" type="text" value="FabrikamFiber1"/> <p>Description</p> <div style="border: 1px solid #ccc; width: 100%; height: 100px; margin-bottom: 10px;"></div> <p>Process</p> <div style="background-color: #f0f0f0; padding: 5px; border-radius: 5px; width: 100%;">Scrum</div> <p>Visibility</p> <div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> 🔒 Private ▼ </div> <p>This determines who can view this project. Learn more about project visibility.</p> <p style="text-align: center;">Save</p>
---	--

3. To confirm the rename, enter the new project name, check the box next to, "I understand the consequences of renaming this project," and then select **Save**.

Change project name

Renaming this project is a disruptive action that can significantly impact all members. The new name will update across all version control paths, work items, queries, URLs and any other project content. Project members may need to react and all currently running builds may fail as a result of this change.

Please ensure you fully understand the impact and have notified all project members before completing this action. [Learn more](#)

Current name: FabrikamFiber

New Project Name

I understand the consequences of renaming this project.

Cancel
Save

Your project is renamed.

::: moniker range=">= tfs-2017"

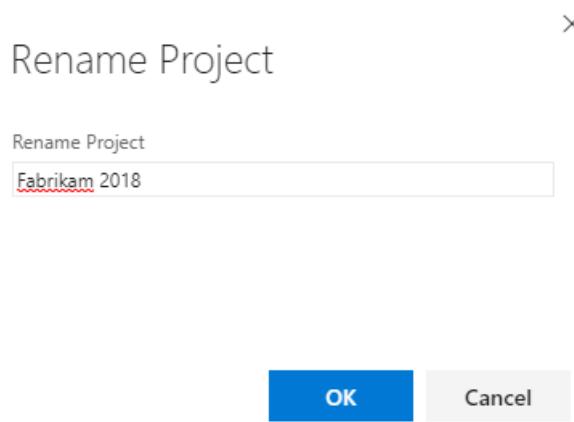
1. From the Projects page, open the **...** actions icon menu for the project that you want to rename and choose **Rename**.

Projects

New team project... |

Project name	Process	Status	Description
Agile 11	MyAgile 2	Online	New agile project
CMMI	MyScrum	Online	Agile team project
Demo 11	MyAgile Test	Online	Web, voice, and phone apps
Fabrikam Fiber	MyAgile	Online	Project used to verify MyAgile process customization
Fabrikam Test	Scrum	Online	Customer-focused apps under development based on Scrum
FabrikamFiber	MyAgile	Online	Test Scrum 2.0 migration
Scrum 2.0	MyAgile	Online	
Test Agile Repo	MyAgile	Online	

2. Edit the name.



If the Rename Project dialog doesn't appear, then you're not a member of the Project Administrators group for that particular project. Learn how to [get added](#) to the Project Administrators group.

1. From the **Overview** tab, open the context icon menu for the project that you want to rename and choose **Rename**.

The screenshot shows the 'Control panel > DefaultCollection' interface. At the top is a navigation bar with tabs for 'Overview', 'Security', and 'Build'. The 'Overview' tab is active. On the left, there's a 'Collection profile' section with a 'Name' field set to 'DefaultCollection'. To the right, there's a 'Projects' section. It starts with a 'New project' button and a refresh icon. Below that is a table with columns for 'Project Name' and 'Description'. The first row in the table is for a project named 'Fabrikam', which has a context menu open over it. The 'Rename' option in this menu is highlighted with a red box. The second row in the table is for a project named 'Fabrikam-Fiber-TFVC'.

2. Edit the name.

Rename Project



If the Rename Project dialog doesn't appear, then you're not a member of the Project Administrators group for that particular project. Learn how to [get added](#) to the Project Administrators group.

Let your team know what they have to do

Now that you've renamed your project, your team must restart their clients and perform additional actions based on the features they use.

Restart your clients

Opened clients keep a cache of all project names in memory and this cache isn't automatically cleared after a project is renamed. To clear the cache, all that is necessary is to restart the client so it populates the new project name. If you don't restart the client, then operations that use the cached project name fails with a project not found exception.

For the following clients, save your work in each and restart:

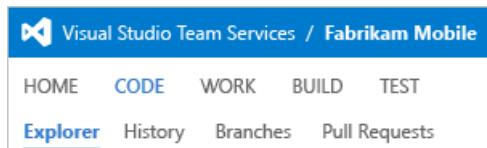
- Visual Studio/Team Explorer
- Eclipse, if your team uses the Team Foundation Server plugin (Team Explorer Everywhere)
- Microsoft Excel, PowerPoint, or Project, if your team uses the Team Foundation Server Extension for these Office products
- Any additional clients which use the .NET Team Foundation Server Client Object Model

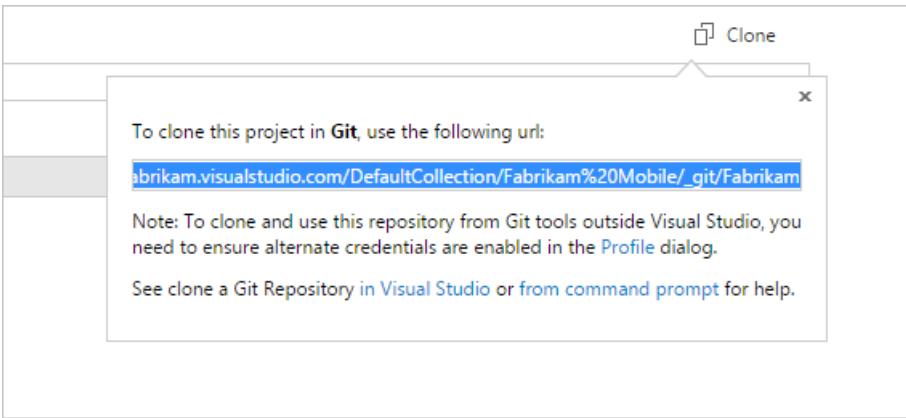
Update your Git remotes

If your project uses Git, then your remote references for each repository from the renamed project need to be updated. This is due to the fact that the remote repository URL contains the project and the repository name. Git uses remote references to fetch and push changes between your local copy of a repository and the remote version stored on the server. Each member of your team must update their local Git repos to continue connecting from their dev machines to the repo in the project.

Get the new URL for the repo

Copy the repository URL to your clipboard.



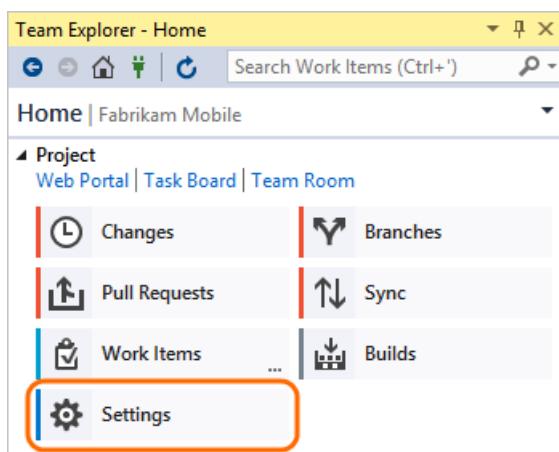


Update your remote in Visual Studio 2015

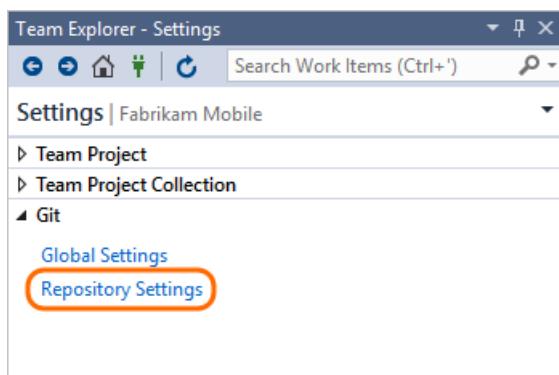
1. Connect to the repo.



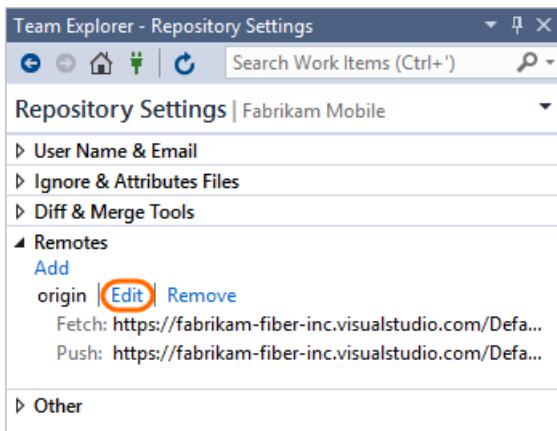
2. Open the project settings.



3. Open the repo settings.



4. Edit the fetch and push remote references and paste the URL that you copied from the remote repo.



Update your remote in older versions of Visual Studio from the command prompt

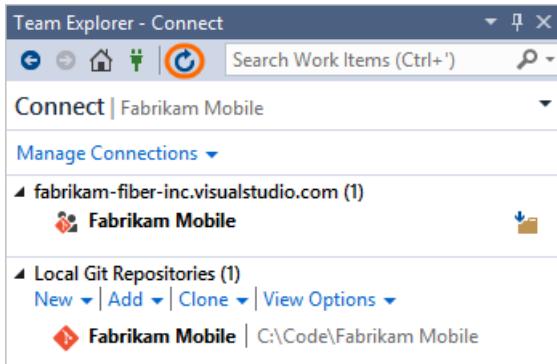
If you use an older version of Visual Studio or work with Git from the command prompt:

1. Open the Git command prompt.
2. Go to the local repository and update the remote to the URL you [copied from the remote repo](#).

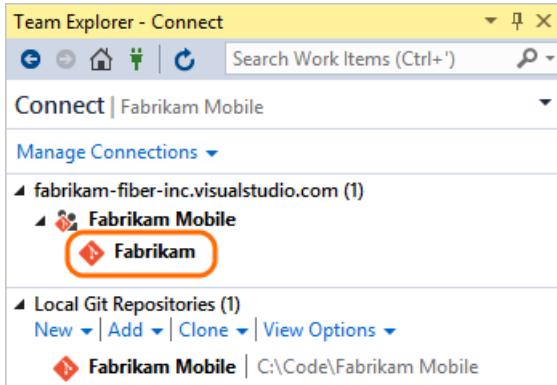
```
git remote set-url origin {URL_you_copied_from_the_remote_repo}
```

Refresh Team Explorer

1. Refresh Team Explorer.



2. Team Explorer now shows the updated repo name.

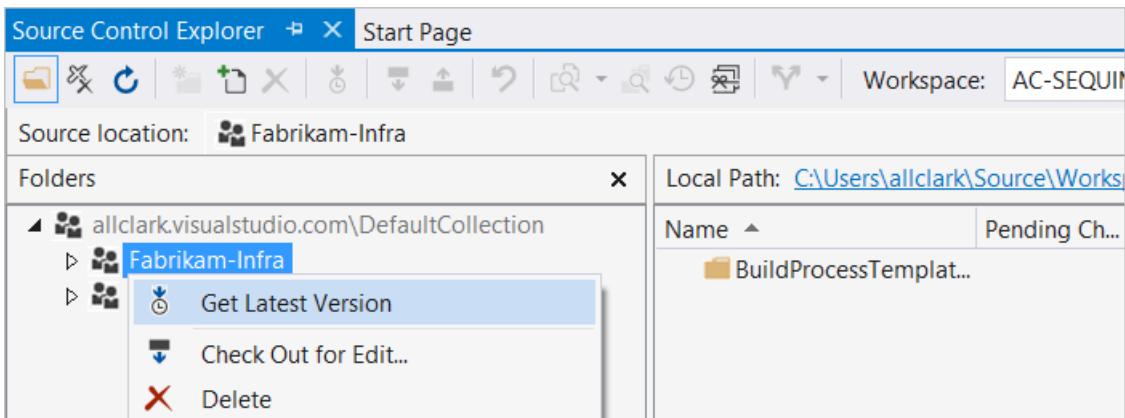


Update your TFVC server workspaces

If your project uses TFVC with [server workspaces](#), these workspaces need to be updated with the new project name. For the following clients, execute a get or check-in and the workspace mapping is corrected to use the new project name:

- Visual Studio 2015 (RC or newer)
- Visual Studio 2013

- Visual Studio 2012
- Visual Studio 2010 (Only supports server workspaces)
- Team Explorer Everywhere (2012 or later versions)



Update your TFVC local workspaces

If your team uses TFVC with [local workspaces](#), these workspaces need to be updated with the new project name. For the following clients, execute a get or check-in and the workspace mapping is corrected to use the new project name:

- Visual Studio 2015 (RC or later versions)
- Visual Studio 2012 with [Update 5](#) (RC or later versions)
- Team Foundation Server plugin [Team Explorer Everywhere 2015](#)

We recommend that you update your clients to the latest update or release, if possible. For all other supported Visual Studio versions, except for Visual Studio 2010 which only supports server workspaces, and Team Foundation Server plugin for Eclipse, you must create a new local workspace mapped to the new project name.

1. [Shelve your changes](#).
2. [Create a new workspace](#) mapped to the new project name.
3. Unshelve your changes.

Since local workspaces are managed locally and not on the server, older clients without the updated rename logic are unable to update local workspaces to the new project name on the next get or check-in.

Update your Team Foundation Server SharePoint and Reporting Integrations (on-premises)

Both SharePoint and Reporting Services integrations continue to work, but some reports don't work as expected until the new project name is populated. The old project name is still present until caches are updated with the new name. The reporting and SharePoint server administrator can manually run these jobs to immediately populate the new name.

- If your team uses reports, they reflect the new names after the next incremental analysis job runs for the data warehouse. By default it runs every two hours. To expedite the process, [manually run the warehouse jobs and incremental analysis job](#), so the new name is synced to warehouse and reports start using the new name. Reports don't work as expected until the jobs have run.
- If your team uses SharePoint Integration and has custom queries or web parts which directly reference the project name, update the name in each to the new project name. All default queries and web parts don't need to be updated and continue to work. Use of `@project` also continues to work after a project rename and also don't need to be updated.

- Excel reports and Excel web parts on MOSS don't show the right data until you execute the following.
 1. Warehouse job - [Run the warehouse jobs](#) so that Excel reports contain the correct data. If the new project name is not synced to the warehouse, Excel reports don't show the correct data. To avoid this, manually run warehouse jobs.
 2. SharePoint timer job - Run the "Team Foundation Server Dashboard Update" job from the SharePoint central admin to update Excel web parts on the dashboard. By default, it runs every 30 minutes. Until this job runs, the Excel web parts on the dashboard and the web parts that show reports directly from the reporting folder won't work because they'll use either the wrong project name or the wrong reporting folder.
 3. SharePoint cache - Manually clear the SharePoint cache to avoid stale data, such as report folder locations, appearing in the dashboards. By default, this cache clears about every hour. You can also clear some TFS specific cache using the tfs redirect url and providing a "clearcache" parameter. For example:

```
http://<SharePointServer>/sites/<TeamProjectCollectionName>/<TeamProjectName>/_layouts/TfsRedirect.aspx?tf:type=Report&tf:clearcache=1
```

Delete a project

7/8/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

In this article, learn how to delete a project from Azure DevOps. Deleting a project helps simplify the navigation to projects that are only in use.

Caution

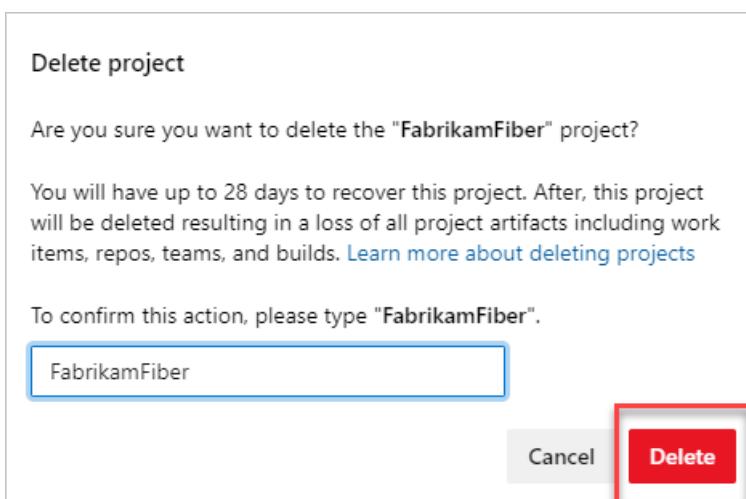
Projects are permanently deleted, if not restored within 28 days. For more information on restoring projects, see [Restore a project](#). If you want to access project data while the project is deleted (without [restoring it](#)) you should [save project data](#).

Delete project

1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>), and then open the project that you want to delete.
2. Select **Project settings > Overview**, scroll down the page to find "Delete project", and then select **Delete**."

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. The left sidebar lists various project management tools: Overview, Boards, Repos, Pipelines, Test Plans, and Artifacts. Below these are 'Project settings' and a 'Delete project' button, both highlighted with red boxes. The main content area is titled 'Project Settings' and contains a 'General' section with 'Overview' (which is also highlighted with a red box), 'Teams', 'Security', 'Notifications', 'Service hooks', 'Dashboards', 'Boards', 'Project configuration', 'Team configuration', and 'GitHub connections'. A separate 'Pipelines' section includes 'Agent pools', 'Parallel jobs', 'Settings', 'Release retention', and 'Service connections'. Under 'Repos', there are 'Repositories' and 'Policies'. The 'Test' section includes 'Retention'. To the right, the 'Project administrators' section lists 'FabrikamFiber-tfvc Team' and the email 'fabrikamfiber5@hotmail.com'. A blue 'Add administrator' button is present. Below this is a section titled 'Azure DevOps services' listing 'Boards', 'Repos', 'Pipelines', 'Artifacts', and 'Test Plans' with their respective descriptions. At the bottom right of the main content area is a large red 'Delete' button.

3. To confirm deletion, enter the project name into the popup screen, and then select **Delete**.



Your project is deleted and can be restored up to 28 days afterward.

Open organization settings

Organization settings configure resources for all projects or the entire organization. For an overview of all

organization settings, see [Project collection administrator role and managing collections of projects](#).

1. Choose the  Azure DevOps logo to open **Projects**, and then choose **Collection settings**.



2. Select a service from the sidebar. Settings are organized based on the service they support. Expand or collapse the major sections such as **Boards** and **Pipelines** to choose a page.



1. Choose the  Azure DevOps logo to open **Projects**, and then choose **Organization settings**.



2. Select a service from the sidebar. Settings are organized based on the service they support. Expand or collapse the major sections such as **Boards** and **Pipelines** to choose a page.



1. Choose the  gear icon to open **Collection Settings**.



2. From there, you can choose a page. Settings are organized based on the service they support.



Delete a project from TFS

Using the administration console, you can delete a project from a project collection. Afterwards, you'll need to manually delete any associated reports and SharePoint project portal. Or, you can use the [TFSDeleteProject command line tool](#) to delete all artifacts.

1. If you're not a member of one or more of the following administrator groups, [get permissions now](#):

- Team Foundation Administrators group (required).
- SQL Server System Administrators group (required).
- Farm Administrators group for SharePoint Products (required when your deployment uses SharePoint Products).

2. Open the administration console for TFS and delete the project from its project collection.

The screenshot shows the 'Team Project Collections' page in the TFS Administration Console. On the left, a navigation tree includes 'Application Tier' with 'Team Project Collections' selected. The main area displays a table of team projects:

Name	State
DefaultCollection	Offline
Agile Project	Active
Fabrikam Fiber Website	Active
FabrikamFiber	Active
Scrum 3.0	Active

Below the table are three tabs: 'General', 'Status' (selected), and 'Team Projects'. A 'Create Collection' and 'Attach Collection' button are also present.

3. Choose whether to delete external data associated with the project and then initiate the delete action.

The screenshot shows the 'Delete Team Projects' dialog box. It contains the following text:

You have selected one or more team projects for deletion. This will permanently delete the projects and all data contained in those projects.

In addition to deleting the team projects, you can also select options to remove data associated with these projects.

Delete external artifacts

Choosing this option will delete data related to these projects from the components that support the collection, including Lab Management and SQL Server Reporting Services. Project portals will not be removed from the SharePoint Web application. If you want to remove the portal, you must do so manually.

Delete workspace data

Choosing this option will delete any workspaces associated with the selected team projects. If you are deleting these projects as part of splitting a collection, you should delete the associated workspace data.

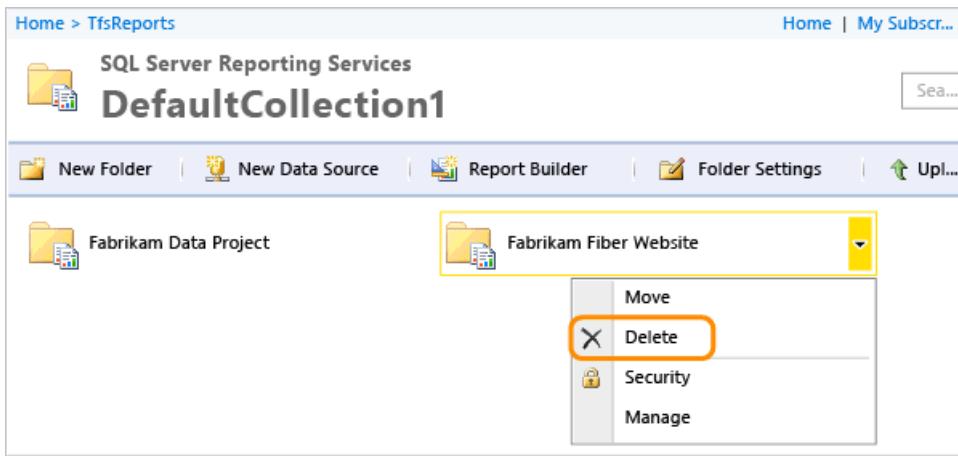
At the bottom are 'Delete' and 'Cancel' buttons.

4. (Optional) To review the status of the delete action, open the **Status** tab.

To review the details of the delete action, you can open the log file from either the **Status** tab or **Logs** tab.

Delete reports that remain after deleting a project

If your on-premises project used reporting, and you didn't choose to delete external artifacts, you can delete the reports using SQL Server Report Manager. From the project collection page, delete the folder that corresponds to the deleted project.



Remove the project portal

If your on-premises project had a project portal, all links to that portal are removed from TWA and Team Explorer, but the SharePoint site or website that acted as the portal is not deleted. If you want to delete the portal, you must do so manually after the project has been deleted. See [How to: Create, Edit, and Delete Windows SharePoint Services Sites](#).

What to do if the delete action doesn't finish

Review the status and log files for the delete action. Open the **Status** tab and for **Deleted**, review the additional information in parentheses, and take the indicated action.

- (**Processing**) means that the process has started and is in progress.
- (**Pending**) means that the deletion process has started from a client application. The deletion might be in progress or might have failed. Because the process was started from a client application, the server cannot accurately report the status of the deletion.

If a project deletion remains pending for a long time, try to delete the project again from the administration console.

- (**Failed**) means that the deletion process started but did not successfully finish. The log file contains specific information about the failure.

Review the information about the failure, and then try to delete the project again.

If partial data remains, you can also use the [TFSDeleteProject](#) command line tool.

Restore a project

7/8/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

You can restore a deleted project up to 28 days after it was deleted. This article shows you how.

Prerequisites

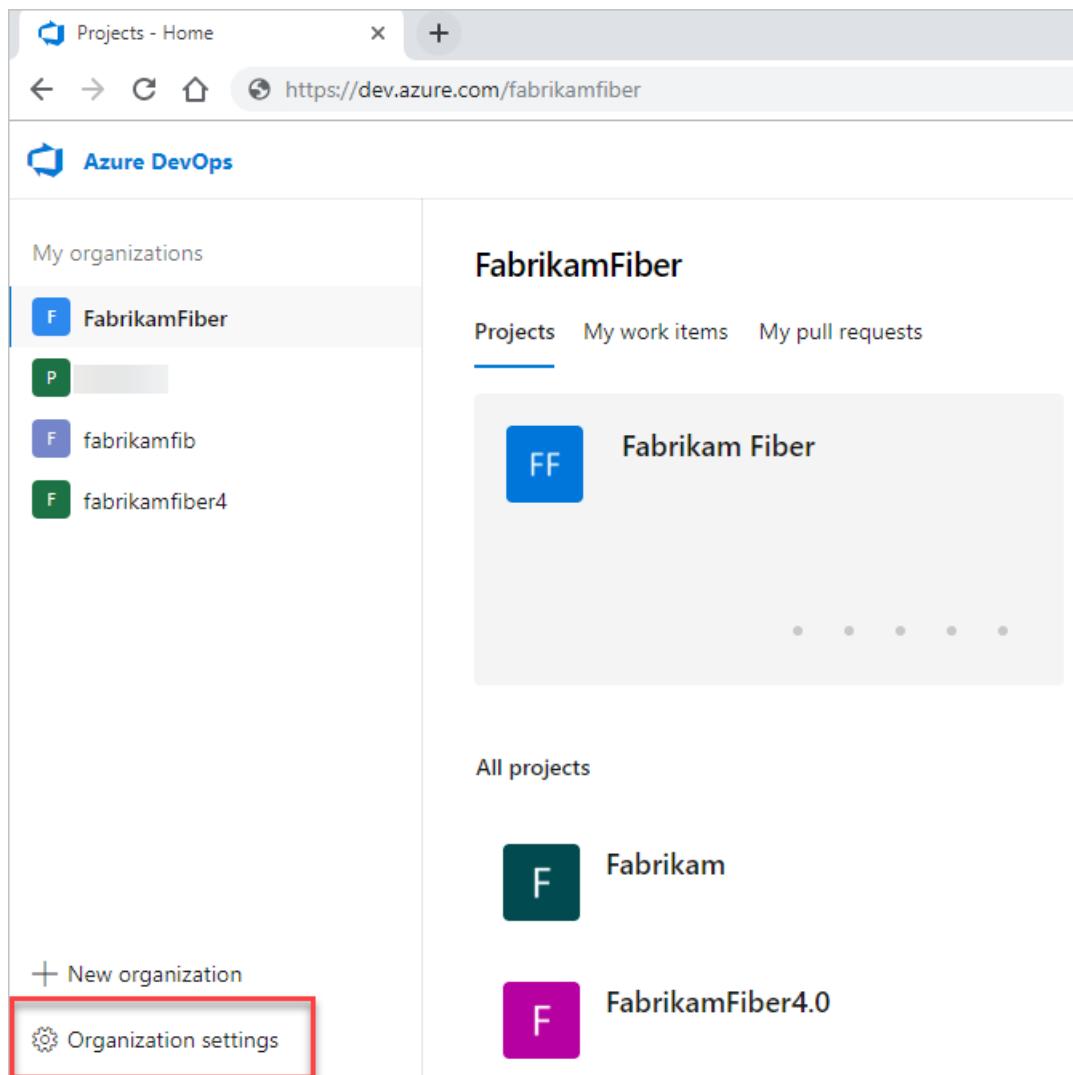
To restore a project, you must have the "delete project" permission set to **Allow**. To learn how to check your permissions, see [View permissions](#).

NOTE

A recently deleted project is only viewable when there is a project that has been deleted from an organization within the last 28 days.

Restore project

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



3. Select **Overview** and scroll down to "recently deleted projects."

My organizations

- fabrikam-fiber**
- fabrikamfiber3**

Related pages

- [What's new in DevOps](#)
- [Documentation](#)
- [Get help](#)

+ New organization

Organization settings

Organization Settings >

General

- Overview**
- Projects
- Policy
- Users
- Security
- Notifications
- Extensions
- Usage

Boards

- Process

Pipelines

- Agent pools
- Deployment pools
- Retention and parallel jobs

OAuth configurations

4. Highlight the project you want to restore, and then select **Restore**.

Recently deleted projects

Restoring a deleted project will recover all project artifacts including work items, repos, teams, and builds. Projects that appear here will be permanently deleted after 28 days.

- DP project
- F Fabrikam

Restore

Your project and associated data are restored.

Related articles

- [Save project data](#)
- [Create a project](#)

Turn a service on or off

5/24/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019

You can control which services are available through the web portal by turning a service on or off. Turning a service off removes the service from the user interface for all project users. However, data defined for the service is preserved and available if you later decide to turn the service on.

Prerequisites

- You must have an organization in Azure DevOps. If you don't have one, [do that now](#).
- As an organization owner or member of the Project Administrators group, you can change policies and change project information. If you're not a [member get added as one](#).
- You must have a project defined. If you don't have one, [add one now](#).
- As a member of the Project Administrators group, you can change policies and change project information. If you're not a [member get added as one](#).
-

Change the visibility for a service

1. a. Sign in to your organization (<https://dev.azure.com/{yourorganization}>) and select a project.
2. Choose **Project settings** in the sidebar.

Fabrikam / FabrikamFiber / Overview / Summary

FabrikamFiber

Private [Invite](#)

Welcome to the project!

What service would you like to start with?

Boards Repos Pipelines

Test Plans Artifacts

or manage your services

[Project settings](#)

3. Select **Overview**, and then choose the slider for the service that you want to enable or disable.

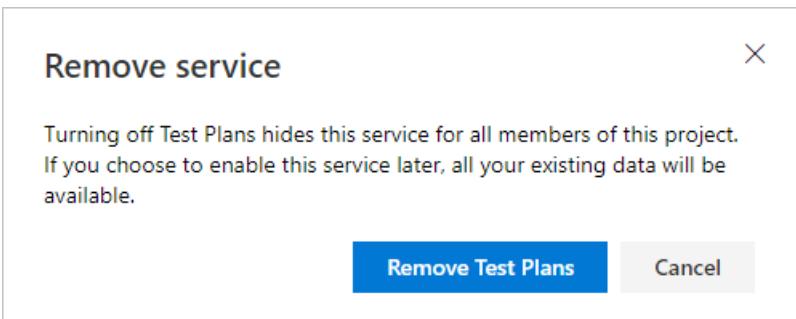
Project Settings > Overview

General

Azure DevOps services

Service	Description	Status
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

4. Confirm that you want to disable the service.



5. Refresh your web browser to view the updates.

Disabled objects and features

If you disable a service, dashboard widgets specific to that service are disabled. For example, if **Boards** is disabled, all work item tracking widgets and all Analytics widgets are disabled and won't appear in the [widget catalog](#).

If you disable **Boards**, you also disable [Analytics views](#).

Related articles

- [About projects and scaling the organization](#)
- [Change the project visibility, public or private](#)
- [About user, team, project, and organization-level settings](#)
- [About projects and scaling the organization](#)
- [About user, team, project, and collection-level settings](#)

Quickstart: Change the project visibility, public or private

6/21/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services - Public Projects

In this quickstart, you learn how to change the visibility of your project to and from public or private. You can easily switch a private project to a public project, and vice-versa. Before you do so, review the notes provided in [Private-to-public migration checklist](#).

TIP

Look through our [migration checklist](#) before you make an existing project public. It has tips and ideas for exposing a limited set of data, in case you don't want your entire history available.

Prerequisites

- You must have an organization created in Azure DevOps. If you don't have one, [do that now](#).
- As an organization owner, you can change policies and change project information. If you're not the owner, then you must be [a member of the Project Collection Administrators Group](#).

Enable anonymous access to projects for your organization

Before you can change a private project, to a public project, you must enable anonymous access for your organization.

1. From your web browser, sign-in to Azure DevOps. You must be signed in to create a public project.
2. Choose the  Azure DevOps logo to open **Projects**. Then choose **Admin settings**.

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with icons for "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are links for "New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main area is titled "FabrikamFiber" and shows a card for "Fabrikam Fiber" with a blue icon and a "FF" logo. Below it are cards for "All projects", "Fabrikam" (with a teal icon and a white "F"), and "FabrikamFiber4.0" (with a magenta icon and a white "F").

3. Choose the **Policy** page, and select **On** for **Allow public projects**.

The screenshot shows the "Organization Settings > Policy" page. The left sidebar has sections: General (selected), Overview, Projects, **Policy** (selected and highlighted with a red box), Users, Security, Notifications, Extensions, and Usage. The main content area is titled "Policy" and contains two sections: "Application connection policies" and "Security policies". Under "Application connection policies", there are three items: "Alternate authentication credentials" (set to "On"), "Third-party application access via OAuth" (set to "On"), and "SSH authentication" (set to "On"). Under "Security policies", there are two items: "External guest access" (set to "On") and "Allow public projects" (set to "On", also highlighted with a red box).

Make a private project public

1. Choose **Project Settings** in the sidebar.

The screenshot shows the Azure DevOps interface for a project named 'MyFirstProject'. On the left, a sidebar lists various project management features like Overview, Summary, Dashboards, Analytics views, Wiki, Boards, Repos, Pipelines, Test Plans, and Project settings. The 'Project settings' option is highlighted with a red box. The main content area displays the project name 'MyFirstProject' with a yellow star icon, a placeholder 'Briefly describe your project...', and a 'Get started with your new project!' message. Below this, there's a section for cloning the repository, showing 'HTTPS' and 'SSH' URLs, a 'Generate Git credentials' button, and a 'Clone in Visual Studio' link. A note provides instructions for authentication issues. Two dropdown menus show options for pushing existing repositories or importing new ones.

2. Choose **Overview**, and then **Edit** for **Privacy**.

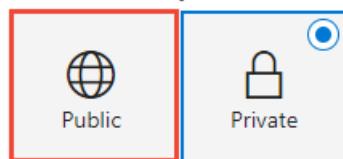
The screenshot shows the 'Project Settings' page for 'MyFirstProject'. The left sidebar has sections for General (with 'Overview' highlighted by a red box) and Work (with 'Project configuration' and 'Team configuration'). The main area is titled 'Project details' with a note that changes will affect all members and URLs. It shows a large pink square with a white 'M'. Under 'Project details', there are fields for 'Name' (MyFirstProject) with a 'Rename' button, 'Description' (empty), and 'Visibility' (set to 'Private'). The 'Edit' button for visibility is also highlighted with a red box.

3. To switch from private to public, choose the **Public** icon.

X

Change project visibility

Select visibility



(i) Only people you give access to will be able to view the project

Change

Cancel

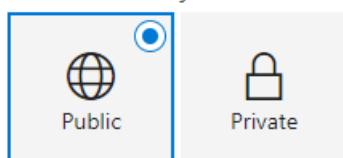
≡

4. Review the information provided, and choose **Change** to confirm your action.

X

Change project visibility

Select visibility



⚠ Anyone on the internet can view the project

Here are a few important things to note:

- TFVC is not supported for project non-members.
- Committer email addresses will be available when Git repositories are cloned.
- Some parts of agile and analytics are not available for non-members.
- Builds will run with project scope regardless of their setting.
- Work item links to files, branches, and wiki pages in other projects have the artifact name mentioned in the link itself.

[Learn more about public projects](#)

By continuing, you agree to the VSTS [code of conduct](#)

Change

Cancel

≡

Make a public project private

1. Choose **Project Settings**.

The screenshot shows the Azure DevOps interface for a project named 'MyFirstProject'. On the left, there's a sidebar with various project management options like Overview, Summary, Dashboards, Analytics views, Wiki, Boards, Repos, Pipelines, Test Plans, and Project settings. The 'Project settings' option is highlighted with a red box. The main content area has a large 'M' icon and the title 'MyFirstProject'. Below the title, there's a section titled 'About this project' with a link to 'MyFirstProject / README.md'. The 'Introduction' section is present but contains placeholder text. The 'Getting Started' section also has placeholder text and a numbered list of 4 items: 1. Installation process, 2. Software dependencies, 3. Latest releases, 4. API references.

2. Choose **Overview** page, and then **Edit** for **Privacy**.

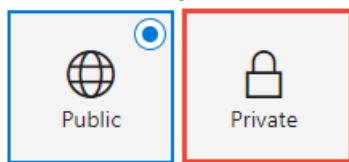
The screenshot shows the 'Project Settings' page for 'MyFirstProject'. The left sidebar lists General (with 'Overview' selected and highlighted by a red box), Services, Teams, Security, Notifications, Service hooks, and Dashboards. Under the 'Work' section, there are Project configuration and Team configuration options. The main content area is titled 'Project details' with a note that changes will affect all members and URLs. It features a large 'M' icon. The 'Name' field is set to 'MyFirstProject' with a 'Rename' button. The 'Description' field is empty. The 'Visibility' section shows 'Private' and an 'Edit' button, which is also highlighted with a red box.

3. To switch from public to private, choose the **Private** icon.

X

Change project visibility

Select visibility



⚠ Anyone on the internet can view the project

Here are a few important things to note:

- TFVC is not supported for project non-members.
- Committer email addresses will be available when Git repositories are cloned.
- Some parts of agile and analytics are not available for non-members.
- Builds will run with project scope regardless of their setting.
- Work item links to files, branches, and wiki pages in other projects have the artifact name mentioned in the link itself.

[Learn more about public projects](#)

By continuing, you agree to the VSTS [code of conduct](#)

[Change](#)

[Cancel](#)

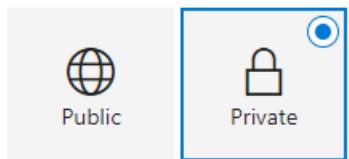
≡

4. Choose **Change** to confirm your action.

X

Change project visibility

Select visibility



ⓘ Only people you give access to will be able to view the project

[Change](#)

[Cancel](#)

≡

Next steps

[Download code](#)

Save project data

7/8/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

When you delete a project, you cannot recover its data later. Therefore, you should save project data.

You can use the following procedures to save data that users most care about, such as source code, build data, and work items.

- **Source code and custom build templates:** You can download your files as a zip file. Open the actions icon for the repository, file, or folder and choose **Download as Zip**. You can also choose the **Download** icon at the right side of the screen to download either all of the files in the currently selected folder, or the currently selected file.

The screenshot shows the Azure DevOps Services interface for the 'PublicProject' repository. The 'Contents' tab is selected. A red box highlights the 'Download as Zip' button next to the 'Calculator' folder. Another red box highlights the 'Download' icon in the top right corner.

The screenshot shows the Visual Studio Online interface for the '\$/FabrikamTFVC' repository. The 'Explorer' tab is selected. A red box highlights the 'Download as Zip' button in the context menu for the 'Main' folder.

This process doesn't save any change history or links to other artifacts.

If you use Git, [clone your repositories](#) to retain the full project history and all the branches.

- **Build data:** To save logs and data in your drop build folders, see [View build results](#).
- **Work item tracking data:** Create a work item query and open it [using Excel](#). Save the Excel spreadsheet.

This process doesn't save any attachments, change history, or links to other artifacts.

To learn more about how we manage and protect your data, read our [Data Protection Overview](#).

You can easily save data stored for a project collection by [making a backup of the database](#). You can also use the same steps as above.

Quickstart: Connect to a project in Azure DevOps

6/21/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In this quickstart, you learn how to connect to a project in order to share code, build apps, track work, and collaborate with team members, from one of the following clients:

- [Web portal](#)
- [Visual Studio or Team Explorer](#)
- [Eclipse/Team Explorer Everywhere](#)
- [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. Within that collection, one or more projects may be defined. At a minimum, at least one project must be created in order to use the system. For more information, see [About projects and scaling your organization](#).

Prerequisites

- If you don't have a project yet, [create one](#). If you need to add a team, see [Add teams](#). If you don't have access to the project, [get invited to the team](#).
- From each of these clients, you can quickly switch context to a different project and connect under a different sign-in user name. If you work remotely, configure your client to [connect to a TFS Proxy server](#).
- To get started with a code base, [set up Git](#) or [set up TFVC](#).

Connect from the web portal

1. If you're not a member of a security group, ask your project administrator to add you.
2. Open a browser window and enter a URL that uses the following form:

```
https://dev.azure.com/OrganizationName/ProjectName
```

```
http://ServerName:8080/tfs/DefaultCollection/ProjectName
```

For example, to connect to the server named **FabrikamPrime**, type: <http://FabrikamPrime:8080/tfs/>.

The default Port is 8080. Specify the port number and directory for your server if defaults aren't used.

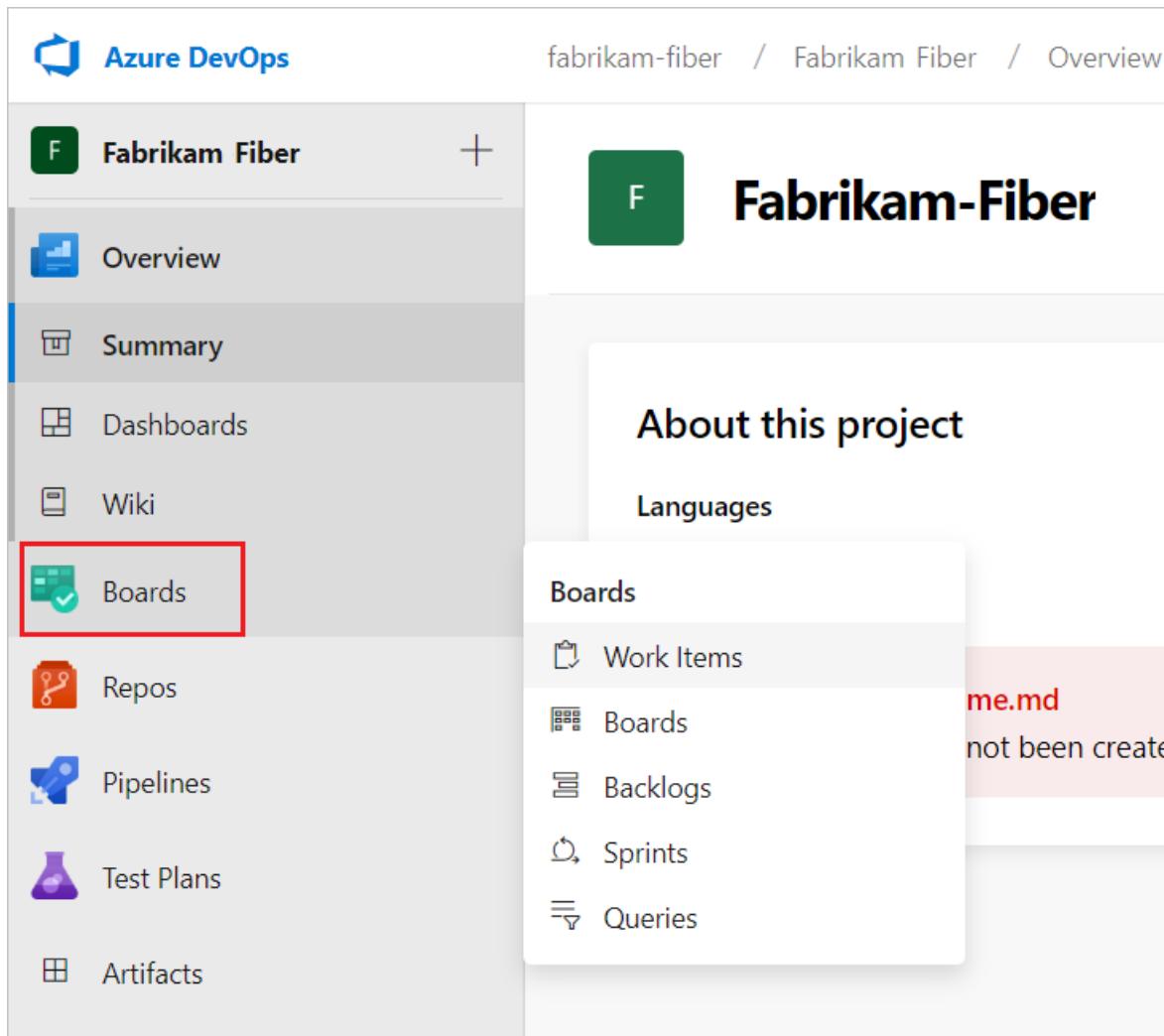
3. When you access the server for the first time, a Windows Identity dialog box appears. Fill in your credentials and choose the **OK** button.

TIP

If you select the **Remember me** check box you won't have to enter your credentials the next time you connect.

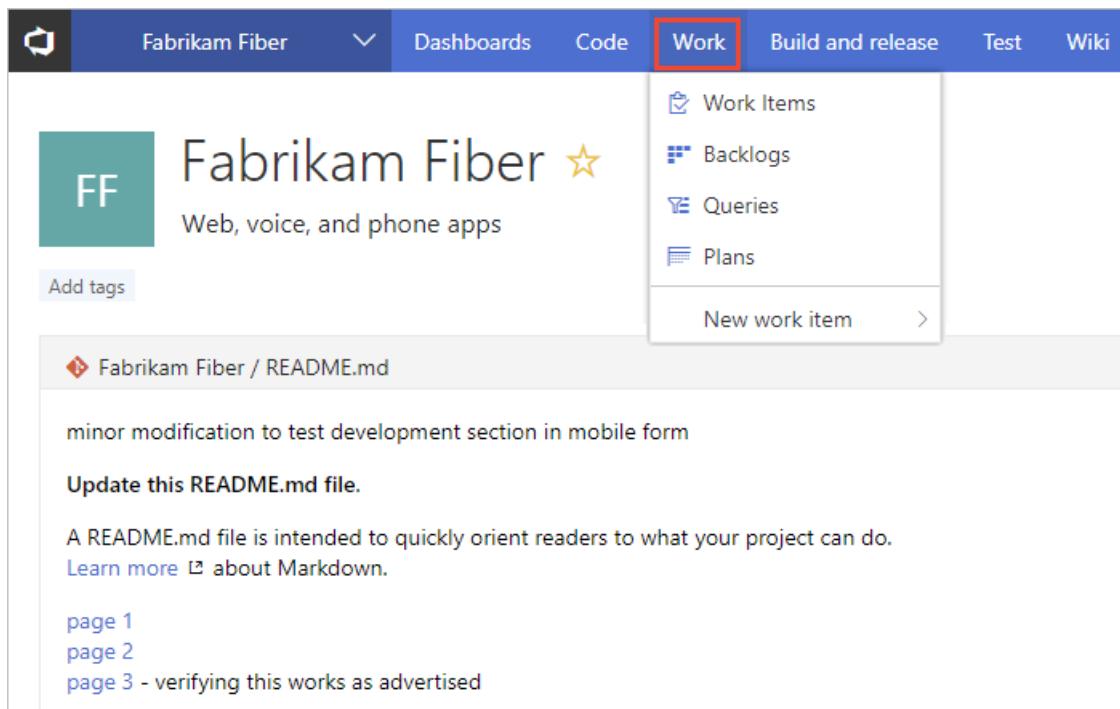
4. Choose your project, team, or page of interest.

From the project summary page, hover over a service and then choose the desired page. To choose another project, choose the  Azure DevOps logo.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, there's a sidebar with various navigation links: Overview, Summary, Dashboards, Wiki, Boards (which is highlighted with a red box), Repos, Pipelines, Test Plans, and Artifacts. The main content area is titled 'Fabrikam-Fiber' and has a section titled 'About this project'. Below it, there's a 'Languages' section and a 'Boards' section. A tooltip for the 'Boards' link in the sidebar lists five options: 'Work Items', 'Boards', 'Backlogs', 'Sprints', and 'Queries'. The 'Boards' option is highlighted in the tooltip.

From the project summary page, hover over a service and then choose the desired page. To choose another project, choose the  Azure DevOps logo.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. At the top, there's a navigation bar with tabs: Dashboards, Code, Work (which is highlighted with a red box), Build and release, Test, and Wiki. The main content area features the 'Fabrikam Fiber' logo and a star icon. Below it, there's a 'Web, voice, and phone apps' section and a 'Add tags' button. A tooltip for the 'Work' tab lists four options: 'Work Items', 'Backlogs', 'Queries', and 'Plans'. The 'Work Items' option is highlighted in the tooltip. The main content area also includes a 'README.md' file section with a link to 'Fabrikam Fiber / README.md' and some text about modifying the file.

Choose your project or team from the set of available links, or choose Browse to access all projects and teams.

The screenshot shows the 'Overview' tab selected in the top navigation bar. Below it, the 'Rooms' tab is visible. The main content area is titled 'About Team Foundation Server' and contains four purple cards: 'Features' (What does Team Foundation Server have to offer?), 'Learn' (Access online help for Team Foundation Server), 'Get Visual Studio' (View all the download options), and 'Administer' (Manage projects, users, groups and permissions). Below this, there are two sections: 'Recent projects & teams' and 'Recent team rooms'. The 'Recent projects & teams' section lists four items: 'Fabrikam Fiber / Web Service' (2 minutes ago), 'Fabrikam Fiber' (21 hours ago), 'Fabrikam Fiber / Migrate' (5/27/2016), and 'Fabrikam Fiber / Fiber Suite' (2/3/2016). The 'Recent team rooms' section shows one room: 'Fabrikam Fiber Team Room' with 0 users in room.

To learn more about each page and the tasks you can perform, see [Web portal navigation](#).

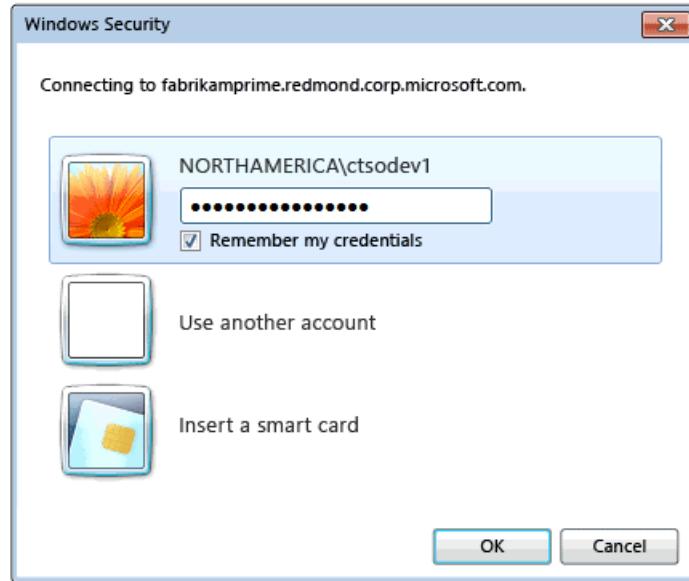
Sign in with different credentials

1. Open Windows Security from the context menu associated with your name.

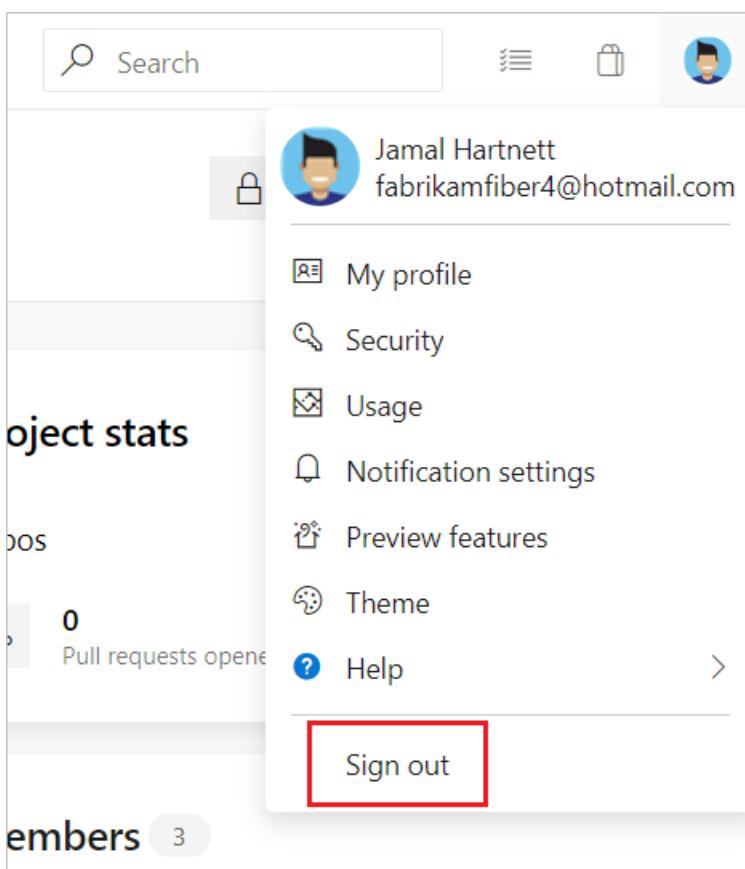
The screenshot shows the 'Overview' tab selected in the top navigation bar. The right side of the screen features a user profile for 'Raisa Pokrovskaya' with a blue profile picture. A dropdown menu is open, showing 'My profile', 'My alerts', and a highlighted 'Sign in as...' option. Below the dropdown, the text 'NORTHAMERICA\ctsodev1' is displayed. On the left, there are sections for 'Visual Studio' (with 'Open in Visual Studio' and 'Get Visual Studio' buttons) and 'Bug' (with a 'Create' button).

2. Enter your credentials.

Sign In As...



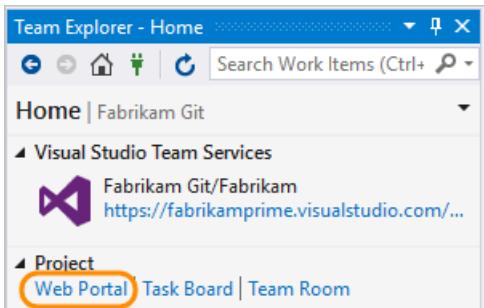
1. Open your profile menu and choose **Sign out**.



2. Choose Sign in and enter the new credentials.

Open the web portal from Team Explorer

- Open the web portal from the home page.

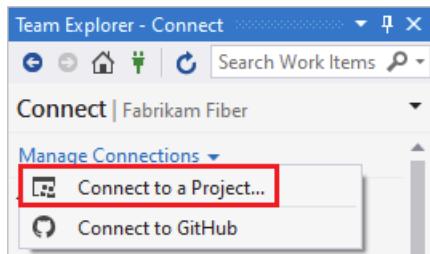


Connect from Visual Studio or Team Explorer

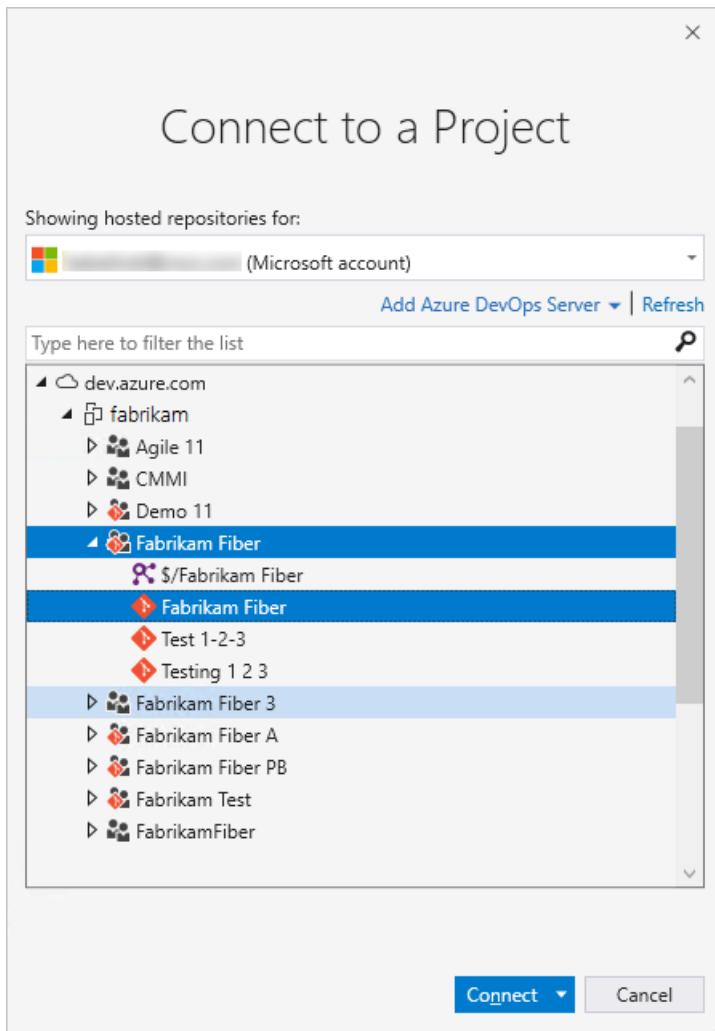
1. If you haven't already, [download and install a version of Visual Studio](#).
2. If you're not a member of an Azure DevOps security group, [get added to one](#).
3. Check with a team member to determine the names of the server, project collection, and project to connect to.
 - [Visual Studio 2019](#)
 - [Visual Studio 2017](#)
 - [Visual Studio 2015](#)

Visual Studio 2019

Select the connect icon in Team Explorer to open up the **Connect** page. Choose the **Connect to Team Project** link to select a project to connect to.



The **Connect to a Project** dialog appears and shows the projects you can connect to, along with the repos in those projects.



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



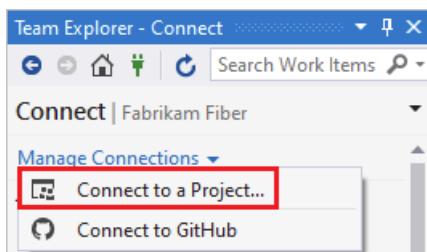
Select a project from the list and select **Connect**.

Change sign-in credentials

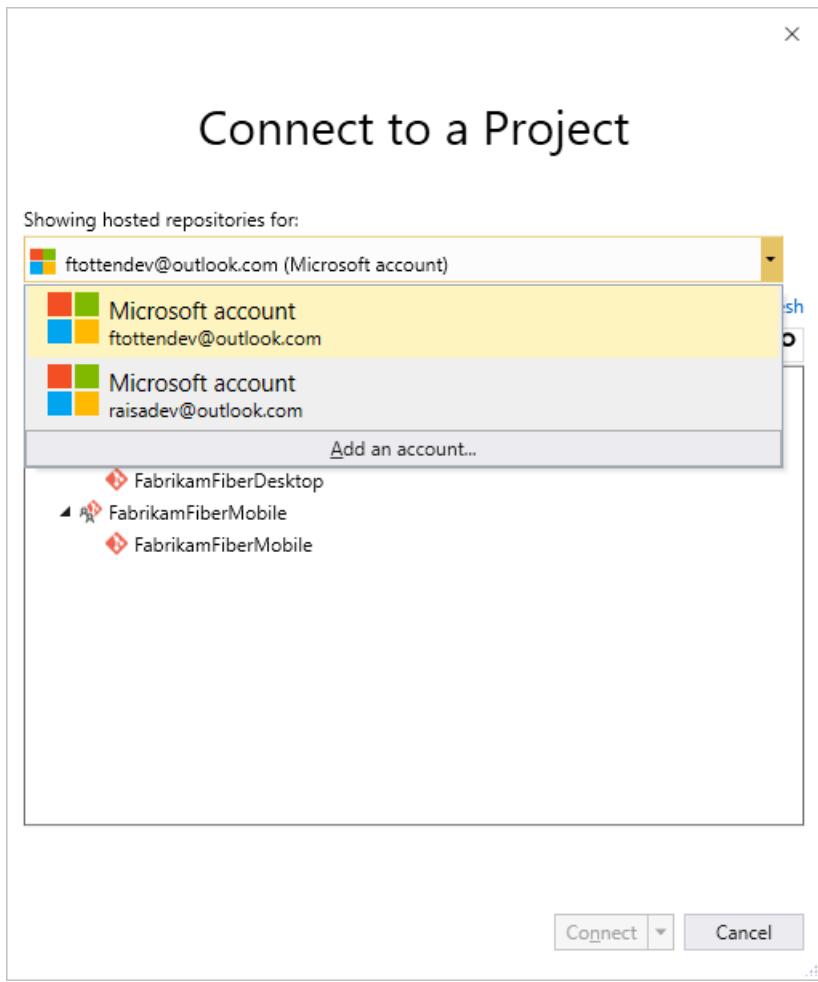
- [Visual Studio 2019](#)
- [Visual Studio 2017](#)
- [Visual Studio 2015](#)

Visual Studio 2019

1. From the Connect page, choose the **Connect to a Project** link to sign in with different credentials.

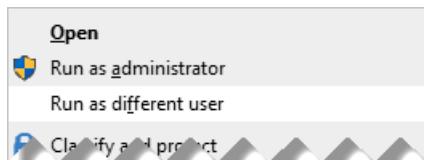


Select a different user from the drop-down or select **Add an account...** to access a project using different sign-in credentials.



- Sign in using an account that is associated with an Azure DevOps project, either a valid Microsoft account or GitHub account.

To run Visual Studio under sign-in credentials that are different from your signed-in Windows account, open the context menu for **devenv.exe** to access your run as options. If you don't see the **run as** option as shown in the following example, you may need to press SHIFT before right-clicking to see the run as options.



You can locate the executable in the following folder:

```
*Drive*:\\Program Files (x86)\\Microsoft Visual Studio xx.0\\Common7\\IDE\\
```

User accounts and licensing for Visual Studio

To connect to a project, you need your user account added to the project. This is typically done by the [organization owner \(Azure DevOps Services\)](#) or a [project administrator](#).

Azure DevOps Services provides access to the first 5 account users free. After that, you need to [pay for more users](#).

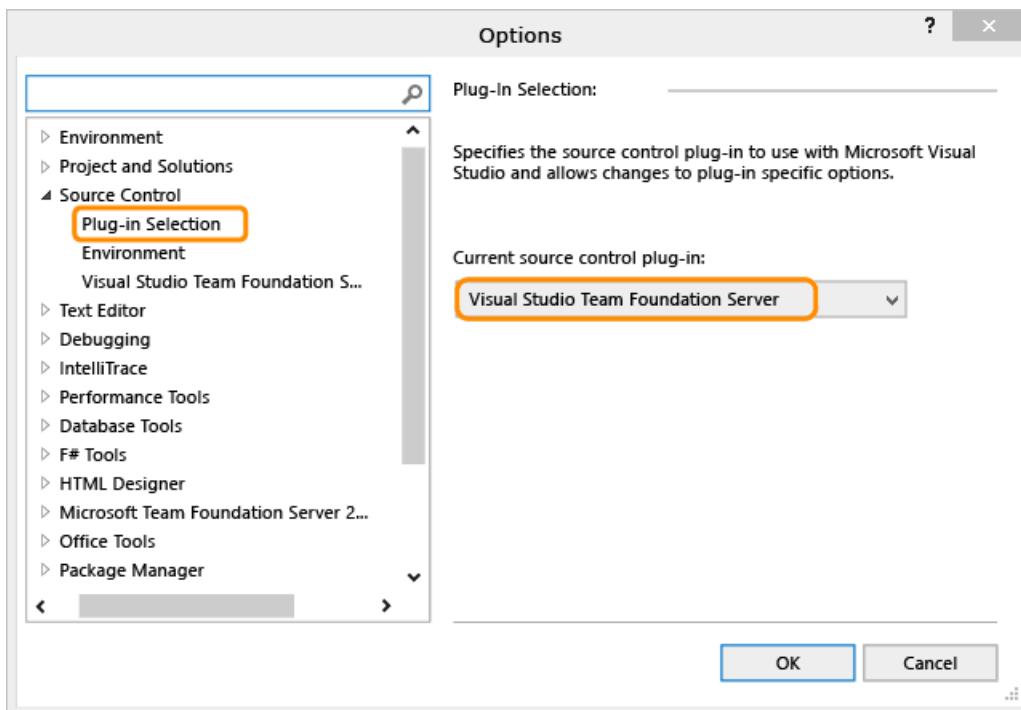
For on-premises TFS, each user account must have a TFS client access license (CAL). All Visual Studio subscriptions and paid Azure DevOps Services users include a TFS CAL. Find out more about licensing from the [Team Foundation Server pricing page](#).

In addition, you can provide access to Stakeholders in your organization who have limited access to select features as described in [Work as a Stakeholder](#).

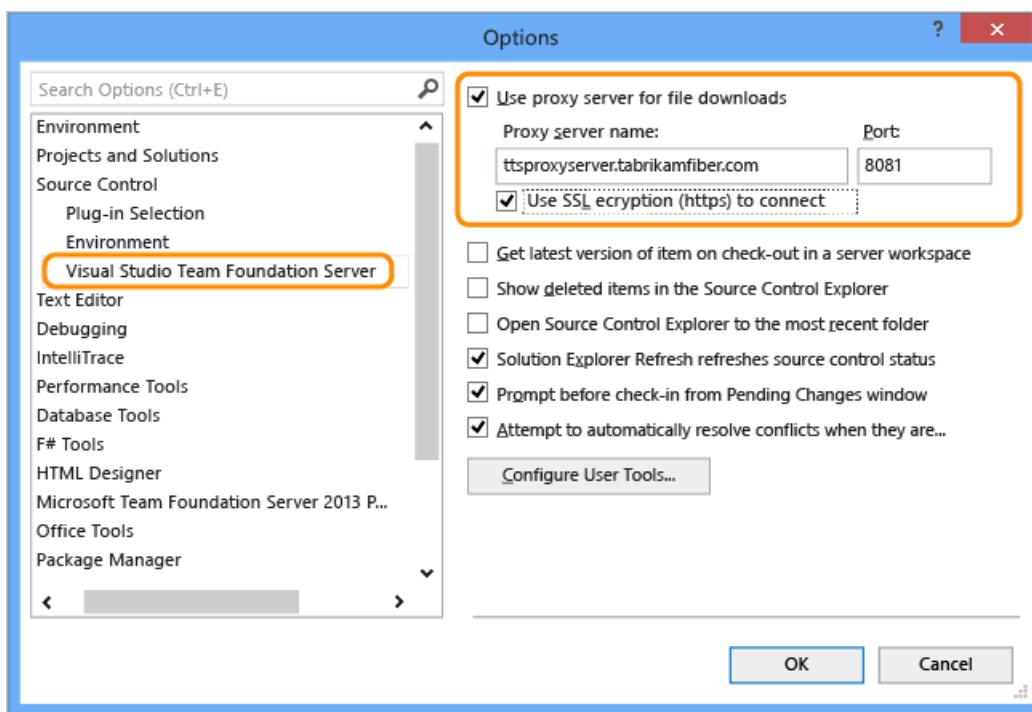
Configure Visual Studio to connect to TFS Proxy

If your remote team uses a [TFS 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. First, make sure that you have connected to TFS as described [in the previous section](#).
2. From the Visual Studio **Tools** menu, open the Options dialog and expand the Source Control folder. On the Plug-in Selection page, confirm that Visual Studio Team Foundation Server is selected.



3. On the Visual Studio Team Foundation Server page, enter the name and port number for the TFS Proxy server. Select the **Use SSL encryption (https) to connect** checkbox.



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

To **Configure User Tools** 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](#).

What other clients support connection to Azure DevOps?

In addition to connecting through a web browser, Visual Studio, Eclipse, Excel, and Project you can connect to a project from these clients:

- [Visual Studio Code](#)
- [Visual Studio Community](#)
- [Eclipse: Team Explorer Everywhere](#)
- [Azure Test Plans](#) (formerly Test Manager)
- [Microsoft Feedback Client](#)

Requirements and client compatibility

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

Determine your platform version

See [Feedback and support](#).

Next steps

Learn more about how to:

- [Work in web portal](#)
- [Work in Team Explorer](#)
- [Work in Office Excel or Project](#)
- [Troubleshoot connection](#)

If all you need is a code repository and bug tracking solution, then start with the [Git get started guide](#) and [Manage bugs](#).

To start planning and tracking work, see [Get started with Agile tools to plan and track work](#).

Troubleshoot creating a project

5/24/2019 • 3 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#) ↗

Resolve errors

To resolve permission related errors

If you receive an error message that states you don't have permission, go get those permissions: become a member of the [Project Collection Administrators group](#).

If you receive an error message that states you don't have permission, go get those permissions: become a member of the [Project Collection Administrators group](#) and the [Team Foundation Content Managers group](#).

If you receive an error message that states you don't have permission, go get those permissions: become a member of the [Project Collection Administrators group](#), the [Team Foundation Content Managers group](#), and gain [Full Control permissions](#) on the server that hosts SharePoint Products.

To resolve Error TF30169

Error TF30169: The New Team Project Wizard was unable to download the process template {0} indicates that SharePoint site process templates aren't available on the server that hosts SharePoint products.

Contact the system administrator for the server that hosts SharePoint Products and request the required process templates be added to the server. See [Requirements and compatibility](#).

To resolve Error TF30321

Error TF30321: The name you entered is already used for another project on the Team Foundation Server indicates that you should use a different name for your project. The name you entered is either in active use or has undergone partial deletion, but not full deletion.

Even when you've deleted a project, you may get the same name error. If a project create or delete operation doesn't successfully finish, some components could be created or deleted even though others aren't. In this event, you can't reuse the name associated with the project.

To verify project deletion or remove remaining components associated with a partially deleted project, use the [Delete project command line tool\(TFSDeleteProject\)](#). Then try again to create the project with the same name.

Even with troubleshooting, you might not be able to use the same name. Some components of the deleted project could be scheduled for deletion but not yet deleted.

To resolve an error message related to a plug-in

The process template used to create the project contains several XML plug-in files. If one of these files contains a format or other error, an error message appears.

Review the project creation log to determine the plug-in that caused the error. After you discover the problem, you can either contact the developer or vendor that provided the plug-in, or attempt to fix the problem yourself. For more information, see [Customize a process template](#).

To resolve a problem connecting to a server

If you receive an error message about a problem connecting to a server, retrieving information from a server, or checking permissions to create projects, it could be caused by an incorrectly configured server in the deployment. This problem is especially common after a server move, failover, or other maintenance activity.

Contact the TFS system administrator and request that they verify the server configuration.

Q & A

Q: How do I add my custom process template to the list?

A: You'll need to first [upload your template](#) using the Process Template Manager. To learn more about customizing a process template, go [here](#).

Q: Where is the log file located?

A: The log file is stored in `$:\Users\user name\AppData\Local\Temp` and labeled `vso_TeamProjectCreation_yyyy_mm_dd_ss.log`.

The log shows each action taken by the wizard at the time of the failure and may include additional details about the error. You can review the log entries to find network or file related issues by searching for **Exception** or **Error**.

Q: How do I delete a project?

A: You can delete a project that you no longer use, which helps simplify the navigation to projects that are in use. See [Delete a project](#).

Q: How do I add SQL Server Reporting or SharePoint portal resources?

A: See [Add reports to a project](#).

Q: How do I add SharePoint portal resources?

A: See one of these topics:

- To add a SharePoint web application: [Add SharePoint products to your deployment](#).
- To configure a project portal to use an existing website or SharePoint site: [Configure a project portal](#).

Q: Where can I go if I have more questions?

A: You can post a question or search for answers in our [Developer Community](#), [Stack Overflow](#), or through our [Support](#) portal.

Troubleshoot renaming a project

1/25/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

Q: What permission do I need to rename a project?

If you're using Azure DevOps Services or Team Foundation Server 2017 or later version, project rename requires the **Rename project** permission for a project. If you're using Team Foundation Server 2015, users require **Edit project-level information** permission on a project to rename it. To learn more, see [Add administrators, set permissions at the project-level or project collection-level](#)

Q: Can I use a project name again?

Yes, project names can be reused.

Q: Why did my attempt to reuse a project name fail due to existing work spaces?

A project name can't be reused if there are still workspace mappings addressing it. This is done to avoid the ambiguity case where a workspace could be mapped to two projects. You need to reach out to the users that have these mappings, and either delete them or [update them](#) to use the new name. If the user's machine containing the workspace is no longer available then you can delete the workspace by running the following command from Visual Studio's developer command prompt:

```
tf workspace /delete [/collection:TeamProjectCollectionUrl] workspacename[;workspaceowner]
```

Q: How does renaming a project impact my browser navigation experience?

After a project is renamed, any browsers with the project opened may encounter some errors. These errors are due to caches held by the browser which include the old project name. Refreshing makes these errors go away since the cache is repopulated with the new project name.

Q: Do other artifacts in the project get renamed when it is renamed?

Yes, all artifacts which share the same name get renamed along with the project. The only exceptions to this are for the default team and repo. The rename of these artifacts is performed as a best effort. For example, if a project *Foo* was renamed to *Bar*, the default team *Foo* would not be renamed if a team named *Bar* already existed in the project.

Yes, all artifacts which share the same name get renamed along with the project. The only exceptions to this are for the default team room, team, and repo. The rename of these artifacts is performed as a best effort. For example, if a project *Foo* was renamed to *Bar*, the default team *Foo* would not be renamed if a team named *Bar* already existed in the project.

Q: Why can't I open queries saved to a disk after a rename?

If you use Visual Studio 2010 and you have queries save to disk, you can't open them after a project is renamed. You can use Visual Studio 2012 or newer to open them.

Q: Why does the existing Lab Management BDT in Visual Studio fail with the error 'old projectName' cannot be found?

This issue is encountered when Build Controller 2013 is used with TFS 2015. To fix the issue, open the existing build pipeline, select the process tab under it, select the ellipses next to the Lab Process settings to open the Lab Workflow Parameters wizard, and then select **Finish**. The issue is permanently resolved by using the TFS 2015 Build Controller that ships with TFS 2015.

General
Trigger
⚠ Source Settings
Build Defaults
Process
Retention Policy

Team Foundation Build uses a build process template defined by a Windows Workflow (XAML) file. The template can be customized by setting the build process parameters provided by the selected template.

Build process template:
LabDefaultTemplate.11.xaml

Build process parameters:

1. Required	To see or edit the details, click ...	
Lab Process Settings		
2. Basic		
Build Number Format	\$(BuildDefinitionName)_\$(Date:yyyyMMMd)	
Logging Verbosity	Normal	
3. Misc		
Timeout For Each Deployment Script (in Minutes)	30	

Troubleshoot adding administrators to projects and project collections

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: When do I need to add someone to the project collection administrator role in Azure DevOps?

A: It varies. For most organizations that use Azure DevOps, project collection administrators manage the collections that members of the **Team Foundation Administrators** group create. Members of the **Project Collection Administrators** group don't create the collections themselves. Project collection administrators also perform many operations that are required to maintain the collection. Operations include creating team projects, adding users to groups, modifying the settings for the collection, and so on.

Q: What are the optimal permissions to administer a project collection across all of its components and dependencies?

A: Project collection administrators must be members of the following groups or have the following permissions:

- Team Foundation Server: A member of the **Project Collection Administrators** group, or have the appropriate **collection-level permissions** set to **Allow**.
- SharePoint Products: If the collection is configured with a site collection resource, then a member of the **Site Collection Administrators** group.
- Reporting Services: If the collection is configured with reporting resources, then a member of the **Team Foundation Content Manager** group.

Q: I'm an admin, but I don't have permission to add a project collection administrator. What do I need?

A: The following permissions are required:

- You must belong to the **Project Collection Administrators** group, or your **View Server-Level Information** and **Edit Server-Level Information** permissions must be set to **Allow**.
- To add permissions for SharePoint Products, you must be a member of the **Site Collection Administrators** or **Farm Administrators** groups for SharePoint Products.
- To add permissions for Reporting Services, you must be a member of the **Content Managers** or **Team Foundation Content Managers** groups for Reporting Services.

IMPORTANT

To perform administrative tasks like creating project collections, your user requires administrative permissions. The service account that the Team Foundation Background Job Agent uses must have certain permissions granted to it. For more information, see [Service accounts and dependencies in Team Foundation Server](#) and [Team Foundation Background Job Agent](#).

Q: Where can I find information about each individual permission?

A: You can find detailed information about individual permissions and their relationship to default security groups in the [Permission and groups reference](#). To give a user project administration permissions, complete the following steps:

1. From the team page, select the settings icon  to go to the team administration page.
2. Add the user to the **Project Administrators** group.

Troubleshoot setting up Visual Studio with Azure DevOps

1/31/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Visual Studio

Q: Why sign in?

A: Your Visual Studio settings, like automatic brace completion, are saved with your profile. These settings roam with your [personal Microsoft account](#), or your [work or school account](#), when you sign in to Visual Studio on any computer.

Sign in to Visual Studio during the 30-day trial period for these benefits:

- Visual Studio Enterprise: Extend your trial for 90 days. When your trial expires, learn [how to unlock Visual Studio](#).
- Visual Studio Express or Community: Continue to use this edition for free.

When you create your profile, you can also create an organization.

Learn more about [the benefits of signing in and creating a profile](#).

Q: Why can't I sign in?

A: To create a profile and save your settings, you'll need to sign in with a [personal Microsoft account](#) or a [work or school account](#) that's managed by Azure Active Directory.

Q: Which versions of Visual Studio can I use with Azure DevOps?

A: You can use:

- Visual Studio 2017
- Visual Studio 2015
- Visual Studio 2013
- Visual Studio 2012
- Visual Studio 2010, which requires [Service Pack 1](#) and [KB2662296](#)
- Visual Studio 2008 SP1, which requires a [GDR update](#)

To connect to Azure DevOps with Visual Studio 2008 through Visual Studio 2012:

1. Start Visual Studio.
2. From the **Team** menu or Team Explorer, go to **Connect to Team Foundation Server > Select Team Projects > Servers**.
3. Add your organization (`{yourorganization}.visualstudio.com`).
4. Select your project and finish connecting.

If you get connection errors, try choosing HTTPS as your protocol.

To connect to Azure DevOps with Visual Studio 2015 and later, learn [how to connect to team projects](#).

Q: Can I use Visual Studio 2015 with Visual Studio 2013 and 2012 on the same computer?

A: Yes, you can run all these versions on the same computer.

Q: My subscription expired. What do I do?

A: Here's [how to unlock Visual Studio](#). If you're having subscription problems, try [Subscription Support](#).

Q: I'm having problems installing or signing in to Visual Studio. How do I get help?

A: Learn more about:

- [Installing Visual Studio](#).
- [Signing in to Visual Studio](#).
- [Managing multiple user organizations](#).

Or contact [Visual Studio Support](#).

Azure DevOps Services

Q: How can I create an organization later?

A: Learn how to [sign up for Azure DevOps](#).

Q: Why won't my browser work with Azure DevOps?

A: This might happen if you're using an unsupported browser. For the best experience, make sure that you're using a [supported browser](#).

Q: Where can I find my organization name (URL)?

A: [Sign in to your Visual Studio profile](#) to find your organization list.

Q: What happens if I forget my password?

A: You can [recover your Microsoft account password](#) or [recover your work or school account password](#) if your organization turned on this feature. Otherwise, contact your Azure Active Directory administrator to recover your work or school account.

Q: Can I change my organization location?

A: Yes. For a better experience, you can change your organization's location during sign-up so that your organization is closest to most users.



Your organization's default location is selected based on the closest [Microsoft Azure region](#) where Azure DevOps is available.

Q: How do you store, secure, and protect my data?

A: Azure DevOps storage features help make sure that your data is available in case of hardware failure, service disruption, or datacenter disasters. Azure DevOps helps protect data from accidental or malicious deletion.

We follow industry best practices and have enterprise-grade security measures to help protect your code and project data. Also, all communication between your computer and the service takes place over an encrypted HTTPS connection. Learn [how your data is secured and protected](#).

Q: Do I still own my code and intellectual property? What do you do with my personal information?

A: Yes, your code and your intellectual property are yours. Please review our [terms of service](#) and [privacy policy](#).

Q: Where can I find the Azure DevOps SLA?

A: You can find it here: [Azure DevOps SLA](#).

Q: Can I change my organization name (URL) or owner?

A: Yes. If you have at least Basic access, you can do this in your organization settings. Learn how to:

- [Rename your organization](#).
- [Change the organization owner](#).

Q: Can I delete an organization that I don't need anymore?

A: Yes. See [Delete or recover your organization](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot connecting to a project

7/2/2019 • 4 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Troubleshoot connectivity

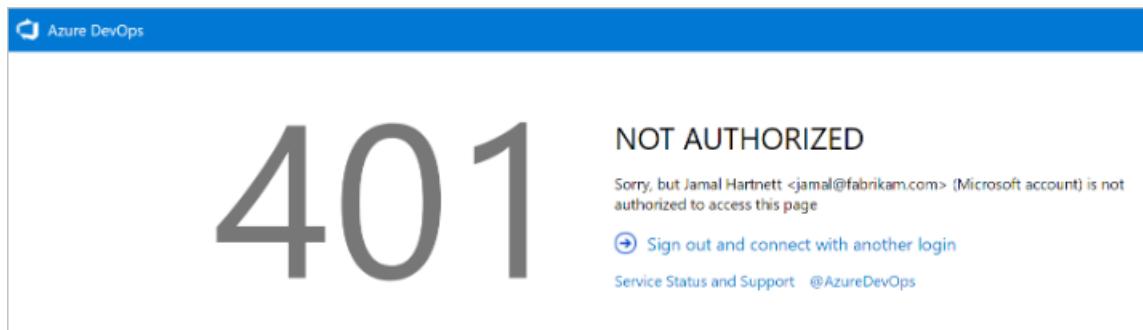
As a first step in resolving connectivity issues with Azure DevOps, complete the following steps:

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, press Ctrl+Shift+Del.
3. Open Internet Explorer and delete the browser cookies. The Visual Studio IDE uses Internet Explorer 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.

Troubleshoot signing in

Two types of identities can sign in: Microsoft accounts and Azure Active Directory (Azure AD) accounts. Depending on your account, you might experience one of the following errors.

401 - Not Authorized



The most common error page is the *401 Not Authorized* error, which occurs when your identity doesn't have permissions to enter an organization. Common reasons for the error include:

- Your identity isn't a member of the organization.
- Your identity has an invalid or missing license assignment.

If you think you're a member of the organization but are blocked by this error page, [contact customer support](#).

Scenario 1

Your work or school Azure AD 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 (Azure AD) that have the same sign-in address exist. You've 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. The work or school Azure AD account might have been created by an administrator when you were added to Office365 or Azure AD.

To sign out of your current work or school Azure AD 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.

TIP

To avoid seeing this prompt, you can rename your Microsoft account. Then, only one identity (your work or school account, or Azure AD account) uses your sign-in address.

Scenario 2

Your personal Microsoft account doesn't have access, but your Azure AD 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 (Azure AD identity) does. The same guidance from Scenario 1 applies, but in reverse.

401 - Work or school, or Personal account

401

NOT AUTHORIZED

[jamal@fabrikam.com](#) has multiple accounts associated with it.Your personal account does not have access to [dev.azure.com/Fabrikam](#), but **your work or school account does have access**.[Sign in with your work or school account](#)[Sign out and connect with another login](#)Service Status and Support [@AzureDevOps](#)**Mitigation**

If you enter your credentials correctly, but are redirected back to the original sign-in page, we recommend clearing all cookies, and then reattempting to sign in. If that doesn't fix the issue, contact customer support.

Troubleshoot TFS connectivity

Here's a list of the most frequently reported connection problems and what to do about them. Complete the list in the order indicated.

1. Verify that you have the required permissions.

If the errors that you receive indicate read-only or blocked actions, you might not have permissions to act on the data.

2. Verify that your computer is connected to the network and that it can access network resources.

3. Verify that TFS hasn't been taken offline. Talk with your TFS administrator.

4. Check whether your project has been moved to another project collection in TFS. If it has been moved, you must create a connection to the new server name.

For additional troubleshooting tips, see [TF31002: Unable to connect to this Team Foundation Server](#).

Switch organizations

When you use two or more organizations that are linked to Azure AD, such as organizations created in the Azure portal, 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 Team Foundation Server** dialog box:

TF31003: Either you have not entered the necessary credentials, or your user account does not have permission to connect to the Team Foundation Server

TF31002: Unable to connect to this Team Foundation 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 Online](#).

Connect to TFS with Secure Sockets Layer

If you connect to a TFS instance that has Secure Sockets Layer (SSL) configured, you must install a certificate and clear the client cache. For details, see [Set up HTTPS with Secure Sockets Layer \(SSL\) for TFS - Configuring client computers](#).

Clear the cache on client computers

When the on-premises TFS configuration changes, such as when you move or split a project collection, you may need to clear the cache.

1. Sign in to your client computer for TFS by using the credentials of the user whose cache you want to clear.
2. Close any open instances of Visual Studio.
3. Open a browser and go to one of the following folders, depending on the operating system that's running on your computer:
 - **Windows 10** *Drive:\Users< i >UserName\AppData\Local\Microsoft\Team Foundation\6.0\Cache*
 - **Windows 8** *Drive:\Users< i >UserName\AppData\Local\Microsoft\Team Foundation\4.0\Cache*
 - **Windows 7 or Windows Vista** *Drive:\Users< i >UserName\AppData\Local\Microsoft\Team*

Foundation\2.0\Cache

4. Delete the contents of the Cache directory, including all subfolders.

TF31002: Unable to connect

5/8/2019 • 5 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

You might receive this error when you try to connect to Azure DevOps Services or an on-premises Azure DevOps Server from Visual Studio.

You receive this error when you try to connect to Azure DevOps Services

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. See Assign licenses to users for details.
Your Azure DevOps Services organization is connected to the Azure Active Directory.	When your Azure DevOps Services organization is connected to a directory that is associated with an Office 365 or Microsoft Azure subscription, only members in the directory can access the account. Check with your directory administrator to have them create an organizational account for you or add your account to the directory as external member .
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, you see a flashing blank sign in dialog box several times. Then, you receive either TF31002 or TF31003 error after you connect to or add a new connection in "Connect to Team Foundation Server" dialog box. To resolve this problem, apply the most recent Visual Studio update . To learn more, see KB Article ID 2958966, You can't switch between different organizational accounts in Visual Studio Online .
You want to sign in to Azure DevOps Services from Visual Studio using different credentials.	See Connect to projects, Sign in with different credentials .

When you try to connect to an on-premises Azure DevOps Server from your client computer

If you determine that you're receiving this error from one computer but not others, or others aren't receiving this error, then check the problem resolutions that are outlined below.

PROBLEM	RESOLUTION
Your password has expired.	Verify that you entered your user ID and password correctly, and that your password hasn't expired.
You've entered an incorrect server URL.	Verify that you've entered the server URL correctly including the server name, port number, and protocol (http/https). See Connect to projects to learn more.
The TFS configuration has changed.	If the configuration for the on-premises Azure DevOps Server has changed, you must create a new connection. You might also need to clear the client cache .
You work remotely and need to connect to a TFS Proxy server to check in files to Team Foundation version control.	Configure Visual Studio to connect to TFS Proxy .
You're connecting to a later version of TFS than your Visual Studio client version.	Your version of Visual Studio or Team Explorer might be incompatible with Team Foundation Server. You might need to install one or more GDR packs. See Requirements and compatibility for details.
Your firewall is blocking TFS services.	See Allow a program to communicate through Windows Firewall .
Visual Studio stops responding when you run a query in Visual Studio.	Your computer might be configured to bypass the proxy server. Verify the configuration of the BypassProxyOnLocal setting on your computer. For more information, see BypassProxyOnLocal Configuration .

Several users can't connect to an on-premises Azure DevOps Server

If the problem occurs on more than one computer, contact your administrator to confirm whether the server is operational and available on the network.

As an administrator, check the event logs for the application-tier server to try to pinpoint the problem. Also, you can use the following table to determine whether the server is misconfigured. In the table, problems that are more likely to occur appear first. Try the resolutions in the order in which they appear, which increases the chance that you can solve the problem quickly.

PROBLEM	RESOLUTION
The <i>TFSService</i> account password has expired or is incorrect.	Many services for Team Foundation Server will stop running when the service account for Team Foundation has expired. For more information, see Change the service account or password for Team Foundation Server .
The application-tier server for Team Foundation is unavailable.	Verify whether each required service is running. If a required service isn't running, you must restart it. If necessary, set it to start automatically. For more information, see Stop and start services, application pools, and websites .
The network is unavailable.	Verify whether your network is operational.
A website identity for Team Foundation is configured incorrectly.	Verify or correct the server binding assignments that are made to websites for Team Foundation.

PROBLEM	RESOLUTION
Access to a website for Team Foundation has been restricted.	Verify or correct restrictions that are made to those websites that are based on IP addresses and domain names.
The firewall or ports are configured incorrectly.	Verify or correct port binding assignments for websites and port assignments for the firewall. First, you should open the administration console for Team Foundation, display the Application Tier page, and review the URL assignments. If necessary, you can click Change URL to modify the URL of a website. Next, you should verify the port assignments for Internet Information Services (IIS) and the ports that are allowed through the firewall. For more information, see Review Server Status and Settings and Verify or Correct Port Assignments .
Trust relationships between domains aren't configured correctly.	If a group of users can't access Team Foundation Server, you might have trust issues between domains.
When users connect to different versions of TFS from Visual Studio, for example, they connect to TFS 2012 and then TFS 2008, they can get the TF31002 error.	<p>This error can occur because the GUIDs for the TFS 2012 collection are the same as TFS 2008. The local client cache gets confused because it tries to maintain the same GUID-based local cache for both the 2008 server and the new Project Collection in 2012.</p> <p>To fix, run the TFSConfig ChangeServerID command. See TFSConfig ChangeServerID command.</p>

If the previous resolutions don't solve the problem, go to the [MSDN Forums - Visual Studio Team System —Team Foundation Server - Administration](#).

Manage organizations

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Sign up for an organization, add users, and manage permissions and access.

- [About managing organizations](#)
- [Access with Azure AD](#)

5-minute quickstarts

- [Create your organization or project collection](#)
- [Try Azure Test Plans for free](#)
- [Set permissions at the project or collection level](#)
- [Add a team admin](#)

Step-by-step tutorials

- [Change individual permissions](#)
- [Grant or restrict permissions](#)

Concepts

- [Plan your organizational structure in Azure DevOps](#)
- [Add more Basic users to organization](#)
- [Resources granted to project members](#)
- [Glossary](#)

How-to guides

- [Set your preferences](#)
- Manage your organization
 - [Change your organization owner](#)
 - [Rename your organization](#)
 - [Delete your organization](#)
 - [Recover your organization](#)
 - [Sign in with different credentials](#)
 - [Change organization location \(region\)](#)
 - [Add privacy policy URL](#)
- Manage access to your organization
 - [Add users to your organization](#)
 - [Manage users](#)
 - [Manage conditional access](#)
 - [Link work accounts to Visual Studio subscriptions](#)
 - [Authenticate with personal access tokens](#)
 - [Revoke user PATs - for admins](#)

- [Change app access policies](#)
- [Delete users](#)
- [Add external users](#)
- [Access with Azure AD](#)
 - [Add Azure AD group to Azure DevOps group](#)
 - [Add Azure DevOps users to Azure AD](#)
 - [Delete Azure DevOps users connected to Azure AD](#)
 - [Connect Azure DevOps to Azure Active Directory](#)
 - [Disconnect your organization from Azure AD](#)
 - [Change your Azure AD tenant connection](#)
- Manage extensions
 - [Install extensions](#)
 - [Approve requests for extensions](#)
 - [Uninstall or disable extensions](#)
- Manage group-based licensing
 - [Add a group rule to assign access levels and extensions](#)
 - [Remove direct assignments](#)

Reference

- [Permissions and access \(Security\)](#)
- [Permission lookup guide \(Security\)](#)
- [Permissions and groups reference \(Security\)](#)
- [Azure DevOps data protection overview](#)
- [Migrate from Azure DevOps Server to Azure DevOps Services](#)

Resources

- [Get started using Azure DevOps](#)
- [Marketplace & extensibility](#)

About organization management in Azure DevOps

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

With an organization, you gain access to the platform in which you can do the following:

- Collaborate with others to develop applications by using our cloud service.
- Plan and track your work as well as code defects and issues.
- Set up continuous integration and deployment.
- Integrate with other services by using service hooks.
- Obtain additional features and extensions.

Create your organization

Before you get started, read [Plan your organizational structure in Azure DevOps](#). Then, you can [create your organization](#) and invite others so they can access your organization.

Choose Git or Team Foundation Server as your version control, so that Azure DevOps can create your project for code and other assets, like builds, tests, and work items. If you're starting with Visual Studio as your development environment, you can create your organization when you [set up Visual Studio](#).

Your organization includes five free users with Basic access, plus unlimited Visual Studio subscribers and Stakeholders at no extra charge. Your organization also includes free monthly amounts of additional services such as build and deployment.

Connect to your organization

When your organization is created, [connect to your projects](#) with tools like Xcode, Eclipse, or Visual Studio, and add code to your project.

Some clients, like Xcode, Git, and NuGet, require basic credentials (a username and password) for you to access Azure DevOps. To connect these clients to Azure DevOps, create personal access tokens to authenticate your identity. Use a credential manager to create, store, and secure your tokens, so you don't have to reenter them every time you push. Or if you don't want to use a credential manager, you can [create personal access tokens manually](#).

Add users and assign access

To share work with others, [add users and assign access](#). That way, you control each user's access. Or [add users to your project](#), and let Azure DevOps assign the next available access to them.

Set up billing

If you need more than the free users and amounts of services included with your organization, [set up billing for your organization](#). You can then pay for more users with Basic access, buy more services, and purchase extensions for your organization.

Access with Azure AD

Azure DevOps works with Azure Active Directory (Azure AD), so that you can control access the same way that you do with Microsoft services like Office 365 and Microsoft Azure. If your enterprise uses a directory managed

by Azure AD, your organization can also [use your directory to authenticate access](#). Or [change your Azure AD instance](#), if you're already connected to an existing directory.

Access your organization with Azure Active Directory

4/5/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to authenticate users and control access to your organization the same way that you can with Microsoft services like Office 365 and Azure. If your organization was created with a Microsoft account, you can connect your organization to your [Azure Active Directory \(Azure AD\)](#). You can then sign in to Azure DevOps with the same username and password that you use with these Microsoft services. You can also enforce policies for accessing your team's critical resources and key assets.

To use existing on-premises identities with Azure DevOps, you can integrate directories with Azure AD by using [Azure AD Connect](#). To switch your organization to another directory, learn [how to change your directory in Azure AD](#).

How does Azure Active Directory control access to Azure DevOps?

Your organization authenticates users through your organization's directory so that only users who are members or guests in that directory can get access to your organization. When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials. Only specific [Azure AD administrators](#) can manage users in your directory, so they control who can get access to your organization.

Without Azure AD, you're solely responsible for controlling organization access. And all users must sign in with Microsoft accounts.

What do I need to set up an existing Azure DevOps instance with Azure AD?

You need the following:

- [Ownership of the organization](#) that you want to connect to Azure AD.
- A "full" [Azure subscription](#), such as a [Pay-As-You-Go subscription](#), associated with Azure Active Directory and at least co-administrator permissions for your subscription.

You need both to make your directory appear in the Azure portal, so that you can link your subscription and connect Azure AD to your organization. Learn about [Azure subscription co-administrator permissions](#).

[Want to use Office 365 Azure AD with Azure DevOps?](#)

- Global administrator permissions for your directory so you can add current Azure DevOps users to that directory.

Otherwise, work with your directory's global administrator to add users. Learn more about [Azure AD administrators](#).

To check your permissions, [sign in to the Azure portal](#) with your work or school account. Go to your directory.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with a 'Create a resource' button, 'All services', 'FAVORITES' (empty), 'Resource groups', and 'Azure Active Directory' (which is selected and highlighted with a red box). Below that are 'Dashboard', 'All resources', 'App Services', 'Function Apps', 'SQL databases', and 'Azure Cosmos DB'. The main content area has a header 'Fabrikam - Overview' under 'Azure Active Directory'. It features a 'Fabrikam' title, a 'Sign-ins' section (with a note that only global administrators, security administrators, security readers, and report readers can view sign-ins, and a 'More info' link), and a 'Find' section for users. A 'Your role' box on the right indicates 'Global administrator' with a 'More info' link, which is also highlighted with a red box.

You must add your Microsoft account to Azure AD.

Although directory membership isn't required to connect your organization to Azure AD, it makes sure that you can sign in and access your organization after you connect to Azure AD. Otherwise, your Microsoft account does not have access to your organization.

What happens to current users?

Your work in Azure DevOps is associated with your sign-in address. After your organization is connected to your directory, users continue working seamlessly if their sign-in addresses appear in the connected directory. If their sign-in addresses don't appear, you must [add those users to your directory](#). Your organization might have policies about adding users to the directory, so find out more first.

What if we can't use the same sign-in addresses?

You have to add these users to the directory with new work or school accounts. If they have existing work or school accounts, they can use those instead. Their work won't be lost and stays with their current sign-in addresses. You must add them as new users, reassign access levels, and readd them to any projects. Users can migrate work that they want to keep, except for their work history. Learn [how to manage organization users](#).

What happens to tools that use my credentials, like alternate credentials?

Alternate credentials won't work anymore for tools that run outside a web browser, like the Git command-line tool. You have to [set up your credentials](#) again for the organization that you connected.

What if I accidentally delete a user in Azure AD?

You should [restore the user](#), rather than create a new one. If you create a new user, even with the same email address, this user is not associated with the previous identity.

Manage organization access with Azure AD

- [Add Azure DevOps users to Azure AD](#)
- [Connect your organization to Azure AD](#)
- [Disconnect your organization from Azure AD](#)

- Delete users from Azure DevOps connected to Azure AD

Quickstart: Create an organization or project collection

6/21/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In this quickstart, you learn how to create an organization. An organization is used to connect groups of related projects, helping to scale up an enterprise. You can use a personal Microsoft account, GitHub account, or a work or school account. Use your work or school account to *automatically connect* your organization to your Azure Active Directory (Azure AD).

Prerequisites

1. Read and understand how to [Plan your organizational structure](#).
2. Complete the following steps if you want to use only Microsoft accounts with your organization.

Without Azure AD, you're solely responsible for controlling organization access. And all users must sign in with their Microsoft account. [What are other differences?](#)

- If you don't have a Microsoft account, you can create one when you sign up for Azure DevOps.
 - Use your Microsoft account if you don't need to authenticate users for an organization with [Azure AD](#). All users must sign in to your organization with a Microsoft account.
3. Complete the following steps if you want to authenticate users and control organization access through your Azure AD.
 - You need a work or school account that's managed by your Azure AD. If you use Azure or Office 365, you might have one already. If you don't, learn how to [sign up for Azure as an organization](#).
 - To use existing on-premises identities, see [use Azure AD Connect for integrating on-premises directories with Azure AD](#).
 - All users must be members in that directory to access your organization. To add users from other organizations, use [Azure AD B2B collaboration capabilities](#).

Create an organization

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

3. Confirm information, and then select **Continue**.

Congratulations, you're now an organization owner!

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

Create a project collection

A project collection is a container of projects. By grouping projects together, you can manage projects more efficiently and assign the same resources to them.

For more information about how to create a project collection, see [create a project collection](#).

Next steps

[Create a project](#)

Plan your organizational structure

5/24/2019 • 15 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Your business structure should act as a guide to 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 or collaborative work in Azure DevOps:

- [Quantity of organizations](#)
- [Quantity of projects under an organization](#)

You also may want to plan for the following scenarios:

- [Mapping your organizations and projects](#) in Azure DevOps to your enterprise, business unit, and team structure
- [Structuring your repositories \(repos\)](#)
- [Structuring your teams](#)- it can either help or hinder teams to be Agile and autonomous
- [Managing access to data](#) - who needs to have access and who doesn't?
- [Reporting needs](#)
- Promoting common practices - learn more about [foundational elements you need to create an agile mindset and culture](#).

You need to have at least one organization, which may represent your company, your larger collection of code projects, or even multiple related business units.

What is an organization?

An organization in Azure DevOps is a mechanism for organizing and connecting groups of related projects.

Examples are business divisions, regional divisions, or other enterprise structure. You can choose one organization for your entire company, or separate organizations for specific business units, or an organization just for you.

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 just 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 Kanban boards
- [Azure Repos](#): Unlimited private Git repos
- [Azure Artifacts](#): Package management
- Load testing (20,000 VUMs per month)
- Unlimited Stakeholders * Five Azure DevOps users (Basic) * Free tier of Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month) * 2GB of Azure Artifacts storage * One self-hosted CI/CD concurrent job * 20,000 virtual user minutes of cloud-based load testing

NOTE

The cloud-based load testing service is deprecated. More information about the deprecation, the service availability, and alternative services can be found [here](#).

How many organizations do you need?

When you're starting out with Azure DevOps, begin with one organization. Then, you can add additional organizations—which may require different security models—later. If you only have a single code repo or project, you don't need more than 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. Read further for more guidance for [mapping your projects to business units](#) and [structure considerations](#).

What is a team?

A team is a unit that supports many [team-configurable tools](#), which help you plan and manage work, and make collaboration easier.

Creating a team for each distinct product or feature team

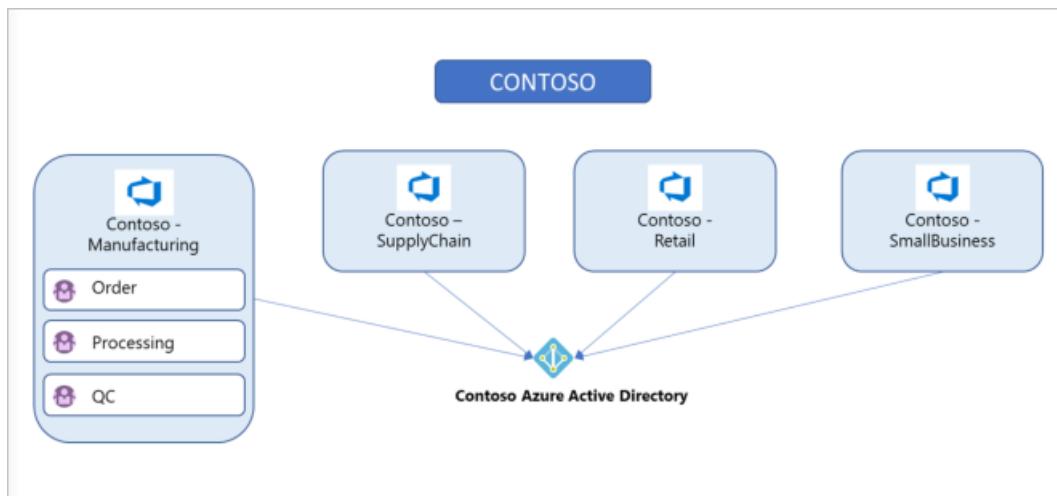
Every team owns their own backlog, to create a new backlog you create a new team. By [configuring teams and backlogs into a hierarchical structure](#), program owners can more easily track progress across teams, manage portfolios, and generate rollup data. A team group is created when you create a team. You can use this group in queries or to set permissions for your team.

What is 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 Contoso company has three projects within their Contoso-Manufacturing organization.



How many projects do you need?

You need 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 is 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 Azure AD tenant. A single Azure AD tenant can be connected to many Azure DevOps organizations.

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. A single project allows teams to 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 on each other 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, the 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

Project structure is best determined 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 is improved.

Azure DevOps provides cross-project experiences when it comes to managing work.

You may want to add another project because of 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:

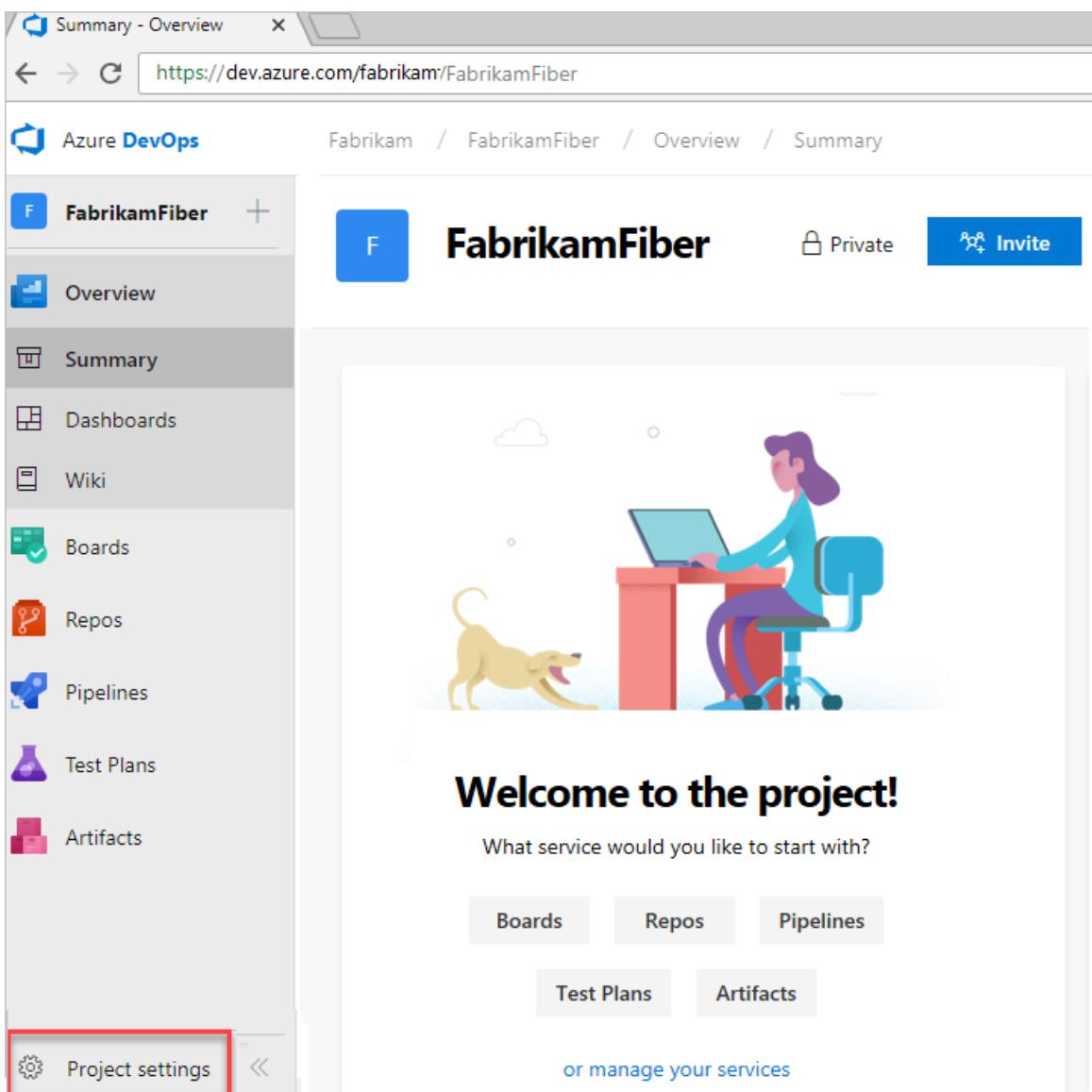
	ONE PROJECT, MANY TEAMS	ONE ORGANIZATION, MANY PROJECTS AND TEAMS	MANY ORGANIZATIONS
General guidance	Best for smaller organizations or larger organizations with highly aligned teams.	Good when different efforts require different processes.	Useful as part of TFS legacy migrations and for hard security boundaries between organizations. Used with multiple projects and teams within each organization.
Scale	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.	
Process	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.
Collaboration	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.
Roll-up reporting and portfolio management	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.
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 will 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.

	ONE PROJECT, MANY TEAMS	ONE ORGANIZATION, MANY PROJECTS AND TEAMS	MANY ORGANIZATIONS
Administrative overhead	Much administration is delegated down to individual teams. Easiest for user licensing and org-level administration. Additional work may be needed if alignment is required between efforts.	Additional administration at the project level. Additional overhead, but can be useful when projects have different administrative needs.	As with additional projects, there's additional administrative overhead, which enables additional 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 should have 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 by visiting its URL and select the **Project settings** button at the lower right of the page.



To learn more about managing projects, see [Manage projects in Azure DevOps](#). You can move a project to a different organization by migrating the data. To learn more about migrating your project, see [Migration options](#).

Managing 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 number 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 desired. Projects can use both TFVC and Git, if appropriate.

One vs. many repos

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.

Starting with a single project containing multiple repos is reasonable, especially if the products/services are working on a coordinated release schedule. If developers are frequently working with multiple repos, keeping them in a single project encourages the processes to remain shared and consistent. Administering repo access is simpler in a single project, as access controls and options like case enforcement and max file size can be set at the project level. Repos can have these access controls and settings managed individually, even if they're in a single project.

If the products stored in multiple repos are working 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, are not easily migrated.

Your decision for one vs. many repos should be largely based on code dependencies and architecture. A good first rule to apply is to 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 there are no tools to assist in coordinating those changes. If your codebase is already a monolith, keep it in one repo. For more information about monolithic repos, see [Git at Scale](#) articles. If you have many disconnected services, one repo per service can be a good strategy.

NOTE

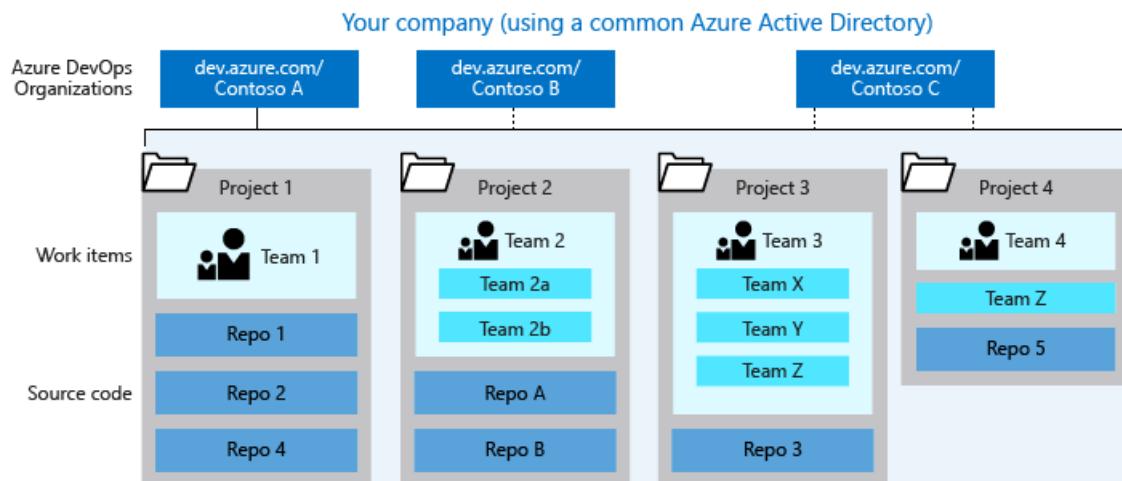
Consider [managing your permissions](#) so not everyone in your organization can [create a repo](#). One of the big challenges a growing team or company faces is the rapid proliferation of repos. If you have too many of them, it's very hard to keep track of who owns what code or other content stored 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. Used 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, it may be useful 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.



More about organizational structure

Choosing your organization admin account type

When you create an organization, the identity that you sign in with defines the identity provider that the organization uses, such as your Azure Active Directory or Microsoft account. Your organization can be created by using a Microsoft account or with an Azure Active Directory account. This account provides the credentials to sign in as an admin to your new organization at <https://dev.azure.com/{yourorganization}>.

Using your Microsoft account

Use your Microsoft account if you don't need to authenticate users for an organization with Azure AD. All users must sign in to your organization with a Microsoft account. If you don't have a Microsoft account, you can [create a Microsoft account](#) at this time.

Microsoft
fabrikamfiber4@hotmail.com
Enter password
.....
 Keep me signed in
[Forgot my password](#)
[Sign in with a different Microsoft account](#)
Sign in

If you don't have an Azure Active Directory instance, create one for free from the [Azure portal](#) or use your Microsoft account to create an organization. Then, you can [connect the organization to Azure AD](#).

Using your Azure Active Directory account

You might have an Azure AD account already if you use Azure or Office 365. If you work for a company that uses Azure AD to manage user permissions, you probably have an Azure AD account.

If you don't have an Azure AD account, learn how to [sign up for Azure AD](#) to automatically connect your

organization to your Azure AD. All users must be members in that directory to access your organization. To add users from other organizations, use [Azure AD B2B collaboration](#).

Azure DevOps authenticates users through your Azure AD, 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 [Azure AD administrators](#) manage users in your directory, so administrators control who accesses your organization.

After you create your Azure account, only members of that directory can access your organization, or you must use [Azure AD business-to-business \(B2B\) collaboration](#) to add users from other organizations.

Learn more about how to [manage users](#).

Mapping organizations to business units

Each business unit within your company gets its own organization in Azure DevOps, along with its own Azure Active Directory tenant. [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 Azure Active Directory accounts). Consider what groups and users share strategies and work, and group them into specific organizations. For example, the (fictional) Fabrikam company might create three organizations: Fabrikam-Marketing, Fabrikam-Engineering, and Fabrikam-Sales. Each organization has a separate URL, such as <https://dev.azure.com/Fabrikam-Marketing>, <https://dev.azure.com/Fabrikam-Engineering>, and <https://dev.azure.com/Fabrikam-Sales>. The organizations are all for the same company but are mostly isolated from each other. You don't need to have anything separated, however you should only create boundaries when it makes sense to your business. You can more easily partition an existing organization with projects, than combine different organizations.

Related articles

- [Create an organization](#)
- [Create a project](#)
- [Code with git](#)

2 minutes to read

2 minutes to read

2 minutes to read

Delete your organization

4/26/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

If you no longer need your organization in Azure DevOps, you can delete it. If you change your mind within 30 days, you can [recover your organization](#). After 30 days, your organization and data are permanently deleted.

When you delete your organization, note the following:

- All users lose access to organization services and resources immediately.
- Your organization URL becomes available for anyone to use. (It might take up to one hour before your organization URL becomes available again.)
- Your organization is disabled, and appears deleted in your profile for 30 days.
- If your organization is linked to an Azure subscription for billing purchases, you must unlink your organization before you delete your organization.

You're still charged for any paid users and services used during this billing cycle. Billing stops after the current cycle ends.

To delete your organization, you need organization owner permissions. [How do I find the organization owner?](#)

Prerequisites

If your organization uses an Azure subscription to bill purchases, you must [first remove billing from your organization](#) before you can delete your organization in Azure DevOps.

Delete organization

To delete your organization, you need at least Basic access and organization owner permissions. [How do I find the organization owner?](#)

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

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' organization. On the left sidebar, under 'My organizations', the 'FabrikamFiber' project is selected and highlighted with a blue border. Below it are other organization entries: 'P', 'fabrikamfib', and 'fabrikamfiber4'. At the bottom of the sidebar, there are links for '+ New organization' and 'Organization settings', with 'Organization settings' being highlighted by a red rectangular box. The main content area displays the 'FabrikamFiber' organization's overview, featuring a large card for the 'Fabrikam Fiber' project, which includes a blue square icon with 'FF' and the project name. Below this, there are sections for 'All projects' showing cards for 'Fabrikam' (dark green square, 'F') and 'FabrikamFiber4.0' (purple square, 'F'), and a section for 'My organizations' listing the same three organizations again.

3. Select **Overview > Delete**.

Organization Settings

General

- Overview**
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory

Security

- Policies
- Permissions

Boards

- Process

Pipelines

- Agent pools
- Settings
- Deployment pools
- Parallel jobs
- OAuth configurations

Privacy URL

[Learn more about the Privacy URL](#)

Description

Add organization description

Time zone

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Region

West Central US

[Learn more about the Region](#)

Save ⓘ Changes made will affect all projects and members of the organization

Organization owner

 andy

andy

[Learn more about the organization owner](#)

Change owner

Delete organization

This will affect all contents and members of this organization.

[Learn more about deleting organizations](#)

Delete

4. In the resulting dialog box, enter the name of the organization, and then select **Delete**.

Delete organization

Are you sure you want to delete the "fabrikam-fiber" organization? All users in your organization will immediately lose access.

You will have up to 30 days to recover this organization after which it will be permanently deleted. This will result in the loss of all organization and related project artifacts. [Learn more about deleting organizations](#)

To confirm this action, please type "fabrikam-fiber".

fabrikam-fiber

By clicking **Delete** you agree to the [Terms of Service](#) and [Privacy Statement](#).

Cancel **Delete**

5. To review your organizations, go to your [Visual Studio profile](#), where you can see your deleted organization.

[Need help?](#)

2 minutes to read

Find or change your organization location

7/2/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

When you [create an organization](#), you can choose the region your organization is hosted in Azure DevOps. You may choose your organization's region based on locality and network latency, or because you have sovereignty requirements for data centers. Your organization's default location is based on the closest [Microsoft Azure region](#) where Azure DevOps is available.

Find your organization location

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

The screenshot shows the Azure DevOps Services home page. On the left, there is a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "fabrikamfib", and "fabrikamfiber4". At the bottom of this sidebar, there are links for "New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main content area is titled "FabrikamFiber" and shows "Fabrikam Fiber" as a project. Below this, under "All projects", there are entries for "Fabrikam" and "FabrikamFiber4.0".

3. Select **Overview**. The region is listed below.

Azure DevOps FabrikamFiber / Organization Settings / Overview

Organization Settings

General

- Overview**
- [Users](#)
- [Billing](#)
- [Auditing](#)
- [Global notifications](#)
- [Usage](#)
- [Extensions](#)
- [Azure Active Directory](#)

Security

- [Policies](#)
- [Permissions](#)

Boards

- [Process](#)

Pipelines

Overview

Name

Use the new URL: <https://dev.azure.com/FabrikamFiber/> [Learn more about URLs](#)

Privacy URL

[Learn more about the Privacy URL](#)

Description

Time zone

Region West Central US [Learn more about the Region](#)

Save Changes made will affect all projects and members of the organization

Change organization location

To change your organization region, call [Azure DevOps Support](#). Support staff coordinates changing the region with the organization owner.

Add a privacy policy URL for your organization

4/16/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

In this article, we explain how to add your privacy policy URL to your organization in Azure DevOps. Your privacy policy URL links to your organization's document that describes how you handle both internal and external guest data privacy. Any member of your organization can add the privacy policy URL.

NOTE

If you're interested in viewing or deleting personal data, please see [Azure Data Subject Requests for the GDPR](#). If you're looking for general info about GDPR, see the [GDPR section of the Service Trust portal](#).

Prerequisites

You need project collection administrator permissions. For more information, see [Quickstart: Set permissions at the project level or project collection level](#).

Add your privacy policy URL in Azure DevOps

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this is a "New organization" button and an "Organization settings" button, which is highlighted with a red box. The main content area is titled "FabrikamFiber" and shows a summary card for the "Fabrikam Fiber" project. It includes a blue "FF" logo icon, the project name, and a horizontal ellipsis. Below this are cards for "All projects", "Fabrikam" (with a teal "F" icon), and "FabrikamFiber4.0" (with a magenta "F" icon). At the bottom of the sidebar, there are links for "Overview", "Projects", "Policy", "Users", "Security", "Permissions", "Notifications", "Extensions", and "Usage".

3. In the **Overview** tab, add your privacy policy URL, and then select **Save**.

The screenshot shows the "Overview" tab of the "Organization settings" page. On the left is a sidebar with the same list of organization settings as the previous screenshot. The main area has a title "OVERVIEW". It contains fields for "Name" (a grayed-out placeholder), a toggle switch for "Use the new URL: https://dev.azure.com/ /", a link "Learn more about URLs", a "Privacy URL" input field (which is highlighted with a red box), and a "Description" input field containing the text "Demo".

A link is added to your organization's privacy document.

To learn more about how we manage and protect your data, read our [Data Protection Overview](#).

Add users to your organization or project

6/26/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to add users to your organization, and specify the level of features they can use, such as Basic or Stakeholder. The following types of users can join your organization for free:

- Five users who get [Basic features](#), such as version control, tools for Agile, Java, build, release, and more
- Unlimited users who get [Stakeholder features](#), such as working with your backlog, work items, and queries
- Unlimited [Visual Studio subscribers](#) who also get Basic features. Additional features, such as [Azure Test Plans](#), can be assigned to users by access level, Basic + Test Plans.

[Need more users with Basic features?](#)

How access differs from permissions

Features that are available to users are controlled by access levels - the full set of organization resources that a user is entitled to access. Permissions control which of these organization resources the user can act on. To learn more, see [Default permissions and access for Azure DevOps](#).

Prerequisites

You must have project collection administrator or owner permissions in Azure DevOps. For more information, see [Set permissions at the project level or project collection level](#).

Add users to your organization

Administrators can now add users to an organization, grant access to appropriate tooling extensions and service access level, and add users to groups all in one view. You can add up to 50 users at once. You can add more than 50 users by repeatedly using this Users view. When you add users, each receives a notification email with a link to the organization page.

NOTE

If you have an Azure Active Directory (Azure AD)-backed organization, and you need to add users who are external to Azure AD, first [add external users](#). On the [Tell us about this user page](#), under **Type of user**, be sure to choose **User with an existing Microsoft account**. After you complete those steps, use the following steps to add the Azure AD user to Azure DevOps.

- [Portal](#)
- [Azure DevOps CLI](#)

To give other users access to your organization, add their email addresses.

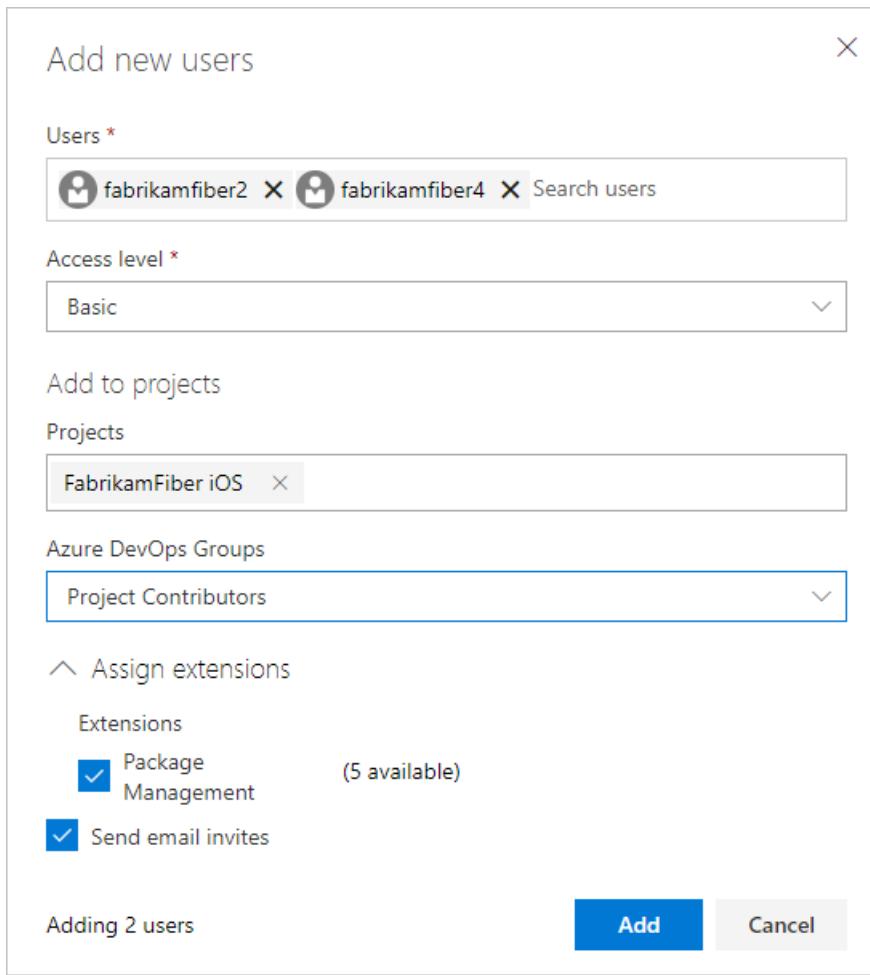
1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Select  **Organization settings**.

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber" (blue card with FF logo), "Fabrikam" (dark teal card with F logo), and "FabrikamFiber4.0" (pink card with F logo). At the bottom of the main area, there's a "All projects" link.

3. Select **Users**, and then select **Add new users** to open the form.

The screenshot shows the "Manage users" page under the "General" tab. The left sidebar has links for "Overview", "Projects", "Policy", "Users" (which is selected and highlighted in blue), and "Security". The main area has tabs for "All users" (selected), "Group rules*", "Summary", and "Add new users" (which is highlighted by a red box). Below these are fields for "Name" and "Access Level". A search bar at the top says "Manage users". At the bottom, there's a table with one row showing "Christie Church" and her email "fabrikamfiber1@hotmail.com". There are also "Extensions" and "... " buttons.

4. Enter information into the form.



- **Users:** Enter the Microsoft account's email address for the user organization.
- **Access level:** Leave the access level at **Basic** for users who contribute to the code base. To learn more, see [About access levels](#).
- **Add to projects:** Select the project that you named in the previous procedure.
- **Groups:** Leave this entry at Project Contributors, the default security group for people who contribute to your project. To learn more, see [Default permissions and access assignments](#).

5. Select **Add** to complete your invitation.

Related articles

- [Connect to a project](#)
- [Change individual permissions, grant select access to specific functions](#)
- [Grant or restrict access to select features and functions](#)
- [Delete users from Azure DevOps](#)
- [Troubleshoot adding and deleting organization users in Azure DevOps](#)
- [Troubleshoot adding members to projects in Azure DevOps](#)

Manage users and their access in Azure DevOps

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to add users to your organization and specify the level of features they can use, such as Basic or Stakeholder.

The following types of users can join your organization for free:

- Five users who get [Basic features](#), such as version control and tools for Agile, Java, and build and release management.
- Unlimited users who get [Stakeholder features](#), such as working with your backlog, work items, and queries.
- Unlimited [Visual Studio subscribers](#) who also get Basic features. In some cases, these users get additional features, such as [Azure Test Plans](#).

Need [more users with Basic features or Visual Studio subscriptions?](#)

NOTE

You can add people to projects instead of to your organization. Users are automatically assigned [Basic features](#) if your organization has seats available, or [Stakeholder features](#) if not. Learn [how to add members to projects](#).

When people don't need access to your organization anymore, [delete them](#) from your organization.

To learn more, read [about access levels](#).

Prerequisites

You must have [project collection administrator or organization owner permissions](#).

Manage users

The Users view shows key information per user in a table. In this view, you can do the following:

- See and modify assigned service extensions and access levels.
- Multi-select users and bulk edit their extensions and access.
- Filter by searching for partial user names, access level, or extension names.
- See the last access date for each user. This can help you choose users to remove access from or lower access to stay within your license limits.

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

[Why am I asked to choose between my work or school account and my personal account?](#)

2. Select  [Organization settings](#).

The screenshot shows the Azure DevOps Home page. On the left, under 'My organizations', there is a list of organizations: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this list are two buttons: '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area displays the selected organization, 'FabrikamFiber', with its projects: 'Fabrikam Fiber' (selected), 'Fabrikam', and 'FabrikamFiber4.0'. At the top of the main area, there are navigation links: 'Projects', 'My work items', and 'My pull requests'. The URL in the browser bar is https://dev.azure.com/fabrikamfiber.

3. Select **Users > Add new users**.

The screenshot shows the 'Manage users' page under the 'General' tab. The left sidebar has options: 'Overview', 'Projects', 'Policy', 'Users' (selected and highlighted in blue), and 'Security'. The main area has a title 'Manage users' with tabs: 'All users' (selected), 'Group rules*', 'Summary', '+ Add new users' (highlighted by a red box), and 'Export users'. Below these are filters for 'Name' and 'Access Level'. A table lists users: 'Christie Church' with the email 'fabrikamfiber1@hotmail.com'. The 'Users' tab in the sidebar is also highlighted in blue.

4. Select a user or group of users. Then, select the ... icon at the end of the **Name** column to open the context menu.

In the context menu, select one of the following options:

- **Add to projects**
- **Remove from projects**
- **Assign extensions**
- **Revoke extensions** (if there are extensions)
- **Change access levels**
- **Remove direct assignments**
- **Remove from organization** (deletes user)

The screenshot shows the 'Manage users' interface in Azure DevOps. At the top, there are navigation links for 'All users' (selected), 'Group rules', 'Change access level', 'Manage projects', and 'Manage extensions'. Below the header are search and filter fields for 'Name', 'Extensions', and 'Access Level', with a 'Clear' button. The main area displays a list of users with their names, email addresses, profile icons, and initials. The first user listed is Jamal Hartnett (fabrikamfiber4@hotmail.com). A red box highlights the three-dot menu icon next to his name. A context menu is open over this icon, listing several options: 'Add to projects', 'Remove from projects', 'Assign extensions', 'Revoke extensions', 'Change access levels', 'Remove direct assignments', and 'Remove from organization'. The menu items are preceded by blue plus or minus signs and crossed-out symbols where applicable.

5. **Save** your changes.

How is *access* different from *permissions*?

Access levels control which features are available to users. Permissions control a user's access to organization resources. To learn more, see [Default permissions and access](#).

Related articles

- [Change number of paid extension users](#)
- [Connect to a project](#)
- [Change individual permissions or grant select access to specific functions](#)
- [Grant or restrict access to select features and functions](#)
- [Delete users from Azure DevOps](#)

Manage conditional access to Azure DevOps

1/31/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Conditional access offers simple ways to help secure resources for organizations in Azure DevOps that are backed by an Azure Active Directory (Azure AD) tenant. Conditional access policies (CAPs) like multi-factor authentication help protect against the risk of compromised credentials and help keep your organization's data safe. In addition to requiring credentials, you can have a policy that only devices that are connected to a corporate network can gain access. More generally, there are a few requirements and actions that you can implement for devices in a device management system. This system is security software that's used by IT departments to manage devices running various operating systems from various locations and networks.

You can require conditions, such as security group membership, location and network identity, a specific OS, an enabled device in a management system, and so on.

Depending on which conditions the user satisfies, you can require multi-factor authentication, require further checks, or block access.

Azure DevOps enforces the policy for usage of personal access tokens (PATs), alternate authentication, OAuth, and SSH keys. See the following details of how and what we enforce.

- For Web flows, CAP is honored 100%
- For third party client flow, like using a PAT with git.exe, we only support IP fencing policies - more specifically we don't support MFA policies. See the following examples:
 - Policy 1 - Block all access from outside of IP range X, Y, and Z
 - If a user is accessing Azure DevOps via the web, the user is allowed from IP X,Y,Z or blocked if outside that list
 - If a user is accessing Azure DevOps via alt-auth, the user is allowed from IP X,Y,Z or blocked if outside that list
 - Policy 2 - Require MFA when outside of IP range X, Y, and Z
 - If a user is accessing Azure DevOps via the web, the user is allowed from IP X,Y,Z or prompted for MFA if outside that list
 - If a user is accessing Azure DevOps via alt-auth, the user is allowed from IP X,Y,Z blocked if outside that list

Enable conditional access for Azure DevOps

To enforce conditional access policy on your organization, you must enable the policy in Azure DevOps, as it is set to off by default.

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

[Why am I asked to choose between my work or school account and my personal account?](#)

2. Select  **Organization settings**.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' organization. On the left sidebar, under 'My organizations', the 'FabrikamFiber' project is selected and highlighted with a blue border. Below it are other organization entries: 'P' (with a grey icon), 'fabrikamfib' (with a purple icon), and 'fabrikamfiber4' (with a green icon). At the bottom of the sidebar, there are two buttons: '+ New organization' and 'Organization settings', with 'Organization settings' being highlighted by a red rectangular box. The main content area is titled 'FabrikamFiber' and contains three tabs: 'Projects' (selected), 'My work items', and 'My pull requests'. Below the tabs is a card for the 'Fabrikam Fiber' project, which has a blue icon with 'FF' and the project name. Further down, under 'All projects', there are cards for 'Fabrikam' (dark teal icon with 'F') and 'FabrikamFiber4.0' (purple icon with 'F').

3. Select **Policy** and from the **dropdown** next to Enable Azure Active Directory Conditional Access Policy Validation select **On**.

Organization Settings	Policy
General	Application connection policies
Overview	Alternate authentication credentials 🔗 On ▾
Projects	Third-party application access via OAuth 🔗 On ▾
Policy	SSH authentication 🔗 On ▾
Users	
Security	
Notifications	
Extensions	Security policies
Usage	External guest access 🔗 On ▾
Boards	Allow public projects 🔗 On ▾
Process	Enable Azure Active Directory Conditional Access Policy Validation 🔗 On ▾
Pipelines	

Related articles

- [What is conditional access in Azure Active Directory?.](#)
- [Detailed instructions and requirements for conditional access.](#)

Authenticate access with personal access tokens

6/18/2019 • 3 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

Personal access tokens (PATs) are alternate passwords that you can use to authenticate into Azure DevOps. In this article, we walk you through how to create or revoke PATS.

Azure DevOps uses enterprise-grade authentication to help protect and secure your data. Clients like Visual Studio and Eclipse (with the Team Explorer Everywhere plug-in) also support Microsoft account and Azure AD authentication. Since PATs are an alternate form of user authentication, using a PAT gives you the same access level. If you create a PAT with a narrower scope, your access is limited to that particular scope.

For non-Microsoft tools that integrate into Azure DevOps but don't support Microsoft account or Azure AD authentication, you must use PATs. Examples include Git, NuGet, or Xcode. To set up PATs for non-Microsoft tools, use [Git credential managers](#) or create them manually.

Create personal access tokens to authenticate access

1. Sign in to either your organization in Azure DevOps (<https://dev.azure.com/{yourorganization}>) or your Team Foundation Server web portal (<https://{{server}}:8080/tfs/>).
2. From your home page, open your profile. Go to your security details.

Azure DevOps Services

TFS 2017

3. Create a personal access token.

4. Name your token. Select a lifespan for your token.

If you're using Azure DevOps Services, and you have more than one organization, you can also select the organization where you want to use the token.

5. Select the [scopes](#) for this token to authorize for *your specific tasks*.

For example, to create a token to enable a [build and release agent](#) to authenticate to Azure DevOps Services or TFS, limit your token's scope to **Agent Pools (read, manage)**.

6. When you're done, make sure to *copy the token*. You'll use this token as your password.

NOTE

Remember that this token is your identity and acts as you when it's used. Keep your tokens secret and treat them like your password.

To keep your token more secure, use credential managers so that you don't have to enter your credentials every time. Here are some recommended credential managers:

- Git: [Git Credential Manager for macOS and Linux](#) or [Git Credential Manager for Windows](#) (requires [Git for Windows](#))
- NuGet: [NuGet Credential Provider](#)

Revoke personal access tokens to remove access

When you don't need your token anymore, just revoke it to remove access.

1. From your home page, open your profile. Go to your security details.

Azure DevOps Services



Azure DevOps Server (formerly TFS)



2. Revoke access.



See the following examples of using your PAT.

Username: `anything` Password: `your PAT here`

or

```
git clone https://anything:<PAT>@dev.azure.com/yourOrgName/yourProjectName/_git/yourRepoName
```

To learn more about how security and identity are managed, see [About security and identity](#).

To learn more about permissions and access levels for common user tasks, see [Default permissions and access for Azure DevOps](#).

For administrators to revoke organization user PATs, see [Revoke other users' personal access tokens](#).

Frequently asked questions

What is my Azure DevOps Services URL?

<https://dev.azure.com/{yourorganization}>

Where can I learn more about how to use PATs?

For examples of how to use PATs, see [Git credential managers](#), [REST APIs](#), [NuGet on a Mac](#), and [Reporting clients](#).

What notifications will I get about my PAT?

Users receive two notifications during the lifetime of a PAT, one at creation and the other seven days before the expiration.

The following notification is sent at PAT creation:

A new personal access token was added to your organization

[Learn more](#) about why you're receiving this email. If you did not make this change, your credentials may have been compromised and we suggest changing your password.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 10/30/2018

Origination IP

User agent

We sent you this notification due to a default subscription

Sent from Azure DevOps.

The following notification is sent - a PAT is near expiration:

One of your personal access tokens will be expiring on 8/4/2018.

Click below to manage your personal access tokens.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 8/4/2018

We sent you this notification due to a default subscription

Sent from Azure DevOps.

What do I do if I get an unexpected PAT notification?

An administrator or a tool might have created a PAT on your behalf. See the following examples:

- When you connect to an Azure DevOps Services Git repo through git.exe, it creates a token with a display name like "git: <https://MyOrganization.visualstudio.com/> on MyMachine."
- When you or an admin sets up an Azure App Service web app deployment, it creates a token with a display name like "Service Hooks :: Azure App Service :: Deploy web app."
- When you or an admin sets up web load testing as part of a pipeline, it creates a token with a display name like "WebAppLoadTestCDIntToken".
- When a Microsoft Teams Integration Messaging Extension is set up, it creates a token with a display name like "Microsoft Teams Integration".

If you still believe that a PAT exists in error, we suggest that you [revoke the PAT](#). Next, change your password. As an Azure Active Directory user, check with your administrator to see if your organization was used from an unknown source or location.

Revoke personal access tokens for organization users

5/7/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

If an organization user's personal access token (PAT) has been compromised, we recommend taking immediate action. Revoke their access tokens, as a precaution to protect your organization. In this article, we show you how administrators of Azure DevOps organizations can revoke PATs for users.

Prerequisites

Only an organization administrator or project collection administrator (PCA) can revoke user PATs. If you're not a member of the **Project Collection Administrators** group, [get added as one](#). To learn how to find your organization's admin, see [Look up administrators and organization owner](#).

For users, if you want to create or revoke your own PATs, see [Create or revoke personal access tokens](#).

Revoke PATs

1. To revoke the OAuth authorizations, including PATs, for your organization's users, see [Token revocations - Revoke authorizations](#).
2. Use this [PowerShell script](#) to automate calling the new REST API by passing a list of user principal names (UPNs). If you don't know the UPN of the user who created the PAT, use this script, however it must be based on a date range.

NOTE

Keep in mind that when you use a date range any JSON web tokens (JWTs) are also revoked. Also be aware that any tooling that relies on these tokens won't work until refreshed with new tokens.

1. After you've successfully revoked the affected PATs, let your users know. They can recreate their tokens, as needed.

Token expiration

FedAuth tokens

A FedAuth token is issued when you sign-in. It is valid for a seven day sliding window. The expiry automatically extends another seven days whenever you refresh it within the sliding window. If users access the service regularly, only an initial sign-in is needed. After a period of inactivity extending seven days, the token becomes invalid and the user must sign in again.

Personal access tokens

Users can choose an expiry date for their personal access token, not to exceed one year. We recommend you use shorter time periods, generating new PATs upon expiry. Users receive a notification email one week before token expiry. Users can generate a new token, extend expiry of the existing token, or change the scope of the existing token, if needed.

Frequently asked questions (FAQs)

What if a user leaves my company?

A: Once a user is removed from Azure AD, the PATs and FedAuth tokens are invalidated within an hour, since the refresh token is valid only for one hour.

What about JSON web tokens (JWTs)?

A: Revoke JWTs, issued as part of the OAuth flow, via the [PowerShell script](#). However, you must use the date range option in the script.

Related articles

- [How Microsoft protects your projects and data in Azure DevOps](#)
- [Create or revoke your personal access tokens](#)

Change application access policies for your organization

5/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

You can change your application access policies for your organization in Azure DevOps. Azure DevOps offers the capability for other apps to integrate with its services and resources in your organization. To access your organization without asking for user credentials multiple times, apps can use the following authentication methods:

- [OAuth](#) to generate tokens for accessing [REST APIs for Azure DevOps Services and Team Foundation Server](#). The [Organizations](#) and [Profiles](#) APIs support only OAuth.
- [Alternate credentials](#) as a single set of credentials across all tools that don't have plug-in, extension, or native support. For example, you can use basic authentication to access [REST APIs for Azure DevOps](#), but you must turn on alternate credentials.
- [SSH authentication](#) to generate encryption keys when you use Linux, macOS, or Windows running [Git for Windows](#) and can't use [Git credential managers](#) or [personal access tokens](#) for HTTPS authentication.
- [Personal access tokens](#) to generate tokens for:
 - Accessing specific resources or activities, like builds or work items
 - Clients like Xcode and Nuget that require usernames and passwords as basic credentials and don't support Microsoft account and Azure Active Directory features like multi-factor authentication
 - Accessing [REST APIs for Azure DevOps](#)

By default, your organization allows access for all authentication methods. You can limit access, but you must specifically restrict access for each method. When you deny access to an authentication method, no app can use that method to access your organization. Any app that previously had access gets an authentication error and can't access your organization.

To remove access for personal access tokens, you must [revoke them](#).

To continue, you'll need at least Basic access and organization owner permissions. [How do I find the organization owner?](#)

Change application access policies

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled 'My organizations' with a list of organizations: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. Under 'Projects', there are cards for 'Fabrikam Fiber' (blue icon), 'Fabrikam' (teal icon), and 'FabrikamFiber4.0' (purple icon). At the bottom of the sidebar, there are links for 'All projects', 'New organization', and 'Organization settings'.

3. In the Policies tab, review your application connection settings. Change these settings, based on your security policies.

The screenshot shows the 'Organization Settings' page under 'FabrikamFiber'. The left sidebar has sections for General (Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions), Azure Active Directory (Azure Active Directory), and Security (Policies, Permissions). The 'Policies' link is highlighted by a red box. The main content area is titled 'Policy' and contains two sections: 'Application connection policies' and 'Security policies'. Under 'Application connection policies', there are three dropdowns: 'Alternate authentication credentials' set to 'On', 'Third-party application access via OAuth' set to 'On', and 'SSH authentication' set to 'On'. Under 'Security policies', there are three dropdowns: 'External guest access' set to 'On', 'Allow public projects' set to 'Off', and 'Enable Azure Active Directory Conditional Access Policy Validation' set to 'Off'.

NOTE

Anonymous access is used to access both private and public repos. Learn more at [Make your project public](#).

Related articles

- [Need help?](#)
- [Assign access levels and extensions by group membership](#)
- [Manage conditional access](#)

Remove users from Azure DevOps

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

If users no longer require access to a project or your organization, you can remove their access to the project or your organization.

Prerequisites

- You need [project collection administrator or organization owner permissions](#).

Remove users from your organization

1. Sign in to your organization: <https://dev.azure.com/{yourorganization}>.

[Why am I asked to choose between my work or school account and my personal account?](#)

2. Select **Organization settings**.

The screenshot shows the Azure DevOps web interface. At the top, there's a navigation bar with a back arrow, forward arrow, refresh button, and a home icon. The URL in the address bar is https://dev.azure.com/fabrikamfiber. Below the address bar, the Azure DevOps logo is visible. On the left, there's a sidebar titled "My organizations" containing a list of organizations: "FabrikamFiber" (selected), "P", "fabrikamfib", and "fabrikamfiber4". A red box highlights the "Organization settings" link at the bottom of this sidebar. The main content area is titled "FabrikamFiber" and contains three projects: "Fabrikam Fiber" (with a blue "FF" icon), "Fabrikam" (with a teal "F" icon), and "FabrikamFiber4.0" (with a magenta "F" icon). Below the projects, there's a section titled "All projects" with a teal "F" icon.

3. Select **Users**.

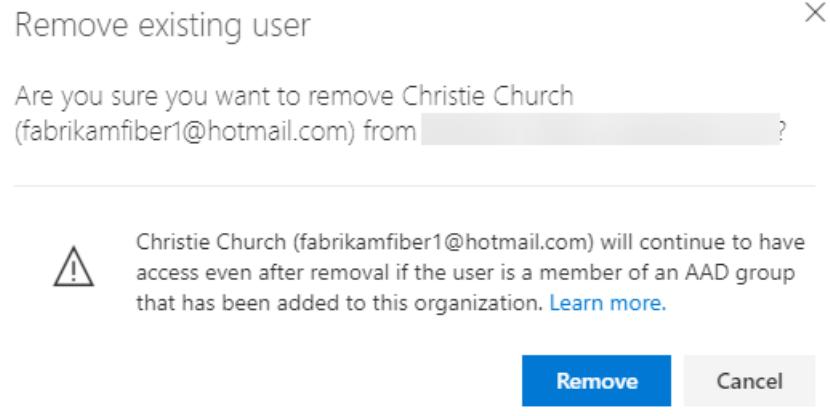
Organization Settings > Users

The screenshot shows the 'Organization Settings' page with the 'Users' section selected. The left sidebar has 'General' expanded, showing 'Overview', 'Projects', 'Policy', 'Users' (which is highlighted with a red box), 'Security', 'Notifications', 'Extensions', and 'Usage'. Below 'General' is 'Boards' with 'Process' listed. Under 'Build and release', there is a plus sign. The main area is titled 'Manage users' with tabs for 'All users' (selected), 'Group rules', 'Summary', and '+ Add new users'. It includes search fields for 'Name' and 'Extensions'. A table lists users: Christie Ch... (fabrikamfiber1...), fabrikamfi... (fabrikamfiber2...), fabrikamfi... (fabrikamfiber5...), fabrikamfi... (fabrikamfiber6...), and Jamal Hart... (fabrikamfiber4...). Each user has a three-dot menu icon.

4. Open the context menu ... for the user to be removed. Select **Remove from organization**.

The screenshot shows the 'Organization Settings' page with the 'Users' section selected. The left sidebar has 'General' expanded, showing 'Overview', 'Projects', 'Policy', 'Users' (selected), 'Security', 'Notifications', 'Extensions', and 'Usage'. Below 'General' is 'Work' with 'Process' listed. The main area is titled 'Manage users' with tabs for 'All users' (selected), 'Group rules', 'Summary', and '+ Add new users'. It includes search fields for 'Name' and 'Extensions'. A table lists users: Christie Ch... (fabrikamfiber1...), fabrikamfi... (fabrikamfiber2...), fabrikamfi... (fabrikamfiber5...), fabrikamfi... (fabrikamfiber6...), and Jamal Hart... (fabrikamfiber4...). The context menu for the first user ('Christie Ch...') is open, showing options: 'Change access level', 'Manage projects', 'Manage extensions', 'Resend invite', 'Remove from organization' (which is highlighted with a red box), and 'Remove direct assignments'.

5. Choose **Remove** in the confirmation dialog.



6. To confirm that you've removed the users completely, make sure they aren't in any of your [security groups](#).

[Why don't users appear or disappear promptly after I add or delete them in the Users Services page?](#)

7. If you deleted paid users who had Basic or higher features, and you don't want to pay for those users, you must also [reduce the users](#). Then you're not charged in your next Azure billing cycle.

To reduce or cancel users for the next month, you must make updates before the last day of the current month. Your bill won't show the changes until the next month because paid users are monthly purchases.

NOTE

- Azure Active Directory (AD)-backed organizations. After you remove a user from Azure AD, you can't assign artifacts to that user anymore. Examples are work items and pull requests. However, we preserve the history of artifacts that were already assigned to the user.
- Managed service account (MSA)-backed organizations. After you remove a user from your MSA-backed organization, the user remains within the tenant and can be re-added at any time.

Remove users from a team or project

To remove users from a project, remove them from the **Teams** groups they belong to or the **Contributors** group for the project. See [Add users to a project or specific team](#). You can remove a user from the **Members** page of a team group or security group.

The screenshot shows the 'Contributors' page in the Azure DevOps 'Contributors' section. On the left, there's a sidebar with a 'Create group' button and a 'Filter users and groups' input field. Below that is a list of 'Azure DevOps Services Groups' under the heading 'Azure DevOps Services Groups'. The 'Contributors' group is selected, highlighted with a grey background. The main area has tabs for 'Permissions', 'Members', and 'Member of'. The 'Members' tab is active. It displays two users: 'Christie Church' and 'Jamal Hartnett'. Each user row has a small profile picture, the display name, the email address, and a 'Remove' button. The 'Remove' button for 'Jamal Hartnett' is highlighted with a red box.

Display Name	Username Or Scope
Christie Church	fabrikamfiber1@hotmail.com
Jamal Hartnett	fabrikamfiber4@hotmail.com

Related articles

- [Set permissions at the project level or project collection level.](#)
- [Change individual permissions and grant select access to specific functions](#)
- [Grant or restrict access to select features and functions](#)
- [Troubleshoot adding and deleting organization users in the Users page](#)
- [Troubleshoot adding members to projects](#)

Add external users to your organization

5/20/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to invite external users to your organization, if you access Azure DevOps via Azure Active Directory (Azure AD). To do so, you must add the identities of those users to your Azure AD and organizations. Doing this also grants the users some additional privileges. Learn more about the [additional organization-level resources](#).

Prerequisites

- You must set the policy **External guest access** to **On** for the organization that you want to invite external users to.

The screenshot shows the 'Organization Settings' interface with the 'Policy' section selected. Under 'Application connection policies', three options are listed: 'Alternate authentication credentials' (On), 'Third-party application access via OAuth' (On), and 'SSH authentication' (On). Under 'Security policies', two options are listed: 'External guest access' (highlighted with a red box) and 'Anonymous access to projects' (Off).

- You must be a member of the Project Collection Administrators group for the organization that you want to invite external users to.
- The Azure AD tenant to which you want to invite external users must allow you to add new users based on your Azure Active Directory guest policies. Learn [how to become eligible to invite external users on your Azure AD tenant](#).

Invite an external user to your organization

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

The screenshot shows the Azure DevOps interface for the organization 'FabrikamFiber'. On the left sidebar, under 'My organizations', the 'FabrikamFiber' project is selected. Below it are other organization items: 'P', 'fabrikamfib', and 'fabrikamfiber4'. A red box highlights the 'Organization settings' button. The main area displays the 'Fabrikam Fiber' project, followed by a list of other projects: 'Fabrikam' and 'FabrikamFiber4.0'.

3. Select **Users**, and then select **Add new users**.

The screenshot shows the 'Manage users' page within the organization settings. The left sidebar has a 'General' section with 'Overview', 'Projects', 'Policy', 'Users' (which is selected and highlighted in blue), and 'Security'. The main area shows a table with a single user entry: 'Christie Church' (email: fabrikamfiber1@hotmail.com). The 'Add new users' button at the top right is highlighted with a red box.

4. Enter the external user's email address followed by a semicolon, and then select **Add**. A warning message appears, indicating that an external user is being added from outside your directory.

Add new users

Users *

Access level *

Add to projects

Projects

Azure DevOps Groups

Project Contributors

Assign extensions

Send email invites

You are inviting users from outside your directory. The user(s) @outlook.com will need to click the link in their invitation e-mail to be able to access the organization and its resources. [Learn more](#).

Adding 1 user **Add** **Cancel**

The screenshot shows the 'Add new users' dialog box. At the top, there's a header 'Add new users' and a close button 'X'. Below it, there's a section for 'Users *' with a text input field containing '@outlook.com'. Next is an 'Access level *' dropdown set to 'Basic'. Then comes a 'Add to projects' section with a 'Projects' dropdown containing 'MyFirstProject' and a delete 'X' button. Below that is an 'Azure DevOps Groups' section with a 'Project Contributors' dropdown. Under these, there are two buttons: 'Assign extensions' and 'Send email invites' (which is checked). A yellow info box states: 'You are inviting users from outside your directory. The user(s) @outlook.com will need to click the link in their invitation e-mail to be able to access the organization and its resources.' At the bottom, there are three buttons: 'Adding 1 user' (disabled), 'Add' (in blue), and 'Cancel'.

5. Advise the external user to locate the email that they received from Azure DevOps and go to the redemption URL. The external user must navigate through an Azure B2B redemption experience, which adds the user to your organization.

NOTE

If you need to resend the invitation email, go to **Users**, select the user, and select **Resend invite**.

The external user is added to the organization to which they were invited and has immediate access.

Related articles

- [What is Azure AD B2B collaboration?](#)
- [Migrate to group-based resource management](#)
- [Assign access levels and extensions to users by group membership](#)

Connect your organization to Azure Active Directory

7/8/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Connect your Azure DevOps organization to [Azure Active Directory \(Azure AD\)](#) so you can sign in with the same username and password that you use with Microsoft services. You can easily find and add members to your Azure DevOps organization who are already a part of your work organization. You can also enforce policies for accessing your team's critical resources and key assets.

For more information about using Azure AD with Azure DevOps, see the [conceptual overview](#).

Prerequisites

- Ensure you're a Project Collection Administrator or [owner of the organization](#) to perform the connection.
- Ensure that you exist in Azure AD as a *member*. For more information, see [how you can convert an Azure AD guest into a member](#).
- Inform users of the upcoming change. There's no downtime during this change, but users are affected. Let them know before you begin that there's a short series of steps to complete. As your company transitions from Microsoft account (MSA) to Azure AD identities, your users' benefits continue with their new identity, as long as their emails match.
- Delete unwanted users from your organization. For example, you can remove a user who left the company and is no longer an employee.
- Prepare your mapping list for inviting users to Azure AD.

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

2. Select  **Organization settings**.

The screenshot shows the Azure DevOps interface for managing organizations. On the left, under 'My organizations', the 'FabrikamFiber' organization is selected, highlighted with a blue border. Below it are other organizations: 'P' (unselected), 'fabrikamfib', and 'fabrikamfiber4'. To the right, the main area displays the 'FabrikamFiber' organization's projects. The first project shown is 'Fabrikam Fiber', followed by a horizontal ellipsis and several other projects. Below this section, there is a heading 'All projects' and two more project cards: 'Fabrikam' and 'FabrikamFiber4.0'. At the bottom left of the organization list, there are two buttons: '+ New organization' and 'Organization settings', with 'Organization settings' being highlighted by a red rectangular box.

Projects - Home

https://dev.azure.com/fabrikamfiber

Azure DevOps

My organizations

F fabrikamfiber

P

F fabrikamfib

F fabrikamfiber4

FabrikamFiber

Projects My work items My pull requests

FF Fabrikam Fiber

All projects

+ New organization

Organization settings

F Fabrikam

F FabrikamFiber4.0

3. Select **Users**.

Organization Settings > Users

General

- Overview
- Projects
- Policy
- Users**
- Security
- Notifications
- Extensions
- Usage

Boards

- Process

> Build and release

Manage users

All users Group rules Summary + Add new users

Name ↑	Extensions
Christie Ch... fabrikamfiber1...	...
fabrikamfi... fabrikamfiber2...	...
fabrikamfi... fabrikamfiber5...	...
fabrikamfi... fabrikamfiber6...	...
Jamal Hart... fabrikamfiber4...	...

4. Compare your Azure DevOps email list with your Azure AD email list. Create an Azure AD email address entry for every user who is in the Azure DevOps organization and NOT in the Azure AD. For any user that you don't create an Azure AD email address, be prepared to invite these users as guests to the Azure AD in future steps.

NOTE

Ensure you're using Azure AD Public. Support for Azure AD Government is currently limited.

Connect your organization to Azure AD

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

The screenshot shows the Azure DevOps Home page for the organization 'FabrikamFiber'. On the left sidebar, under 'My organizations', the 'FabrikamFiber' project is selected, indicated by a blue border around its card. Other organizations listed are 'P' (grayed out), 'fabrikamfib', and 'fabrikamfiber4'. Below the sidebar, there's a section titled 'All projects' featuring cards for 'Fabrikam' (blue F icon) and 'FabrikamFiber4.0' (purple F icon). At the bottom of the sidebar, there are links for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box.

3. Select **Azure Active Directory**, and then select **Connect directory**.

The screenshot shows the 'Organization Settings' page for 'FabrikamFiber'. The left sidebar lists various settings: General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' item is highlighted by a red box. The main content area is titled 'Azure Active Directory' and contains the text 'Connect your organization to an Azure Active Directory.' Below this is a link 'Follow steps and learn more' and a prominent blue button labeled 'Connect directory', which is also highlighted by a red box.

4. Select a directory from the dropdown menu, and then select **Connect**.

Azure Active Directory Connection



Connect your organization to a directory.

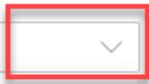
You are signed in as



Jamal Hartnett
fabrikamfiber4@hotmail.com

Azure Active Directory

Select



FabrikamFiberAAD12

Microsoft

Commerce Test Directory

FabrikamFiberAAD

Cancel

Connect

If you can't

find your directory, contact your Azure AD administrator and request that they add you as a member to the Azure AD.

5. Select **Sign out**.

Connect success!

Your organization **FabrikamFiber** is successfully connected to **Commerce Test Directory** Azure Active Directory.

As a result of a successful connection, you and all FabrikamFiber users must sign out now.

Sign out

Your organization is now connected to your Azure AD.

6. Confirm that the process is complete. Sign out, and then open your browser in a private session and sign in to your organization with your Azure AD or work credentials.
7. If you have disconnected members, sign back in to Azure DevOps and map them to their Azure AD identities or invite them as guests into the Azure AD. See the [FAQ](#) for further information.

Organization Settings

Azure Active Directory

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory**

Your organization is connected to the **Commerce Test Directory** directory.

Commerce Test Directory
mstestvscommerceoutlook.onmicrosoft.com
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Disconnect directory

Resolve disconnected users

Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

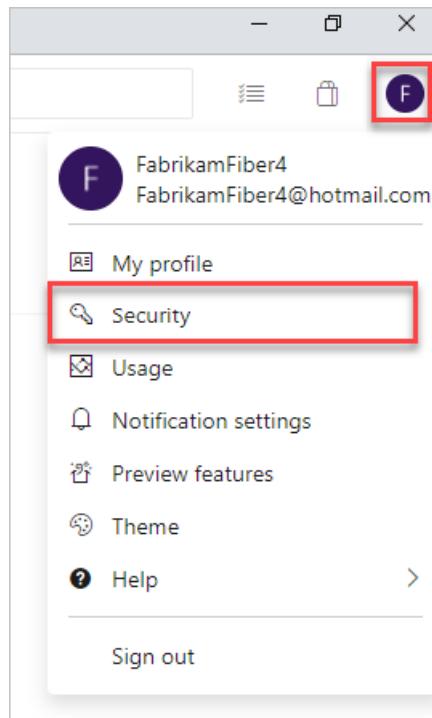
Inform users of the completed change

When you inform your users of the completed change, include the following tasks for each user in the

organization to complete:

- Clear the cache for the [Git Credential Manager](#) if you use Visual Studio or the Git command-line tool. Delete the `%LocalAppData%\GitCredentialManager\tenant.cache` file on each client machine.
- [Regenerate new personal access tokens](#). Complete the following steps:

a. In Azure DevOps, select your profile icon, and then select **Security** from the resulting dropdown menu.



b. Select **Personal access tokens**, and then select **New Token**.

A screenshot of the Azure DevOps User settings interface. On the left is a sidebar with options: General, About, Time and Locale, Notifications, Theme, Usage, Security, Personal access tokens (which is highlighted with a red box), and SSH public keys. The main panel shows the "Personal Access Tokens" section with a sub-instruction: "These can be used instead of a password". A red box highlights the "+ New Token" button.

c. Complete the form, and then select **Create**.

Create a new personal access token

X

Name

New token name

Organization

FabrikamFiber

Expiration (UTC)

30 days

Fri Jun 14 2019



Scopes

Authorize the scope of access associated with this token

Scopes

Full access Custom defined

Work Items

Work items, queries, backlogs, plans, and metadata

Read Read & write Read, write, & manage

Code

Source code, repositories, pull requests, and notifications

Read Read & write Read, write, & manage Full Status

Build

Artifacts, definitions, requests, queue a build, and updated build properties

Read Read & execute

Release

Read, update, and delete releases, release pipelines, and stages

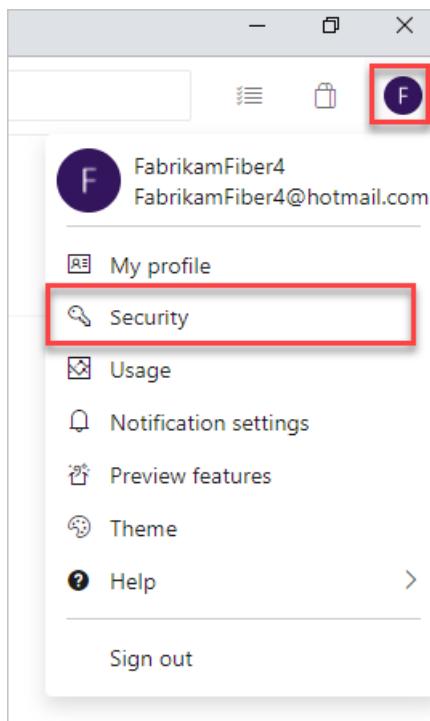
Read Read, write, & execute Read, write, execute, & manage

Show all scopes (27 more)

Create

Cancel

- d. When the token is created, copy it, as it can't be viewed again.
- Request that SSH keys be manually cleared by [Support](#), and then recreate SSH keys. Complete the following steps.
 - a. In Azure DevOps, select your profile icon, and then select **Security** from the resulting dropdown menu.



b. Select **SSH public keys**, and then select **Add**.

A screenshot of the Azure DevOps User settings page. The left sidebar lists various settings: General, About, Time and Locale, Notifications, Theme, Usage, Security, Personal access tokens, and SSH public keys (which is highlighted with a red box). The main content area has a heading "User settings" and a sub-heading "Contribute to a Git repository without typing a username and password every time." It includes an "Add" button (highlighted with a red box) and a message: "You haven't added any SSH public keys that can access your organization. To get started, add a key from a file or generate one." Other visible items include "General" (with a gear icon), "About" (with a person icon), "Time and Locale" (with a clock icon), "Notifications" (with a bell icon), "Theme" (with a color palette icon), and "Usage" (with a bar chart icon).

c. Enter a description and key data, and then select **Save**.

A screenshot of the "Add an SSH public key" dialog box. It has two main sections: "Description" (containing a text input field with "ssh description...") and "Key Data" (containing a large text area for pasting key data). At the bottom are two buttons: "Save" (highlighted with a red box) and "Cancel".

- d. When the token is created, copy it, as it can't be viewed again.
- [Rename your Microsoft account](#) to a different email that doesn't conflict with your Azure AD identity if you don't want to be prompted to choose between accounts.
- [Manage your Visual Studio with MSDN subscription](#), if you used a Microsoft account to sign up for Azure DevOps. Link work or school accounts to this subscription.

Related articles

- [Disconnect from Azure AD](#)
- [Change Azure AD connection](#)
- [Enforce conditional access policies](#)
- [Manage access with Azure AD groups](#)

Change connection to Azure AD

5/30/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

If you need to switch your organization connection from one Azure Active Directory (Azure AD) to another, complete the following steps.

For more information about using Azure AD with Azure DevOps, see the [Conceptual overview](#).

Prerequisites

- Before you disconnect your organization from your directory, make sure to **change the organization Owner to a Microsoft account** and not to a school or work account. You can't sign in to your organization unless your work or school account has the same email address as your Microsoft account.
- Add your Microsoft account to the Project Collection Administrator group in Organization settings and confirm that you have Global Administrator Permissions in your Azure AD for your Microsoft account. You need both because Azure AD users can't disconnect organizations from directories. You can add Microsoft accounts to a directory as external users.
- Ensure that you exist in Azure AD as a *member*. For more information, see [how you can convert an Azure AD guest into a member](#). > [!IMPORTANT] > If you want to connect your organization to a different Azure Active Directory at any time, ensure that any connected organizations are disconnected from the original directory BEFORE you delete that directory. Once a new directory is established, connect your organization to the new directory so users can regain access. Learn more about [connecting your organization to Azure AD](#).
- Inform users of the upcoming change. There's no downtime during this change, but users are affected. Let them know before you begin that there's a short series of steps to complete. As your company transitions from Microsoft account (MSA) to Azure AD identities, your users' benefits continue with their new identity, as long as their emails match.
- Delete unwanted users from your organization. For example, you can remove a user who left the company and is no longer an employee.

Change the Azure AD connection

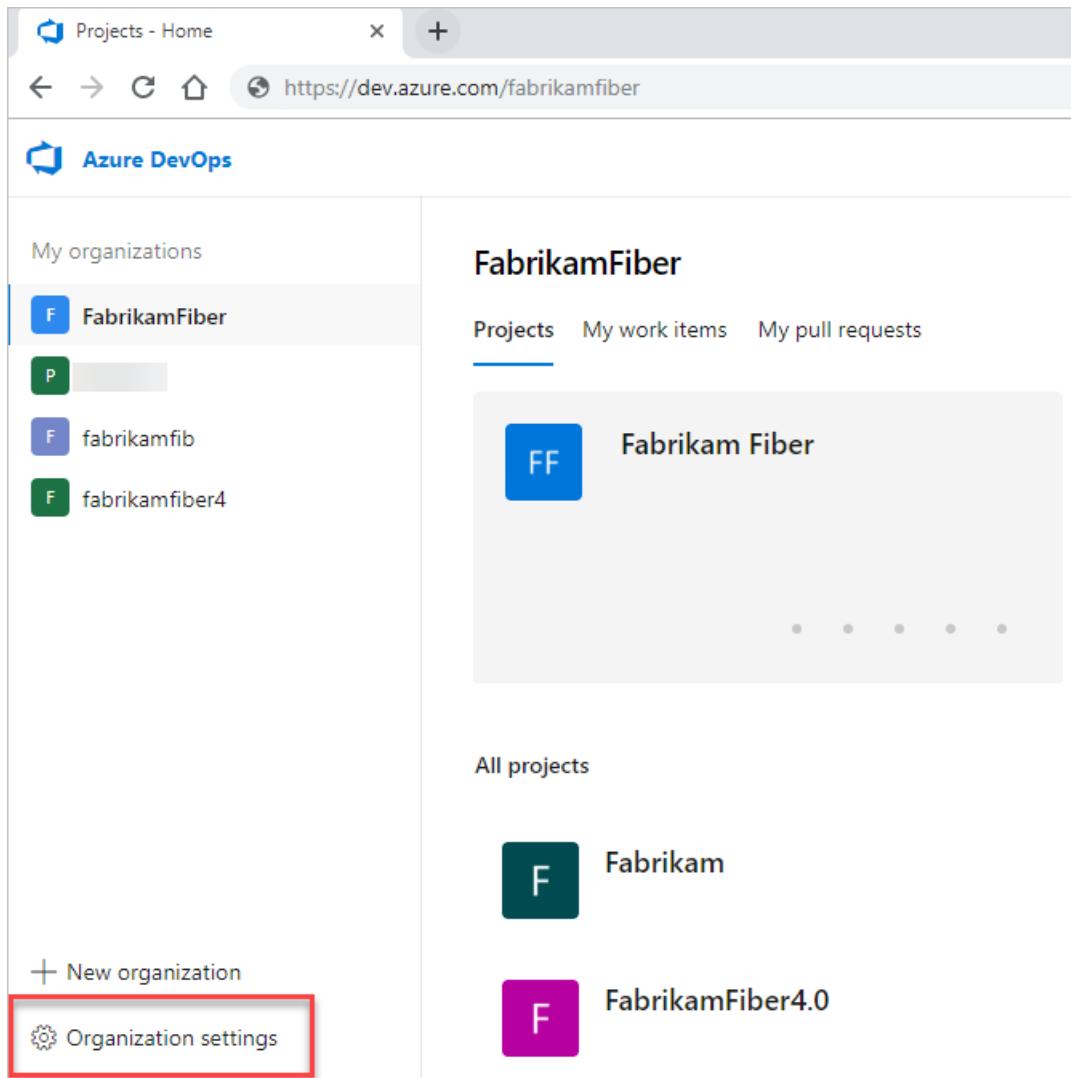
1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Select  **Organization settings**.

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", which is highlighted with a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber" (blue icon), "Fabrikam" (teal icon), and "FabrikamFiber4.0" (purple icon). There are also sections for "All projects" and "Recent activity".

3. Select **Disconnect directory**.

The screenshot shows the "Organization Settings" page under "Azure DevOps". The left sidebar has sections like General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory (which is highlighted with a red box). The main area is titled "Azure Active Directory" and displays a message: "10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory. Delete any unwanted users in Organization settings, and then Resolve for remaining members." It includes a "Resolve" button. Below this, it says "Your organization is connected to the Commerce Test Directory directory." It shows the "Commerce Test Directory" logo, the URL "outlook.onmicrosoft.com", and the Tenant Id: "97ac18ac-aa35-484a-9f52-[redacted]". At the bottom, there's a "Disconnect directory" button highlighted with a red box.

4. Sign out, and then sign back in to Azure DevOps.
5. Prepare your mapping list for inviting users to Azure AD.
 - a. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
 - b. Select  **Organization settings**.



The screenshot shows the Azure DevOps 'Organization settings' page for the organization 'FabrikamFiber'. The left sidebar lists 'My organizations' with items: 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main content area displays the organization name 'FabrikamFiber' and three projects: 'Fabrikam Fiber' (blue card), 'Fabrikam' (dark teal card), and 'FabrikamFiber4.0' (purple card). A horizontal ellipsis indicates more projects.

- c. Select **Users**.

Organization Settings > Users

General

- Overview
- Projects
- Policy
- Users**
- Security
- Notifications
- Extensions
- Usage

Boards

- Process

> Build and release

Manage users

All users Group rules Summary + Add new users

Name ↑	Extensions
 Christie Ch... fabrikamfiber1...	...
 fabrikamfi... fabrikamfiber2...	...
 fabrikamfi... fabrikamfiber5...	...
 fabrikamfi... fabrikamfiber6...	...
 Jamal Hart... fabrikamfiber4...	...

- d. Compare your Azure DevOps email list with your Azure AD email list. Create an Azure AD email address entry for every user who is in the Azure DevOps organization and NOT in the Azure AD. For any user that you don't create an Azure AD email address for, be prepared to invite these users as guests to the Azure AD in future steps.

6. Connect to Azure AD, so users can regain access.

Azure DevOps fabrikamfiber12 / Organization Settings / Azure Active Directory

Organization Settings

General

- Overview
- Projects
- Users**
- Global notifications
- Usage
- Extensions

Azure Active Directory

Connect your organization to an Azure Active Directory.

Follow detailed steps and learn more

Connect directory

Security

Policies

Security

Related articles

- [Disconnect your organization from Azure AD](#)
- [Connect your organization to Azure AD](#)
- [Manage Azure AD groups](#)

Disconnect your organization from Azure Active Directory

5/30/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

To stop using your organization's Azure Active Directory (Azure AD) and return to signing in with Microsoft accounts, disconnect your organization from your directory.

For more information about using Azure AD with Azure DevOps, see the [Conceptual overview](#).

Prerequisites

- Before you disconnect your organization from your directory, make sure to **change the organization owner to a Microsoft account** and not to a school or work account. You can't sign in to your organization unless your work or school account has the same email address as your Microsoft account.
- Add your Microsoft account to the Project Collection Administrator group in Organization Settings and confirm that you have Global Administrator Permissions in your Azure AD for your Microsoft account. You need both because Azure AD users can't disconnect organizations from directories. You can add Microsoft accounts to a directory as external users.

Learn about how to [Manage Azure administrators](#).

What happens to current users? Users can migrate everything except work history. They can reconnect Visual Studio subscriptions and have their access levels reassigned to their new identities.

IMPORTANT

If you want to connect your organization to a different Azure Active Directory at any time, ensure that any connected organizations are disconnected from the original directory BEFORE you delete that directory. Once a new directory is established, connect your organization to the new directory so users can regain access. Learn more about [connecting your organization to Azure AD](#).

Disconnect organization from directory

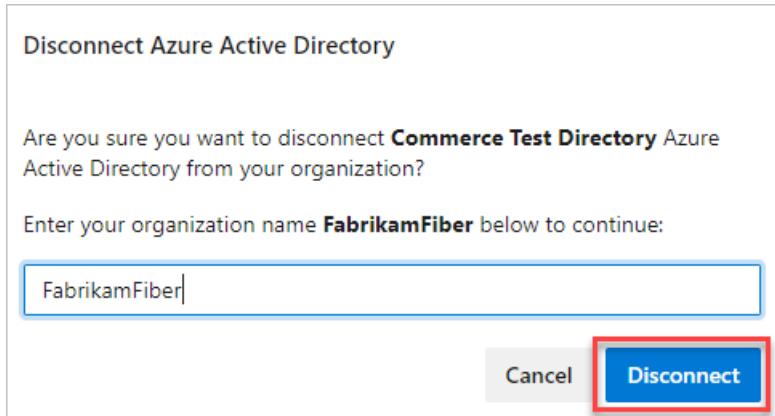
- Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
- Select  **Organization settings**.

The screenshot shows the Azure DevOps home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", which is highlighted with a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber" (blue icon), "Fabrikam" (teal icon), and "FabrikamFiber4.0" (purple icon). At the bottom of the sidebar, there's a "New organization" button.

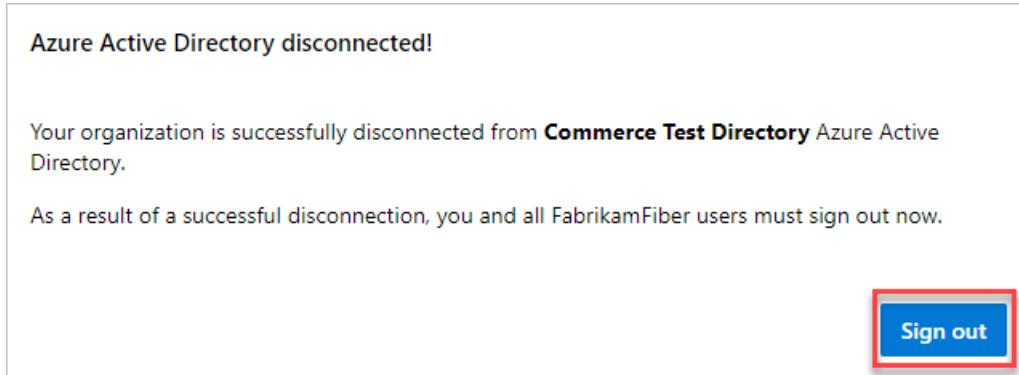
3. Select **Azure Active Directory**, and then select **Disconnect directory**.

The screenshot shows the "Organization Settings" page. The left sidebar has sections like General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory (which is highlighted with a red box). The main area is titled "Azure Active Directory" and shows a warning message: "10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory. Delete any unwanted users in Organization settings, and then Resolve for remaining members." A "Resolve" button is visible. Below this, it says "Your organization is connected to the Commerce Test Directory directory." It shows the "Commerce Test Directory" logo, the URL "outlook.onmicrosoft.com", and the Tenant Id: "97ac18ac-aa35-484a-9f52-[redacted]". At the bottom, there's a "Disconnect directory" button, which is also highlighted with a red box.

4. Enter the name of your organization, and then select **Disconnect**.



5. Select **Sign out**.



Your organization is disconnected from Azure AD. Only users with Microsoft accounts can sign in.

For answers to frequently asked questions about connecting, disconnecting, or changing your Azure AD, see the [FAQ](#).

Related articles

- [Connect your organization to Azure Active Directory](#)
- [Access with Azure AD](#)

2 minutes to read

Add organization users to your Azure Active Directory

Azure DevOps Services

If your organization was created with a Microsoft account, you can connect your organization to your directory (tenant) in [Azure Active Directory \(Azure AD\)](#). Then you can sign in to Azure DevOps with the same user name and password that you use with these Microsoft services. You can also enforce policies for accessing your team's critical resources and key assets.

For more information, see the [conceptual overview](#) for using Azure AD with Azure DevOps.

If your users don't already exist in Azure AD

1. Sign in to the [Azure portal](#) as global administrator for your organization's directory. See the following topics for information about signing in:
 - [Add users in the Azure portal](#)
 - [Add users in the Azure portal](#)
 - [Why am I asked to choose between a "work or school account" and a "personal account"?](#)
2. Add the sign-in addresses for all of your organization users to your directory. Include yourself as the organization owner, if you're not already in the directory.

What does an example directory look like?

Suppose Jamal is an Azure AD global administrator at Fabrikam and is listed in the Fabrikam directory with his work account (jamalhartnett@fabrikam.com). He's also the organization owner and a user with a Microsoft account (jamalhartnett@live.com). He wants to keep his work history, so he adds his Microsoft account to the Fabrikam directory. If Jamal doesn't need his work history, he can use his work account with Azure DevOps. To free up the access used by his Microsoft account, he must change the organization owner to his work account.

Nicole is user at Fabrikam. She has a work account (nicolezamora@fabrikam.com) that shares the same sign-in address as her Microsoft account. Nicole continues to work seamlessly with the same sign-in address.

Here's what the Fabrikam directory might look like in the Azure portal after Jamal adds users from his organization:

The screenshot shows the Microsoft Azure portal's 'Users - All users' page. The top navigation bar includes a 'Secure' lock icon and the user's email address, 'JamalHartnett@fabrik...'. The main content area displays a table of users with columns for NAME, USER NAME, USER TYPE, and SOURCE. The users listed are:

NAME	USER NAME	USER TYPE	SOURCE
Francis Totten	francistotten@live.com	Member	Microsoft Account
Jamal Hartnett	jamalhartnett@live.com	Member	Microsoft Account
Jamal Hartnett	jamalhartnett@fabrika...	Member	Windows Azure AD
Nicole Zamora	nicolezamura@fabrika...	Member	Windows Azure AD

For more information about how to set up users, see this [FAQ](#).

3. After adding your organization users to your directory, [connect your organization to your directory](#).

Related articles

- [Add users to your organization](#)
- [Add users to your team](#)
- [Add external users](#)

2 minutes to read

Troubleshoot permissions and access with Azure Active Directory

6/12/2019 • 14 minutes to read • [Edit Online](#)

Azure DevOps Services

General

Q: I made changes to Azure Active Directory (Azure AD), but they didn't seem to take effect

A: Changes made in Azure AD can take up to 24 hours to be visible in Azure DevOps.

Q: Can I use Office 365 and Azure AD with Azure DevOps?

A: Yes.

- Don't have an organization yet? [Create an organization in Azure DevOps](#).
- Already have an organization? [Connect your organization to Azure AD](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: My organization uses Microsoft accounts only. Can I switch to Azure AD?

A: Yes, but before you switch, make sure that Azure AD meets your needs for sharing work items, code, resources, and other assets with your team and partners.

Learn more about the differences in how you [control access with Microsoft accounts or with Azure AD, and how to switch when you're ready](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface for managing organizations. On the left, under 'My organizations', the 'FabrikamFiber' organization is selected, indicated by a blue border around its card. Other organizations listed include 'P' (grayed out), 'fabrikamfib', and 'fabrikamfiber4'. Below this is a section for 'All projects' which lists 'Fabrikam' and 'FabrikamFiber4.0'. At the bottom of the left sidebar, there are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' being the one highlighted with a red box.

2. Find the current owner.



Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.



Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Understand Azure AD groups

Q: Why can't I assign Azure DevOps permissions directly to an Azure AD group?

A: Because these groups are created and managed in Azure, you can't assign Azure DevOps permissions directly or secure version control paths to these groups. You'll get an error if you try to assign permissions directly.

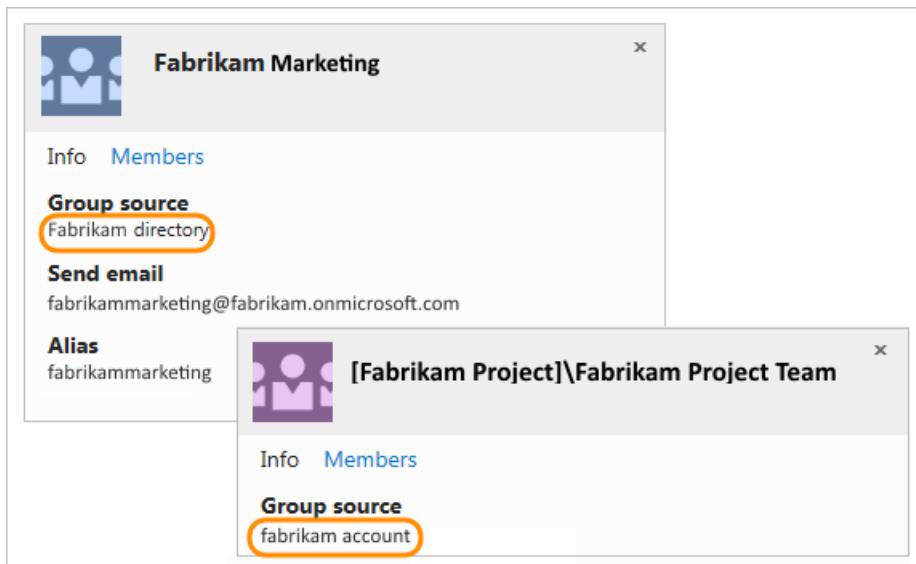
You can add an Azure AD group to the Azure DevOps group that has the permissions you want. Or, you can assign these permissions to the group instead. Azure AD group members inherit permissions from the group where you add them.

Q: Can I manage Azure AD groups in Azure DevOps?

A: No, because these groups are created and managed in Azure. Azure DevOps doesn't store or sync member status for Azure AD groups. To manage Azure AD groups, use the [Azure portal](#), Microsoft Identity Manager (MIM), or the group management tools that your organization supports.

Q: How do I tell the difference between an Azure DevOps group and an Azure AD group?

A: On the group's identity card, check the group's source.



Q: Why doesn't Users show all Azure AD group members?

A: These users have to sign in to your organization before they appear in Users.

Q: How do I assign organization access to Azure AD group members?

A: When these group members sign in to your organization for the first time, Azure DevOps assigns an access level to them automatically. If they have [Visual Studio subscriptions](#), Azure DevOps assigns the respective access level to them. Otherwise, Azure DevOps assigns them the next "best available" [access level](#), in this order: Basic, Stakeholder.

If you don't have enough access levels for all Azure AD group members, those members who sign in get a Stakeholder access.

Q: Why doesn't the Security tab show all members when I select an Azure AD group?

A: The Security tab shows Azure AD group members only after they sign in to your organization, and have an access level assigned to them.

To see all Azure AD group members, use the [Azure portal](#), MIM, or the group management tools that your organization supports.

Q: Why doesn't the team members widget show all Azure AD group members?

A: The team members widget shows only users who previously signed in to your organization.

Q: Why doesn't the team capacity pane show all Azure AD group members?

A: The team capacity pane shows only users who previously signed in to your organization. To set capacity, manually add users to your team.

Q: Why doesn't the team room show offline users?

A: The team room shows Azure AD group members, but only when they're online.

Q: Why doesn't Azure DevOps reclaim access levels from users who aren't Azure AD group members anymore?

Azure DevOps doesn't automatically reclaim access levels from these users. To manually remove their access, go to [Users](#).

Q: Can I assign work items to Azure AD group members who haven't signed in?

A: You can assign work items to any Azure AD member who has permissions for your organization. This also adds that member to your organization. When you add users this way, they'll automatically appear in Users, with the best available access level. They'll also appear in the security settings.

Q: Can I use Azure AD groups to query work items by using the "In Group" clause?

A: No, querying on Azure AD groups is unsupported.

Q: Can I use Azure AD groups to set up field rules in my work item templates?

A: No, but you might be interested in our [process customization plans](#).

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Add users to directory

[Add organization users to your Azure Active Directory](#).

Q: Can I switch current users from Microsoft accounts to work accounts in Azure DevOps?

A: No. Although you can add new work accounts to your organization, they're treated as new users. If you want to access all your work, including its history, you must use the same sign-in addresses that you used before your organization was connected to your Azure AD. You can do this by adding your Microsoft account as a member to your Azure AD.

Q: Why can't I add users from other directories to my Azure AD?

A: You must be a member or have read access in those directories. Otherwise, you can add them [using B2B collaboration through your Azure AD administrator](#). You can also add them by using their Microsoft accounts, or by creating new work accounts for them in your directory.

Q: How do I use my work or school account with my Visual Studio with MSDN subscription?

A: If you used a Microsoft account to activate a [Visual Studio with MSDN subscription](#) that includes Azure DevOps as a benefit, you can add a work or school account. The account must be managed by Azure AD. Learn [how to link work or school accounts to Visual Studio with MSDN subscriptions](#).

Q: Can I control access to my organization for external users in the connected directory?

A: Yes, but only for external users who are [added as guests through Office 365](#) or [added using B2B collaboration by your Azure AD administrator](#). These external users are managed outside the connected directory. To learn more, contact your Azure AD administrator. The following setting doesn't affect [users who are added directly to your organization's directory](#).

Before you start, make sure you have at least Basic access, not Stakeholder.

Complete the following steps to control organization access for external users added through Office 365 or Azure AD B2B collaboration.

1. Go to **Organization settings**.

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and shows 'Projects' (selected), 'My work items', and 'My pull requests'. It displays a card for 'Fabrikam Fiber' and lists other projects: 'All projects', 'Fabrikam', and 'FabrikamFiber4.0'.

2. Select **Policy** and choose to allow or deny organization access for external users added as guests.

The screenshot shows the 'Organization Settings > Policy' page. The left sidebar has sections like General (Overview, Projects, Policy selected), Users, Security, Notifications, Extensions, and Usage. The right panel is titled 'Policy' and contains two main sections: 'Application connection policies' and 'Security policies'. Under 'Application connection policies', 'Alternate authentication credentials' and 'Third-party application access via OAuth' are set to 'On'. Under 'Security policies', 'External guest access' is set to 'On' (highlighted by a red box) and 'Anonymous access to projects' is set to 'Off'.

Remove users or groups

Q: How do I remove an Azure AD group from Azure DevOps?

A: Go to your project collection or project. In the bar at the top, select the gear icon, and then select **Security**.

Find the Azure AD group, and delete it from your organization.

The screenshot shows the Azure DevOps Security interface. On the left, there's a sidebar with options like 'Create group' and 'Filter users and groups'. Below that is a list of 'Azure DevOps Services Groups' with items like 'Contributors', 'Project Administrators', and 'Project Collection Admi...'. The main area shows a group named 'Fabrikam > Project Administrators'. The 'Members' tab is selected. It lists two users: 'Project Collection Build Se... [Fabrikam Project]' and 'Christie Church'. The 'Remove' button next to the first user is highlighted with a red box.

Q: Why am I asked to remove a user from an Azure AD group when I delete that user from my organization?

A: Users can belong to your organization, both as individuals and as members of Azure AD groups that were added to Azure DevOps groups. These users can still access your organization while they're members of these Azure AD groups.

To block all access for these users, remove them from Azure AD groups in your organization, or remove these groups from your organization. Although we'd like to make it possible to block access completely or make exceptions for such users, Azure DevOps doesn't currently have this capability.

Q: If an Azure AD user is removed, will all their related PATs be revoked as well?

A: When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials.

Connect, disconnect, or change Azure AD

- [Connect your organization to Azure AD](#)
- [Disconnect your organization from your directory](#)
- [Change the directory that's connected to Azure DevOps](#)

Q: Can I connect my organization to an Azure AD created from Office 365?

A: Yes. If you can't find your Azure AD created from Office 365, see [Why don't I see the directory that I want to connect?](#).

Q: Why don't I see the directory that I want to connect to? What should I do?

A: This might happen due to any of the following circumstances:

- You don't have [organization Owner permissions](#) to manage directory connections.
- Talk to your Azure AD organization administrator and ask them to make you a member of the organization. It's possible that you're not part of the organization.

Q: Why is my organization already connected to a directory? Can I change that directory?

A: Your organization was connected to a directory when the organization owner created the organization, or sometime after that. When you create an organization with a work or school account, your organization is automatically connected to the directory that manages that work or school account. You can [disconnect your](#)

organization from this directory, and [reconnect to another directory](#). You might have to migrate some users.

Q: My alternate credentials don't work anymore. What do I do?

A: This happens after you connect your organization to a directory. [Set up your credentials](#) again for the organization that you connected.

Q: Some users are disconnected, but they have matching identities in Azure AD. What should I do?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

The screenshot shows the 'Organization Settings' page in the Azure DevOps portal. On the left, there's a sidebar with various options like General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' option is highlighted with a red box. The main content area is titled 'Azure Active Directory'. It displays a message: '10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory.' Below this message is a 'Resolve' button, which is also highlighted with a red box. Further down, it says 'Your organization is connected to the Commerce Test Directory' and provides details: 'Commerce Test Directory', 'mstestvscommerceoutlook.onmicrosoft.com', and 'Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5'. At the bottom of this section is a 'Disconnect directory' button.

- Match the identities. Select **Next** when you're done.

Resolve disconnected users



Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

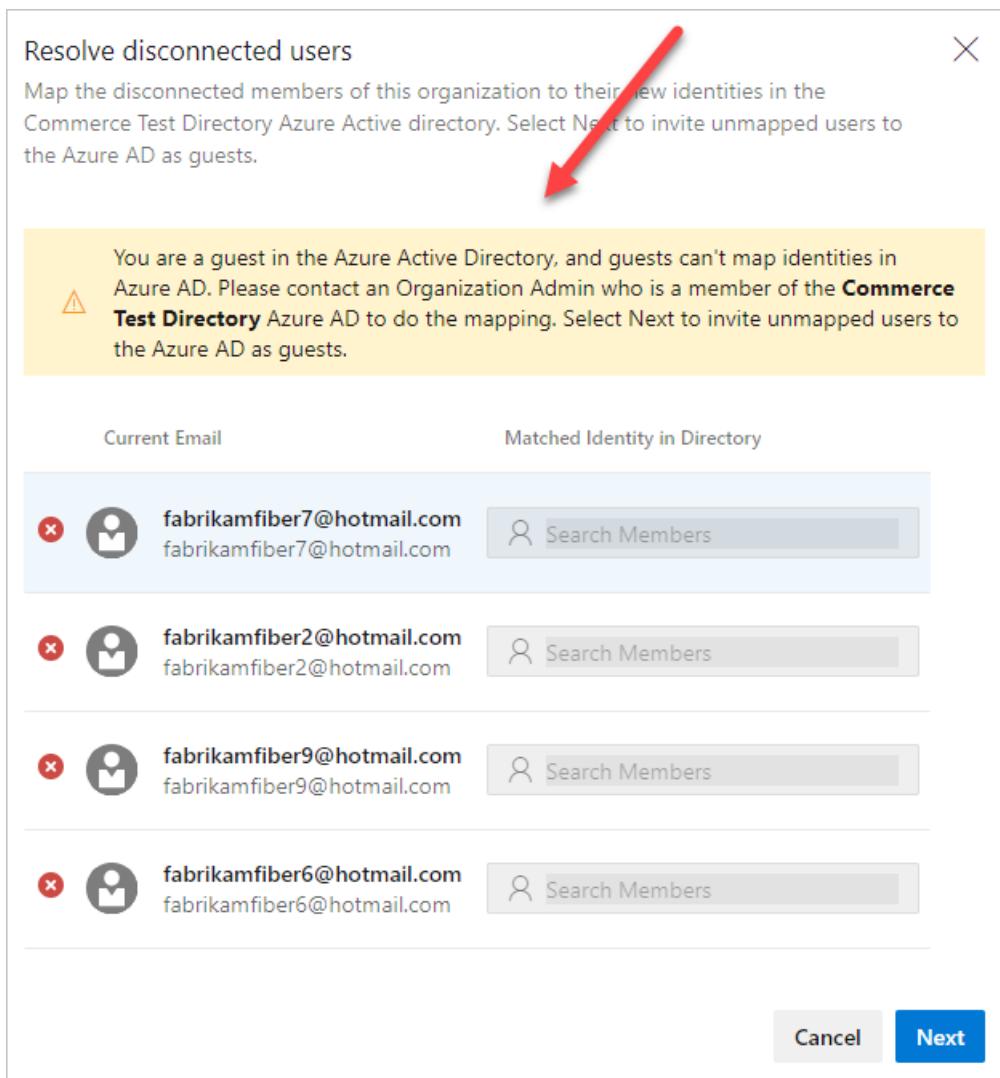
Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
CR fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: I got an error message when I was resolving disconnections. What should I do?

A:

- Try again.
- You might be a guest in Azure AD. Request that an organization administrator, who is a member of Azure AD, do the mapping. Or, request that an admin of the Azure AD convert you to a member.



- If the error message includes a user in your domain, but you don't see them active in your directory, the user likely left your company. Go to the organization user settings to remove the user from your organization.

Q: When I was trying to invite a new user to my Azure AD, I got a 403 forbidden exception. What do I do?

A: You may be a guest in Azure AD and don't have the right permission to invite users. Go to **External collaboration settings** in Azure AD and move the "Guests can invite" toggle to **Yes**. Refresh Azure AD and try again.

Q: Will my users keep their existing Visual Studio subscriptions?

A: Visual Studio subscription administrators ordinarily assign subscriptions to users' corporate email addresses, so that users can receive welcome email and notifications. If the identity and subscription email addresses match, users can access the benefits of the subscription. As you transition from Microsoft to Azure AD identities, users' benefits still work with their new Azure AD identity. But, the email addresses must match. If the email addresses don't match, your subscription administrator must [reassign the subscription](#). Otherwise, users must [add an alternate identity to their Visual Studio subscription](#).

Q: What if I'm required to sign in when I use the people picker?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: What if my email account isn't found in Azure AD?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

Organization Settings

Azure Active Directory

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory**

Your organization is connected to the **Commerce Test Directory** directory.

Commerce Test Directory
mstestvscommerceoutlook.onmicrosoft.com
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Disconnect directory

- Match the identities. Select **Next** when you're done.

Resolve disconnected users

Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

Current Email	Matched Identity in Directory
(X) fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
(X) CR fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
(X) fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
(X) fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: What if my work items are indicating that the users aren't valid?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: Once my organization is connected to Azure AD, will it update Azure Boards work items, pull requests, and other pieces where I'm referenced in the system with my new ID?

A: Yes, all pieces in the system are updated with the new ID when a user's ID is mapped from their personal email to their work email.

Q: What if I get a warning about members who will lose access to the organization?

A: You can still connect to Azure AD, but try to resolve the mapping issue after you've connected. If you still need help, [contact support](#).

Azure Active Directory Connection

Connect your organization to a directory.

You are signed in as

 Jamal Hartnett
fabrikamfiber4@hotmail.com

Azure Active Directory

Commerce Test Directory

 Commerce Test Directory
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Warning: Some members will lose access to the FabrikamFiber organization

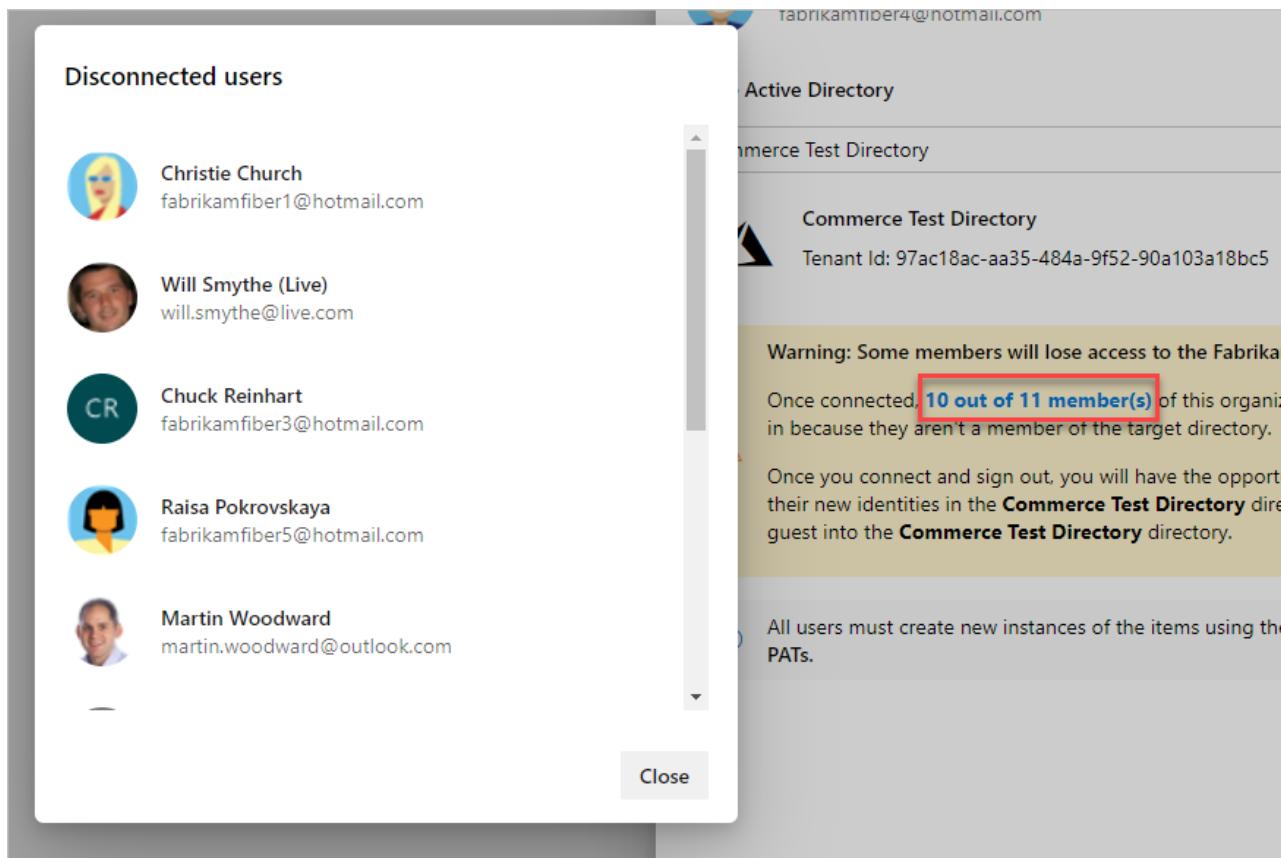
Once connected, **10 out of 11 member(s)** of this organization won't be able to sign in because they aren't a member of the target directory.

 Once you connect and sign out, you will have the opportunity to map these users to their new identities in the **Commerce Test Directory** directory, or to invite them as a guest into the **Commerce Test Directory** directory.

 All users must create new instances of the items using their work account: SSH Keys, PATs.

Cancel Connect

Select the bolded text to see which users are affected.



Q: What if I have over 100 users and want to connect to Azure AD?

A: If you have more than 100 users, [contact support](#).

Q: I have more than 100 members in my Azure DevOps organization, how can I connect to an Azure AD?

A: Currently, the in-app feature doesn't support connections for organizations with over 100 members. Please [contact support](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Add a group rule to assign access levels and extensions

6/20/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Azure DevOps includes group-based licensing for Azure Active Directory (Azure AD) groups and Azure DevOps groups. You can add a group rule to assign an access level or extension to a group. Resources in Azure DevOps are assigned to all members of the group. Group rules are used only for *licensing* and not for permissions.

When users leave the group, the licenses are freed and returned to your pool. You don't need to automate license management to reflect changes in your organizational structure on a per-user basis.

NOTE

We recommend that you reevaluate rules regularly on the **Group** rules tab of the **Users** page. Clarify whether any group membership changes in Azure AD might affect your organization. Automated reevaluation occurs every six hours and any time the group rule changes.

Prerequisites

To manage licenses and group rules, you must be a Project Collection Administrator (PCA) for the organization. If you're not a member of the **Project Collection Administrators** group, [get added as one](#). To assign an extension to a user (and consequently, a group) a PCA must first [install the extension](#) on the organization.

Add group rule

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

The screenshot shows the Azure DevOps Home page. On the left, under 'My organizations', the 'FabrikamFiber' project is selected, highlighted with a blue border. Below it are other organization items: 'P', 'fabrikamfib', and 'fabrikamfiber4'. At the bottom of this list are two buttons: '+ New organization' and 'Organization settings', with 'Organization settings' also having a red border around it. The main content area is titled 'FabrikamFiber' and shows a summary card for 'Fabrikam Fiber' with a blue icon containing 'FF'. Below this are cards for 'All projects', 'Fabrikam' (with a teal icon containing 'F'), and 'FabrikamFiber4.0' (with a purple icon containing 'F').

3. Go to the **Security** page and check the membership of the **Project Collection Administrators** group.

The screenshot shows the 'Organization Settings' page. On the left, the 'General' sidebar has a red box around the 'Security' option. The main content area shows the 'Create group' interface. In the 'Members' tab, there is a list of users. One user, 'Project Collection Service ... [fabrika]', is highlighted with a red box. The 'Permissions' tab is also visible. The breadcrumb navigation at the top right shows 'Fabrikam Fiber > Project Collection Settings'.

4. Select **Users > Group rules**. This view shows you all of your created group rules.

Organization Settings > Users

General

- Overview
- Projects
- Policy
- Users**
- Security

Manage users

All users **Group rules**

Name ↑

5. Select **Add a group rule**.

Organization Settings > Users

General

- Overview
- Projects

Manage users

All users **Group rules** Summary

Name ↑

+ Add a group rule

6. Complete the dialog box for the group for which you want to create a rule. Include an access level for the group and any optional project access or extensions for the group. Select **Add**.

Add a group rule

Azure DevOps or Azure AD group *

[fabrikam-fiber]\Project Collection Valid Users

Create a new Azure DevOps group

Access level *

Basic

^ Add to projects

Projects

FabrikamFiber

Azure DevOps Groups

Project Contributors

> Assign extensions

Add Cancel

A notification is displayed that shows the status and outcome of the rule. If the assignment couldn't be completed (for example, because your organization didn't have enough purchased licenses), select **View status** to see the details.

Users

1 actions completed successfully. Add Project Collection Valid Users group rule. [View status](#)

Manage users

All users Group rules | Summary + Add a group rule ⚡ Re-evaluate Rules

Name ↑	Extensions	Access Level
 Project Col... [fabrikam-fiber]\...	...	Basic

Resolve assignment errors

As users sign in to your organization, they're assigned access levels and extensions based on their group memberships. If there aren't enough licenses or extensions to assign the specified resources to the user, based on their group memberships, Azure DevOps notifies all **Project Collection Administrators** via email that further resources need to be purchased. To find users in an error state, the Project Collection Administrator can do the following steps:

1. Go to the **Users** page in **Organization settings**. A notification on the page indicates there are users who are missing extensions or access levels.
2. To see how many of each resource are missing, choose **Fix assignment errors**.
3. Complete purchases for any missing resources, and then choose **Fix errors** to have the purchases automatically assigned to the specified users.

Manage group members

1. Highlight a group rule and from the command bar, select **Manage members**.

Manage users

All users Group rules | Change access level Manage projects

Name ↑	Extensions
 Project Col... [fabrikam-fiber]\...	

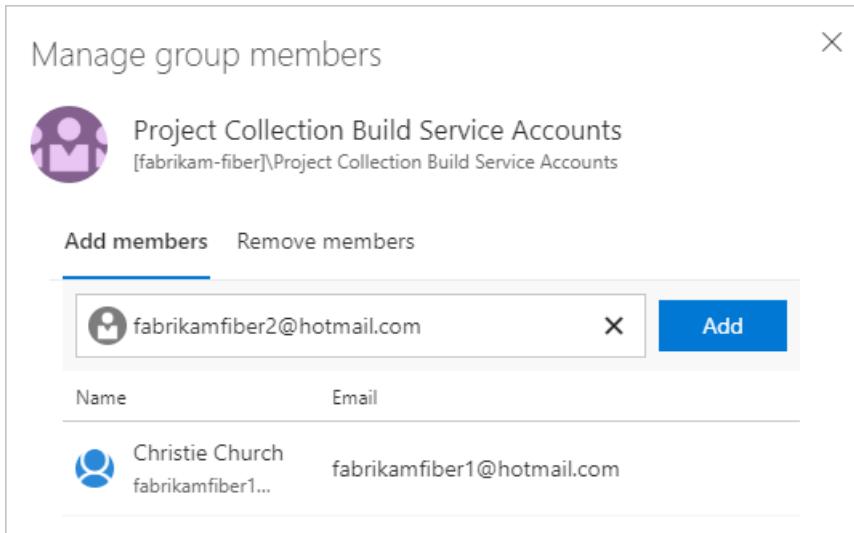
⋮

- Change access level
- Manage projects
- Manage extensions
- Manage members**
- Remove rule

NOTE

Leave existing automation for managing access levels or extensions for users running as-is (for example, PowerShell). The goal is to reflect the same resources that the automation is applying to those users.

2. Add members and select **Add**.



When the same access level or extension is assigned to the user both directly and through a group, the user consumes only one access level or extension. No additional licenses are required to perform the migration.

Verify group rule

- Verify that the resources are applied to each group. On the **Group rules** tab, highlight a group and select **Summary**.
- Verify individual user resources. On the **Users** page, highlight a user and select **Summary**.
- Verify that no assignments have failed. On the **Users** page, on the **Groups** tab, check for assignment errors.

Your group rule is in effect.

Related articles

- [Buy and install extensions](#)
- [Install Active Directory and Azure Active Directory users or groups to a built-in security group](#)

Remove direct assignments from users in Azure DevOps

4/27/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

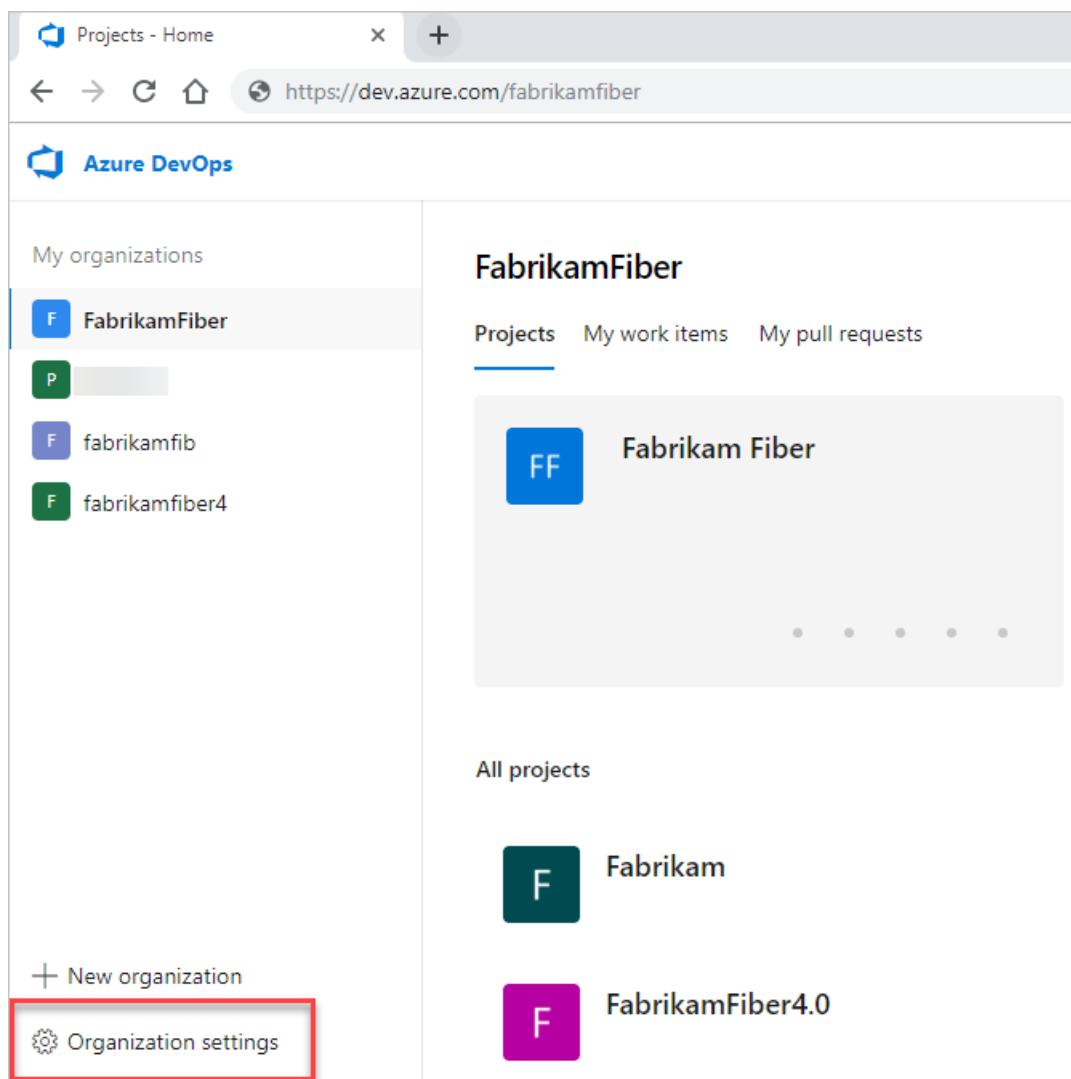
To manage a user's resources only by the groups that they're in, you must remove the direct assignments. Resources that are directly assigned to a user via individual assignment stay assigned to the user, whether the resources are assigned or taken away from the user's groups.

Prerequisites

- You must be a member of the **Project Collection Administrators** group for the organization that you would like to manage users' direct assignments.

Remove assignments

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



3. Select the **Users** tab.

Organization Settings > Users

General

- Overview
- Projects
- Policy
- Users**

Manage users

All users Group rules

Name
Name ↑

4. Select all users with resources that should be managed only by groups.

Manage users

All users Group rules Summary Change access level Manage extensions ...

Name	Extensions	...
Name ↑	Extensions	A <input checked="" type="checkbox"/> Remove direct assignments
<input checked="" type="checkbox"/>  Jamal Hart... fabrikamfiber4...	...	Early Adopter
<input checked="" type="checkbox"/>  Johnnie M... fabrikamfiber5...	...	Early Adopter

5. To confirm that you want to remove the direct assignments, select **Remove**.

Direct assignments are removed from the users.

NOTE

If a user isn't a member of any groups, then the user isn't affected.

Related articles

- [What is Azure Active Directory B2B Collaboration?](#)
- [Migrate to group-based resource management](#)
- [Assign access levels and extensions to users by group membership](#)

Troubleshoot creating an organization

6/18/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: What users can join for free? What benefits do users get from joining Azure DevOps?

A: Azure DevOps is free for these users to join:

- Five users who get [Basic features](#), like version control and tools for Agile, Java, and build and release management.
- Unlimited users who get [Stakeholder features](#), like working with your backlog, work items, and queries.
- Unlimited [Visual Studio subscribers](#) who also get Basic features. In some cases, these users get additional features, like [Azure Test Plans](#).

[Learn what else you get with Azure DevOps.](#)

Q: Why won't my browser work with Azure DevOps?

A: This might happen if you're using an unsupported browser. For the best experience, make sure that you're using a [supported browser](#).

Q: Which Visual Studio subscriptions can I use with Azure DevOps?

A: [Find Visual Studio subscriptions that include Azure DevOps.](#)

Q: Why am I asked to provide profile details?

A: If you're a new user, you can change your profile details. You need to do this only once.

1. Confirm your profile details.

The screenshot shows a form titled "We need a few more details". It contains three input fields: "Your name" with the value "Jamal Hartnett", "From" with the value "United States" and a dropdown arrow, and "We'll reach you at" with the value "jamalhartnett@outlook.com".

We need a few more details

Your name:
Jamal Hartnett

From:
United States

We'll reach you at:
jamalhartnett@outlook.com

2. Continue creating your organization.



[Edit profile](#)

Jamal Hartnett

jamalhartnett@outlook.com

United States

jamalhartnett@outlook.com



Get started with Visual Studio Team Services

Services for teams to share code, track work, and ship software – for any language, all in a single package.

[Create new account](#)

Q: How do I find the region where my organization is located?

A: [Find your organization's region](#)

Q: How do I change my project name, organization location, or process?

A: Change these when you sign up for your organization.

Azure DevOps uses Agile as the default [process](#) to organize your work. Your organization's default location is based on the closest [Microsoft Azure region](#) where Azure DevOps is available. For a better experience, select a location that's closest to most users in your organization.

If a new region or location opens later, you can [change your organization location or region](#). You can also select another process, like Scrum, if that works best for you.

If you connected your organization to Azure Active Directory but you belong to multiple directories and want to select a different directory, change your directory here:

Q: Why are some features not available in my organization?

A: Some features require you to install an extension, which might be available for free or paid.

For example, web-based test case management requires [Azure Test Plans](#). You can try the Basic + Test Plans trial if you haven't started it already. Otherwise, you can [pay for user access](#).

Q: How many organizations can I create?

A: You can [create multiple organizations](#). But instead of creating another organization, you might consider [creating another project](#). Your organization can have unlimited private projects by using Git or Microsoft Team Foundation Version Control.

There's no limit to the number of organizations that you can join.

Q: How do I create another organization?

A: Just sign in to your [Visual Studio profile](#).



Visual Studio Team Services accounts

› fabrikam.visualstudio.com (Owner)

[Create new account](#)

Q: Can I create more than one project?

A: Yes, multiple projects help you keep work separate when you have development projects for different teams. Only one project collection is supported.

To create projects, you need project collection administrator or organization owner permissions. For details, see [Create a project](#).

To learn more about projects and when you should or shouldn't add one, see [About projects and scaling your organization](#).

Q: Can I delete a project that I created?

A: Yes, you can [delete a project](#) that you don't use anymore.

Q: Where can I find my organization name (URL)?

A: [Sign in to your Visual Studio profile](#) to find your organization list.

Q: What happens if I forget my password?

A: You can [recover your Microsoft account password](#) or [recover your work or school account password](#) if your organization turned on this feature. Otherwise, contact your Azure Active Directory administrator to recover your work or school account.

Q: Can I change my organization name (URL) or owner?

A: Yes. If you have at least Basic access, you can do this in your organization settings. Learn how to:

- [Rename your organization](#).
- [Change the organization owner](#).

Q: Can I delete an organization that I don't need anymore?

A: Yes. See [Delete or recover your organization](#).

Q: What's the difference between using a Microsoft account and a work account or school account to sign up?

A: Your choice of account type affects how you control access and authenticate users for your organization.

When you sign up with a Microsoft account:

- You're solely responsible for managing access to your organization.
- All users must sign in with Microsoft accounts.

When you sign up with a work or school account:

- Your organization is automatically connected to your directory in Azure Active Directory.
- All users must be members in the connected directory to get access to your organization.
- The directory administrator has control over who can join the directory.
- You sign in with work or school accounts, or with Microsoft accounts if your company allows that.

To [add users to the directory](#), you must be a directory administrator. If you don't have access, work with your directory administrator to add users. Learn more about [work or school accounts for your organization](#).

Q: Can I change the directory after signup?

A: Yes, see [Disconnect your organization from Azure Active Directory](#) and [Connect your organization to Azure AD](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Choose **Work or school account** if you want to use your directory to authenticate users and control organization access. This option limits access to members in your organization's directory. In this case, all other users also must sign in with work or school accounts.
- Choose **Personal account** if you want to use your Microsoft account with Azure DevOps. In this case, all other users also must sign in with Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do you store, secure, and protect my data?

A: Azure DevOps storage features help make sure that your data is available in case of hardware failure, service disruption, or datacenter disasters. Azure DevOps helps protect data from accidental or malicious deletion.

We follow industry best practices and have enterprise-grade security measures to help protect your code and project data. Also, all communication between your computer and the service takes place over an encrypted HTTPS connection. Learn [how your data is secured and protected](#).

Q: Do I still own my code and intellectual property? What do you do with my personal information?

A: Yes, your code and your intellectual property are yours. Please review our [terms of service](#) and [privacy policy](#).

Q: Where can I find the Azure DevOps SLA?

A: You can find it here: [Azure DevOps SLA](#).

Q: I'm having problems with my Visual Studio subscription. How can I get help?

A: Try [Subscription Support](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot adding and deleting organization users

7/3/2019 • 12 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Permissions

Q: Why can't I manage users?

A: To access and manage users, you must have Azure DevOps [project collection administrator](#) or [organization owner](#) permissions.

Q: How do I find a Project Collection Administrator?

A: If you have at least Basic access, you can find your [Project Collection Administrator](#) in your organization's security settings.

1. See [Show members of the Project Collection Administrators group](#).
1. See [Show members of the Project Administrators group](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your **Organization settings**.

The screenshot shows the Azure DevOps interface for managing organizations. On the left, there's a sidebar with 'My organizations' containing items like 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. At the bottom of this sidebar are links for '+ New organization' and 'Organization settings'. The main area shows the details for 'FabrikamFiber', including its projects ('Fabrikam Fiber', 'Fabrikam', 'FabrikamFiber4.0'), work items, and pull requests. The 'Organization settings' link in the sidebar is highlighted with a red box.

2. Find the current owner.

Q: Why don't users appear or disappear promptly in Azure DevOps after I add or delete them in the Users hub?

A: If you experience delays finding new users or having deleted users promptly removed from Azure DevOps (for example, in drop-down lists and groups) after you add or delete users, [file a problem report on Developer Community](#) so we can investigate.

Visual Studio subscriptions

Q: When do I select "Visual Studio/MSDN Subscriber"?

A: Assign this access level to users who have active, valid [Visual Studio subscriptions](#). Azure DevOps automatically recognizes and validates Visual Studio subscribers who have Azure DevOps as a benefit. You need the email address that's associated with the subscription.

For example, if a user selects **Visual Studio/MSDN Subscriber** but the user doesn't have a valid, active Visual Studio subscription, the user can work only [as a Stakeholder](#).

Q: Which Visual Studio subscriptions can I use with Azure DevOps?

A: See [Azure DevOps benefits for Visual Studio subscribers](#).

Q: Why won't my Visual Studio subscription validate?

A: See [Why won't Azure DevOps recognize my Visual Studio subscription?](#)

Q: Why do Visual Studio subscriber access levels change after a subscriber signs in?

A: Azure DevOps recognizes Visual Studio subscribers. Azure DevOps automatically assigns a user access that's based on the user's subscription and not on the current access level that's assigned to the user.

Q: What happens if a user's subscription expires?

A: If no other access levels are available, users can [work as Stakeholders](#). To restore access, a user must renew their subscription.

Q: What happened to Visual Studio Online Professional?

A: On December 1, 2015, we replaced Visual Studio Online Professional with the [Visual Studio Professional monthly subscription](#).

Although a Visual Studio Online Professional purchase now appears on your monthly invoice as a Visual Studio Professional monthly subscription, you need to transition manually to get the new offering. The transition provides an upgrade by offering access to unlimited organizations (not just one organization) like Visual Studio Online Professional.

The rest stays the same. You get monthly access to the Visual Studio Professional IDE. Pricing remains the same at \$45 per user, per month. Learn more about [Visual Studio subscriptions](#).

If you're purchasing user access to Visual Studio Professional for a specific organization (possible only if you purchased before November 2015) and want to upgrade, do the following:

1. Before the last day of the calendar month, sign in to your organization (
<https://dev.azure.com/{yourorganization}>).
2. Select  **Organization settings**.

The screenshot shows the Azure DevOps portal interface. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "[redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main content area is titled "FabrikamFiber" and shows tabs for "Projects", "My work items", and "My pull requests", with "Projects" selected. It displays a card for "Fabrikam Fiber" with a blue "FF" icon. Below this is a section titled "All projects" with cards for "Fabrikam" (green "F" icon) and "FabrikamFiber4.0" (pink "F" icon).

3. Select **Billing**.

The screenshot shows the "Organization Settings" page. On the left, there's a sidebar with the following options: General, Overview, Projects, Users, **Billing** (highlighted by a red box), Global notifications, Usage, Extensions, and Azure Active Directory.

4. Reduce the number of paid Visual Studio Online Professional users to 0.

This change takes effect on the first day of the next month. For the rest of the current calendar month, you aren't billed for any Visual Studio Online Professional users.

5. On the first day of the next calendar month, [go to Visual Studio Marketplace Subscriptions > Visual Studio Professional - monthly subscription](#), and buy Visual Studio Professional monthly subscriptions for the same users. Learn [how to buy Visual Studio subscriptions](#).

User access

Q: What does "Last Access" mean in the All Users view?

The value in **Last Access** is the last date a user accessed any resources or services. Accessing Azure DevOps includes using *organizationname.visualstudio.com* directly and using resources or services indirectly. For example, you might use the [Azure Artifacts](#) extension, or you might access the service by pushing code to Azure DevOps from a Git command line or IDE.

Q: Can a user who has paid for Basic access join other organizations?

A: No, a user can join only the organization for which the user has paid for Basic access. But a user can join any organization where free users with Basic access are still available. The user can also join as a user with Stakeholder access for free.

Q: Why can't users access some features?

A: Make sure that users have the correct [access level](#) assigned to them.

- Learn [how to manage users and access levels for Azure DevOps](#).
- Learn [how to change access levels for Team Foundation Server](#).

Some features are available only as [extensions](#). You need to install these extensions. Most extensions require you to have at least Basic access, not Stakeholder access. Check the extension's description in the [Visual Studio Marketplace](#), Azure DevOps tab.

For example, to search your code, you can install the free [Code Search extension](#), but you need at least Basic access to use the extension.

To help your team improve app quality, you can install the free [Test & Feedback extension](#), but you get different capabilities based on your access level and whether you work offline or connected to Azure DevOps Services or Team Foundation Server (TFS).

To create test plans, assign the [Basic + Test Plans access level](#). Some [Visual Studio subscribers](#) can use this feature for free, but Basic users need to upgrade to Basic + Test Plans access before they can create test plans.

- Learn [how to get extensions for Azure DevOps](#).
- Learn [how to get extensions for TFS](#).
- Learn [how to buy access to TFS Test](#).

Q: Why does a user lose access to some features?

A: This might happen for different reasons (although the user can continue to [work as a Stakeholder](#)):

- The user's Visual Studio subscription has expired. Meanwhile, the user can [work as a Stakeholder](#), 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. This affects all purchases made with this subscription, including Visual Studio subscriptions. To fix this issue, visit the [Azure account portal](#).
- The Azure subscription used for billing was unlinked from your organization. Learn more about [linking your organization](#).
- Your organization has more users with Basic access than the number of users that you're paying for in Azure. Your organization includes five free users with Basic access. If you need to add more users with Basic access, you can [pay for these users](#).

Otherwise, on the first day of the calendar month, users who haven't signed 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](#).

- The user no longer has access to [features that are available only as extensions](#). This might happen for different reasons:
 - The user's access level no longer meets the extension's requirements. Most extensions require at least Basic access, not Stakeholder access. For more information, see the extension's description in the [Marketplace](#).
 - The extension was uninstalled. Users can [reinstall the extension](#).
 - If the extension is a paid extension, the Azure subscription used for billing might be unlinked from your organization or might no longer be active. Learn more about [linking your organization](#) or visit the [Azure portal](#) to check payment details.

Azure Active Directory and your organization

Q: Why do I have to add users to a directory?

A: Your organization authenticates users and controls access through Azure Active Directory (Azure AD). All users must be directory members to get access.

If you're a directory administrator, you can [add users to the directory](#). If you're not an administrator, work with your directory administrator to add users. Learn more about [how to control access by using a directory](#).

Q: How do I find out whether my organization uses Azure AD to control access?

A: If you have at least Basic access, here's how to find out:

Go your **Organization settings**, and then select the **Azure Active Directory** tab. See the following examples of an organization that is not connected, and then an organization that is connected to Azure AD.

The screenshot shows the Azure DevOps Organization Settings interface. On the left, there's a sidebar with a tree view of settings categories: General, Overview, Projects, Users, Billing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' item is highlighted with a red box. Below the sidebar, the status 'Not connected' is displayed. To the right, the main content area is titled 'Azure Active Directory' and contains instructions to 'Connect your organization to an Azure Active Directory.' It includes a 'Follow steps and learn more' link and a 'Connect directory' button. The top navigation bar shows the user's name 'fabrikamfiber13' and the current location 'Organization Settings / Azure A'.

<p>Organization Settings</p> <p>General</p> <ul style="list-style-type: none">OverviewProjectsUsersAuditingGlobal notificationsUsageExtensions <p>Azure Active Directory</p>	<p>Azure Active Directory</p> <p>Your organization is connected to the Directory directory.</p> <p> Directory [REDACTED].onmicrosoft.com Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5</p> <p>Disconnect directory</p>
---	---

If your organization is connected to your organization's directory, only users from your organization's directory can join your organization. Learn [how to control organization access by using Azure AD](#).

Q: My organization controls access by using Azure Active Directory. Can I just delete users from the directory?

A: Yes, but deleting a user from the directory removes the user's access to all organizations and other assets associated with that directory. You must have Azure AD global administrator permissions to [delete a user from your Azure AD directory](#).

Q: Why are "no identities found" when I try to add users from Azure AD to my Azure DevOps organization?

A: You're probably a *guest* in the Azure AD that backs your Azure DevOps organization, rather than a *member*. By default, Azure AD guests can't search the Azure AD in the manner required by Azure DevOps. Learn how to [convert an Azure AD guest into a member](#).

Q: How can I convert an Azure AD guest into a member?

A: Select from the following two options:

- Have the Azure AD administrator(s) remove you from the Azure AD and re-add you, making you an Azure AD *member* rather than a *guest* when they do. For more information, see [Can Azure AD B2B users be added as members instead of guests](#).
- [Change the UserType of the Azure AD guest using Azure AD PowerShell](#). This is an advanced process and is not advised, but it allows the user to query Azure AD from the Azure DevOps organization thereafter.

Convert Azure AD UserType from guest to member using Azure AD PowerShell

WARNING

This is an advanced process and is not advised, but it allows the user to query Azure AD from the Azure DevOps organization thereafter.

Prerequisites

The user making the UserType change must have the following:

- A work/school account (WSA)/native user in Azure AD. You can't do this with a Microsoft Account.
- Global administrator permissions

IMPORTANT

We recommend that you create a brand new (native) Azure AD user who is a global admin in the Azure AD, and then complete the following steps with that user. This new user should eliminate the possibility of connecting to the wrong Azure AD. You can delete the new user when you're done.

Process

1. Sign in to the [Azure portal](#) as global administrator for your organization's directory.
2. Go to the tenant that backs your Azure DevOps organization.
3. Check the UserType. Confirm that the user is a guest.

The screenshot shows the 'Identity' section of the Azure portal's user creation form. It includes fields for Name, User name, First name, Last name, Photo (with a placeholder globe icon), Select a file (for photo upload), User type (set to 'Guest'), Source (set to 'Microsoft Account'), and Object ID. The 'User type' field is highlighted with a red border.

4. Open an Administrative Windows PowerShell prompt.
5. Execute `Install-Module -Name AzureAD`. The [Azure Active Directory PowerShell for Graph](#) downloads from the PowerShell Gallery. You may see prompts about installing NuGet and untrusted repository, as pictured below. If you run into issues please review the system requirements and information at the [Azure Active Directory PowerShell for Graph](#) page.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> Install-Module -Name AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based reposi-
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\trevorh\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet p-
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShell to
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the re
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\windows\system32>
```

6. Once the installation completes, execute `Connect-AzureAD`. You're prompted to sign in to the Azure AD. Be sure to use an ID that meets the criteria above.
7. Execute `Get-AzureADUser -SearchString "<display_name>"`, where `<display_name>` is part of the entire display name for the user, as seen inside the Azure portal). The command returns four columns for the user found - ObjectId, DisplayName, UserPrincipalName, UserType - and the UserType should say `guest`.
8. Execute `Set-AzureADUser -ObjectID <string> -UserType Member`, where `<string>` is the value of ObjectId returned by the previous command. This should set the user to member status.

9. Execute `Get-AzureADUser -SearchString "<display_name>"` again to verify the UserType has changed. You can also verify this in the Azure Active Directory section of the Azure portal. While not the norm, we have seen it take several hours or even days before this change is reflected inside Azure DevOps. If it doesn't fix your Azure DevOps issue immediately, give it some time and keep trying.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

More support

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot adding members to projects

7/3/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Q: Why can't I add any more members to my project?

A: Your organization is free for the first five users with Basic access. You can add unlimited Stakeholders and Visual Studio subscribers for no extra charge. After you assign all five free users with Basic access, you can continue adding Stakeholders and Visual Studio subscribers.

To add six or more users with Basic access, you need to [set up billing in Azure](#). Then you can [pay for more users who need Basic access](#), return to your organization, [add these users](#), and [assign them Basic access](#). When billing is set up, you can pay monthly for the extra users' access. And you can cancel at any time.

If you need more Visual Studio subscriptions, learn [how to buy subscriptions](#).

Q: Why can't some users sign in?

A: This problem might happen because users must sign in with Microsoft accounts unless your organization controls access with Azure Active Directory (Azure AD). If your organization is connected to Azure AD, users must be directory members to get access. See [How do I find out if my organization uses Azure Active Directory \(Azure AD\)?](#)

If you're an Azure AD administrator, you can add users to the directory. If you're not, work with the directory administrator to add them. Learn [how to control organization access with Azure AD](#).

Q: Why can't users access some features?

A: Make sure that users have the correct [access level](#) assigned to them.

- Learn [how to manage users and access levels for Azure DevOps](#).
- Learn [how to change access levels for Team Foundation Server](#).

Some features are available only as [extensions](#). You need to install these extensions. Most extensions require you to have at least Basic access, not Stakeholder access. Check the extension's description in the [Visual Studio Marketplace](#), Azure DevOps tab.

For example, to search your code, you can install the free [Code Search extension](#), but you need at least Basic access to use the extension.

To help your team improve app quality, you can install the free [Test & Feedback extension](#), but you get different capabilities based on your access level and whether you work offline or connected to Azure DevOps Services or Team Foundation Server (TFS).

To create test plans, assign [Basic + Test Plans access level](#). Some [Visual Studio subscribers](#) can use this feature for free, but Basic users need to upgrade to Basic + Test Plans access before they can create test plans.

- Learn [how to get extensions for Azure DevOps](#).
- Learn [how to get extensions for TFS](#).
- Learn [how to buy access to TFS Test](#).

Q: Why did some users lose access to certain features?

A: Loss of access might happen for [different reasons](#).

Q: How do I find out whether my organization uses Azure AD to control access?

A: If you have at least Basic access, here's how to find out:

Go your **Organization settings**, and then select the **Azure Active Directory** tab. See the following examples of an organization that is not connected, and then an organization that is connected to Azure AD.

The screenshot shows the 'Organization Settings' page for an organization named 'fabrikamfiber13'. The left sidebar lists various settings categories: General, Overview, Projects, Users, Billing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' item is highlighted with a red box. Below the sidebar, the status 'Not connected' is displayed. The main content area is titled 'Azure Active Directory' and contains instructions to 'Connect your organization to an Azure Active Directory.' It includes a 'Follow steps and learn more' link and a 'Connect directory' button.

Connected

The screenshot shows the 'Organization Settings' page for a connected organization named 'FabrikamFiber'. The left sidebar lists the same settings categories as the previous screenshot. The 'Azure Active Directory' item is highlighted with a red box. The main content area displays a message stating 'Your organization is connected to the [redacted] Directory directory.' It shows the directory icon, the domain name '[redacted].onmicrosoft.com', and the Tenant Id: '97ac18ac-aa35-484a-9f52-90a103a18bc5'. A 'Disconnect directory' button is present at the bottom of this section.

If your organization is connected to your organization's directory, only users from your organization's directory can join your organization. Learn [how to control organization access by using Azure AD](#).

Q: How do I remove users from my organization?

A: Learn [how to delete users](#) across all projects in your organization. If you paid for more users but don't need their organization access anymore, you must reduce your paid users to avoid charges.

Q: Why can't I find members from my connected Azure AD, even though I'm the Azure AD global admin?

A: You're probably a guest in the Azure AD instance that backs Azure DevOps. By default, Azure AD guests can't search in Azure AD. That's why you aren't finding users in your connected Azure AD to add to your organization.

First, check to see if you're an Azure AD guest:

1. Go to the **Settings** section of your organization. Look at the **Azure Active Directory** section at the bottom. Make a note of the tenant that backs your organization.
2. Sign in to the new Azure portal, portal.azure.com. Check your user profile in the tenant from step 1. Check

the **User type** value shown as follows:

The screenshot shows a user profile creation form. The 'User type' field is highlighted with a red border and contains the value 'Guest'. Other fields visible include Name (Linkia@me.com), User name (Linkia@me.com), First name (Linkia), Last name (Default Directory), Photo (a globe icon), Select a file (button), Source (Microsoft Account), and Object ID (redacted).

If you're an Azure AD guest, do one of the following:

- Have another Azure DevOps admin, who isn't an Azure AD guest, manage the users in Azure DevOps for you. Members of the Project Collection Administrators group inside Azure DevOps can administer users.
- Have the Azure AD admin remove you from the connected Azure AD and re-add you. The admin needs to make you an Azure AD member rather than a guest. See **Can Azure AD B2B users be added as members instead of guests?**
- Change the **User Type** of the Azure AD guest by using Azure AD PowerShell. This is an advanced topic, and we don't advise it. But it works and allows the user to query Azure AD from Azure DevOps thereafter.

1. [Download and install Azure AD PowerShell module](#).

2. Open PowerShell and run the following cmdlets.

a. Connect to Azure AD:

```
C:\Users\rajr> Connect-AzureAD
```

b. Find the **objectId** of the user:

```
C:\Users\rajr> Get-AzureADUser
```

c. Check the **usertype** attribute for this user to see if they're a guest or member:

```
C:\Users\rajr> Get-AzureADUser -objectId cd7d47bf-1c6e-4839-b765-13edcd164e66
```

d. Change the **usertype** from **member** to **guest**:

```
C:\Users\rajr> Set-AzureADUser -objectId cd7d47bf-1c6e-4839-b765-13edcd164e66 -UserType Member
```

Q: Why don't users appear or disappear promptly in Azure DevOps after I add or delete them in the Users hub?

A: If you experience delays finding new users or having deleted users promptly removed from Azure DevOps (for example, in drop-down lists and groups) after you add or delete users, [file a problem report on Developer Community](#) so we can investigate.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I find a Project Collection Administrator?

A: If you have at least Basic access, you can find your [Project Collection Administrator](#) in your organization's security settings.

1. See [Show members of the Project Collection Administrators group](#).
1. See [Show members of the Project Administrators group](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface. On the left, there's a sidebar titled 'My organizations' with a list of projects: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. Under 'Projects', there's a card for 'Fabrikam Fiber' with a blue 'FF' icon. Below it, under 'All projects', are cards for 'Fabrikam' (dark green 'F') and 'FabrikamFiber4.0' (magenta 'F').

2. Find the current owner.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot permissions and access with Azure Active Directory

6/12/2019 • 14 minutes to read • [Edit Online](#)

Azure DevOps Services

General

Q: I made changes to Azure Active Directory (Azure AD), but they didn't seem to take effect

A: Changes made in Azure AD can take up to 24 hours to be visible in Azure DevOps.

Q: Can I use Office 365 and Azure AD with Azure DevOps?

A: Yes.

- Don't have an organization yet? [Create an organization in Azure DevOps](#).
- Already have an organization? [Connect your organization to Azure AD](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: My organization uses Microsoft accounts only. Can I switch to Azure AD?

A: Yes, but before you switch, make sure that Azure AD meets your needs for sharing work items, code, resources, and other assets with your team and partners.

Learn more about the differences in how you [control access with Microsoft accounts or with Azure AD, and how to switch when you're ready](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface for managing organizations. On the left, under 'My organizations', the 'FabrikamFiber' organization is selected, indicated by a blue border around its card. Other organizations listed include 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this is a section for 'All projects', showing cards for 'Fabrikam' (blue F icon) and 'FabrikamFiber4.0' (purple F icon). At the bottom of the left sidebar, there are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' being the one highlighted with a red box.

2. Find the current owner.



Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.



Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Understand Azure AD groups

Q: Why can't I assign Azure DevOps permissions directly to an Azure AD group?

A: Because these groups are created and managed in Azure, you can't assign Azure DevOps permissions directly or secure version control paths to these groups. You'll get an error if you try to assign permissions directly.

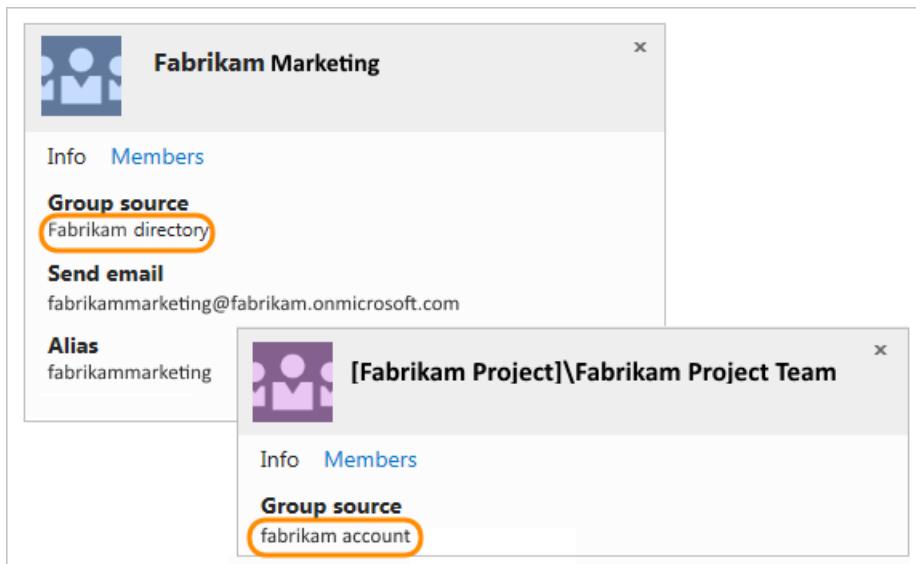
You can add an Azure AD group to the Azure DevOps group that has the permissions you want. Or, you can assign these permissions to the group instead. Azure AD group members inherit permissions from the group where you add them.

Q: Can I manage Azure AD groups in Azure DevOps?

A: No, because these groups are created and managed in Azure. Azure DevOps doesn't store or sync member status for Azure AD groups. To manage Azure AD groups, use the [Azure portal](#), Microsoft Identity Manager (MIM), or the group management tools that your organization supports.

Q: How do I tell the difference between an Azure DevOps group and an Azure AD group?

A: On the group's identity card, check the group's source.



Q: Why doesn't Users show all Azure AD group members?

A: These users have to sign in to your organization before they appear in Users.

Q: How do I assign organization access to Azure AD group members?

A: When these group members sign in to your organization for the first time, Azure DevOps assigns an access level to them automatically. If they have [Visual Studio subscriptions](#), Azure DevOps assigns the respective access level to them. Otherwise, Azure DevOps assigns them the next "best available" [access level](#), in this order: Basic, Stakeholder.

If you don't have enough access levels for all Azure AD group members, those members who sign in get a Stakeholder access.

Q: Why doesn't the Security tab show all members when I select an Azure AD group?

A: The Security tab shows Azure AD group members only after they sign in to your organization, and have an access level assigned to them.

To see all Azure AD group members, use the [Azure portal](#), MIM, or the group management tools that your organization supports.

Q: Why doesn't the team members widget show all Azure AD group members?

A: The team members widget shows only users who previously signed in to your organization.

Q: Why doesn't the team capacity pane show all Azure AD group members?

A: The team capacity pane shows only users who previously signed in to your organization. To set capacity, manually add users to your team.

Q: Why doesn't the team room show offline users?

A: The team room shows Azure AD group members, but only when they're online.

Q: Why doesn't Azure DevOps reclaim access levels from users who aren't Azure AD group members anymore?

Azure DevOps doesn't automatically reclaim access levels from these users. To manually remove their access, go to [Users](#).

Q: Can I assign work items to Azure AD group members who haven't signed in?

A: You can assign work items to any Azure AD member who has permissions for your organization. This also adds that member to your organization. When you add users this way, they'll automatically appear in Users, with the best available access level. They'll also appear in the security settings.

Q: Can I use Azure AD groups to query work items by using the "In Group" clause?

A: No, querying on Azure AD groups is unsupported.

Q: Can I use Azure AD groups to set up field rules in my work item templates?

A: No, but you might be interested in our [process customization plans](#).

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Add users to directory

[Add organization users to your Azure Active Directory](#).

Q: Can I switch current users from Microsoft accounts to work accounts in Azure DevOps?

A: No. Although you can add new work accounts to your organization, they're treated as new users. If you want to access all your work, including its history, you must use the same sign-in addresses that you used before your organization was connected to your Azure AD. You can do this by adding your Microsoft account as a member to your Azure AD.

Q: Why can't I add users from other directories to my Azure AD?

A: You must be a member or have read access in those directories. Otherwise, you can add them [using B2B collaboration through your Azure AD administrator](#). You can also add them by using their Microsoft accounts, or by creating new work accounts for them in your directory.

Q: How do I use my work or school account with my Visual Studio with MSDN subscription?

A: If you used a Microsoft account to activate a [Visual Studio with MSDN subscription](#) that includes Azure DevOps as a benefit, you can add a work or school account. The account must be managed by Azure AD. Learn [how to link work or school accounts to Visual Studio with MSDN subscriptions](#).

Q: Can I control access to my organization for external users in the connected directory?

A: Yes, but only for external users who are [added as guests through Office 365](#) or [added using B2B collaboration by your Azure AD administrator](#). These external users are managed outside the connected directory. To learn more, contact your Azure AD administrator. The following setting doesn't affect [users who are added directly to your organization's directory](#).

Before you start, make sure you have at least Basic access, not Stakeholder.

Complete the following steps to control organization access for external users added through Office 365 or Azure AD B2B collaboration.

1. Go to **Organization settings**.

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and shows 'Projects' (selected), 'My work items', and 'My pull requests'. It displays a card for 'Fabrikam Fiber' and lists other projects: 'All projects', 'Fabrikam', and 'FabrikamFiber4.0'.

2. Select **Policy** and choose to allow or deny organization access for external users added as guests.

The screenshot shows the 'Organization Settings > Policy' page. The left sidebar has sections like General (Overview, Projects, Policy selected), Users, Security, Notifications, Extensions, and Usage. The right panel is titled 'Policy' and contains two main sections: 'Application connection policies' and 'Security policies'. Under 'Application connection policies', 'Alternate authentication credentials' and 'Third-party application access via OAuth' are set to 'On'. Under 'Security policies', 'External guest access' is set to 'On' (highlighted by a red box) and 'Anonymous access to projects' is set to 'Off'.

Remove users or groups

Q: How do I remove an Azure AD group from Azure DevOps?

A: Go to your project collection or project. In the bar at the top, select the gear icon, and then select **Security**.

Find the Azure AD group, and delete it from your organization.

The screenshot shows the Azure DevOps Security interface. On the left, there's a sidebar with options like 'Create group' and 'Filter users and groups'. Below that is a list of 'Azure DevOps Services Groups' with items like 'Contributors', 'Project Administrators', and 'Project Collection Admi...'. The main area shows a group named 'Fabrikam > Project Administrators'. The 'Members' tab is selected. It lists two users: 'Project Collection Build Se... [Fabrikam Project]' and 'Christie Church'. The 'Remove' button next to the first user is highlighted with a red box.

Q: Why am I asked to remove a user from an Azure AD group when I delete that user from my organization?

A: Users can belong to your organization, both as individuals and as members of Azure AD groups that were added to Azure DevOps groups. These users can still access your organization while they're members of these Azure AD groups.

To block all access for these users, remove them from Azure AD groups in your organization, or remove these groups from your organization. Although we'd like to make it possible to block access completely or make exceptions for such users, Azure DevOps doesn't currently have this capability.

Q: If an Azure AD user is removed, will all their related PATs be revoked as well?

A: When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials.

Connect, disconnect, or change Azure AD

- [Connect your organization to Azure AD](#)
- [Disconnect your organization from your directory](#)
- [Change the directory that's connected to Azure DevOps](#)

Q: Can I connect my organization to an Azure AD created from Office 365?

A: Yes. If you can't find your Azure AD created from Office 365, see [Why don't I see the directory that I want to connect?](#).

Q: Why don't I see the directory that I want to connect to? What should I do?

A: This might happen due to any of the following circumstances:

- You don't have [organization Owner permissions](#) to manage directory connections.
- Talk to your Azure AD organization administrator and ask them to make you a member of the organization. It's possible that you're not part of the organization.

Q: Why is my organization already connected to a directory? Can I change that directory?

A: Your organization was connected to a directory when the organization owner created the organization, or sometime after that. When you create an organization with a work or school account, your organization is automatically connected to the directory that manages that work or school account. You can [disconnect your organization](#) if you need to change the directory connection.

organization from this directory, and [reconnect to another directory](#). You might have to migrate some users.

Q: My alternate credentials don't work anymore. What do I do?

A: This happens after you connect your organization to a directory. [Set up your credentials](#) again for the organization that you connected.

Q: Some users are disconnected, but they have matching identities in Azure AD. What should I do?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

The screenshot shows the 'Organization Settings' page in the Azure DevOps portal. The left sidebar lists various settings categories: General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' item is highlighted with a red box. The main content area is titled 'Azure Active Directory'. It displays a message: '10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory.' Below this message is a 'Resolve' button, which is also highlighted with a red box. Further down, it states 'Your organization is connected to the Commerce Test Directory' and provides details: 'Commerce Test Directory', 'mstestvscommerceoutlook.onmicrosoft.com', and 'Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5'. A 'Disconnect directory' button is located at the bottom of this section.

- Match the identities. Select **Next** when you're done.

Resolve disconnected users



Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

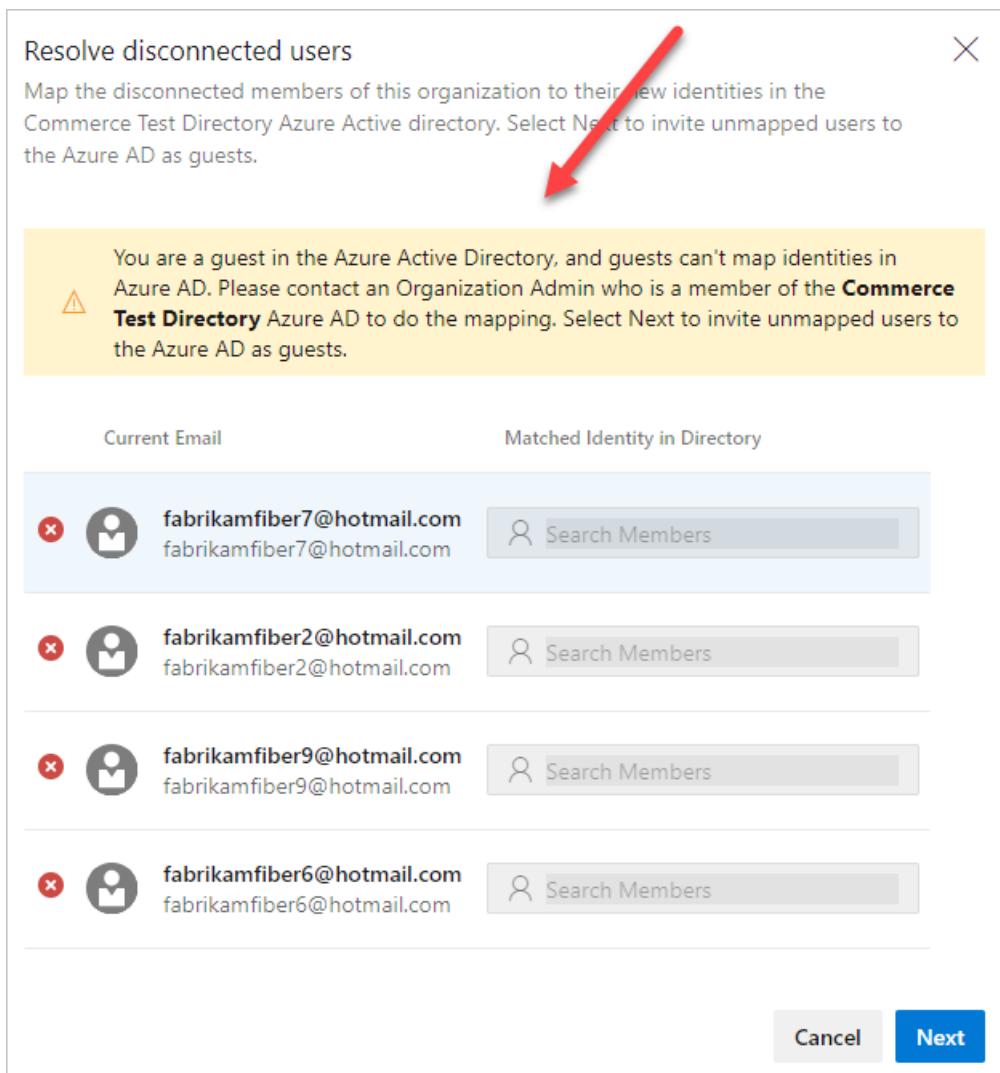
Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
CR fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: I got an error message when I was resolving disconnections. What should I do?

A:

- Try again.
- You might be a guest in Azure AD. Request that an organization administrator, who is a member of Azure AD, do the mapping. Or, request that an admin of the Azure AD convert you to a member.



- If the error message includes a user in your domain, but you don't see them active in your directory, the user likely left your company. Go to the organization user settings to remove the user from your organization.

Q: When I was trying to invite a new user to my Azure AD, I got a 403 forbidden exception. What do I do?

A: You may be a guest in Azure AD and don't have the right permission to invite users. Go to **External collaboration settings** in Azure AD and move the "Guests can invite" toggle to **Yes**. Refresh Azure AD and try again.

Q: Will my users keep their existing Visual Studio subscriptions?

A: Visual Studio subscription administrators ordinarily assign subscriptions to users' corporate email addresses, so that users can receive welcome email and notifications. If the identity and subscription email addresses match, users can access the benefits of the subscription. As you transition from Microsoft to Azure AD identities, users' benefits still work with their new Azure AD identity. But, the email addresses must match. If the email addresses don't match, your subscription administrator must [reassign the subscription](#). Otherwise, users must [add an alternate identity to their Visual Studio subscription](#).

Q: What if I'm required to sign in when I use the people picker?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: What if my email account isn't found in Azure AD?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

Organization Settings

Azure Active Directory

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory**

Your organization is connected to the **Commerce Test Directory** directory.

Commerce Test Directory
mstestvscommerceoutlook.onmicrosoft.com
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Disconnect directory

- Match the identities. Select **Next** when you're done.

Resolve disconnected users

Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: What if my work items are indicating that the users aren't valid?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: Once my organization is connected to Azure AD, will it update Azure Boards work items, pull requests, and other pieces where I'm referenced in the system with my new ID?

A: Yes, all pieces in the system are updated with the new ID when a user's ID is mapped from their personal email to their work email.

Q: What if I get a warning about members who will lose access to the organization?

A: You can still connect to Azure AD, but try to resolve the mapping issue after you've connected. If you still need help, [contact support](#).

Azure Active Directory Connection

Connect your organization to a directory.

You are signed in as



Jamal Hartnett
fabrikamfiber4@hotmail.com

Azure Active Directory

Commerce Test Directory

 Commerce Test Directory
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Warning: Some members will lose access to the FabrikamFiber organization

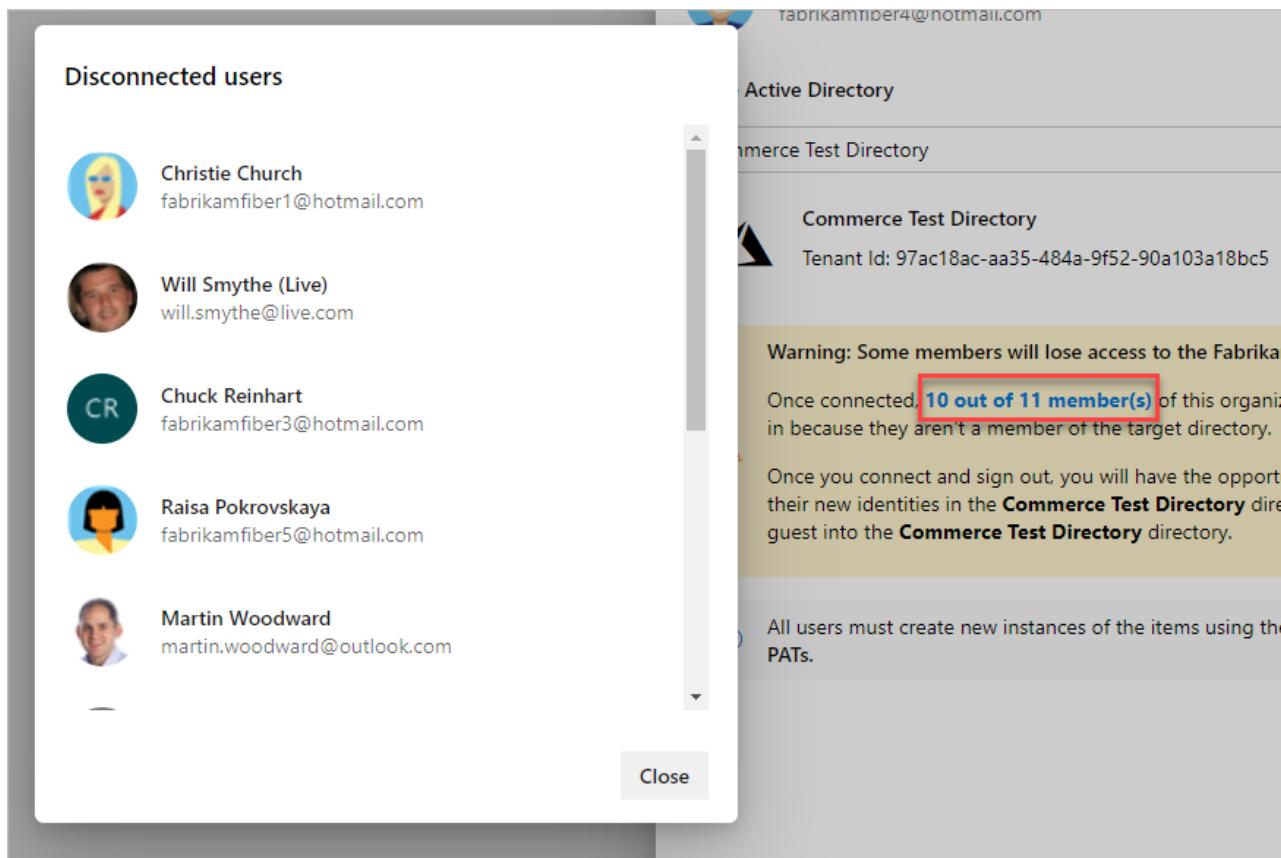
Once connected, **10 out of 11 member(s)** of this organization won't be able to sign in because they aren't a member of the target directory.

 Once you connect and sign out, you will have the opportunity to map these users to their new identities in the **Commerce Test Directory** directory, or to invite them as a guest into the **Commerce Test Directory** directory.

 All users must create new instances of the items using their work account: SSH Keys, PATs.

Cancel **Connect**

Select the bolded text to see which users are affected.



Q: What if I have over 100 users and want to connect to Azure AD?

A: If you have more than 100 users, [contact support](#).

Q: I have more than 100 members in my Azure DevOps organization, how can I connect to an Azure AD?

A: Currently, the in-app feature doesn't support connections for organizations with over 100 members. Please [contact support](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot changing app access policies for your organization

1/31/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: How do personal access tokens differ from alternate authentication credentials?

A: Personal access tokens are a more convenient and secure replacement for alternate authentication credentials. You can limit a token's use to a specific lifetime, to an organization, and to [scopes](#) of activities that the token authorizes. Learn more about [personal access tokens](#).

Q: If I deny access to one authentication method in one organization, does that affect all the organizations that I own?

A: No, you can still use that method in all the other organizations that you own. [Personal access tokens](#) apply to specific organizations or to all organizations, based on your selection when you created the token.

Q: If I deny access to an authentication method, then allow access again, will the apps that need access continue to work?

A: Yes, those apps continue to work.

Q: What apps integrate with Azure DevOps?

A: Find the [apps that integrate with Azure DevOps](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface for managing organizations. On the left, under 'My organizations', the 'FabrikamFiber' organization is selected, indicated by a blue border around its card. Other organizations listed include 'P' (grayed out), 'fabrikamfib', and 'fabrikamfiber4'. Below this is a section for 'All projects' which lists 'Fabrikam' and 'FabrikamFiber4.0'. At the bottom of the left sidebar, there are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' being the one highlighted with a red box.

2. Find the current owner.



Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.



Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot adding administrators to projects and project collections

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: When do I need to add someone to the project collection administrator role in Azure DevOps?

A: It varies. For most organizations that use Azure DevOps, project collection administrators manage the collections that members of the **Team Foundation Administrators** group create. Members of the **Project Collection Administrators** group don't create the collections themselves. Project collection administrators also perform many operations that are required to maintain the collection. Operations include creating team projects, adding users to groups, modifying the settings for the collection, and so on.

Q: What are the optimal permissions to administer a project collection across all of its components and dependencies?

A: Project collection administrators must be members of the following groups or have the following permissions:

- Team Foundation Server: A member of the **Project Collection Administrators** group, or have the appropriate **collection-level permissions** set to **Allow**.
- SharePoint Products: If the collection is configured with a site collection resource, then a member of the **Site Collection Administrators** group.
- Reporting Services: If the collection is configured with reporting resources, then a member of the **Team Foundation Content Manager** group.

Q: I'm an admin, but I don't have permission to add a project collection administrator. What do I need?

A: The following permissions are required:

- You must belong to the **Project Collection Administrators** group, or your **View Server-Level Information** and **Edit Server-Level Information** permissions must be set to **Allow**.
- To add permissions for SharePoint Products, you must be a member of the **Site Collection Administrators** or **Farm Administrators** groups for SharePoint Products.
- To add permissions for Reporting Services, you must be a member of the **Content Managers** or **Team Foundation Content Managers** groups for Reporting Services.

IMPORTANT

To perform administrative tasks like creating project collections, your user requires administrative permissions. The service account that the Team Foundation Background Job Agent uses must have certain permissions granted to it. For more information, see [Service accounts and dependencies in Team Foundation Server](#) and [Team Foundation Background Job Agent](#).

Q: Where can I find information about each individual permission?

A: You can find detailed information about individual permissions and their relationship to default security groups in the [Permission and groups reference](#). To give a user project administration permissions, complete the following steps:

1. From the team page, select the settings icon  to go to the team administration page.
2. Add the user to the **Project Administrators** group.

Troubleshoot changing the organization owner

7/3/2019 • 5 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Q: How do I find a Project Collection Administrator?

A: If you have at least Basic access, you can find your [Project Collection Administrator](#) in your organization's security settings.

1. See [Show members of the Project Collection Administrators group](#).
1. See [Show members of the Project Administrators group](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area shows the 'FabrikamFiber' organization with its projects: 'Fabrikam Fiber' (selected), 'Fabrikam', and 'FabrikamFiber4.0'. At the bottom, there's a large empty box with a placeholder text 'Find the current owner'.

2. Find the current owner.

Q: Why can't I find the user who I want to make the new owner?

A: This might happen for one of the following reasons:

- The user isn't in your organization, or the user doesn't have organization access. Learn how to [add a user to your organization](#).
- The user hasn't created a Visual Studio profile and agreed to the Terms of Service.
- If you recently added this person to your organization, you might experience a delay before the user appears in the possible organization owners list.
- If your organization uses Azure Active Directory to control access, directory members don't appear in the possible organization owners list until they meet the requirements described in this article.

Q: What happens if I forget my password?

A: You can [recover your Microsoft account password](#) or [recover your work or school account password](#) if your organization turned on this feature. Otherwise, contact your Azure Active Directory administrator to recover your work or school account.

Q: Can I reverse an organization owner change?

A: Yes, if you're a Project Collection Administrator.

Q: Can I change the organization name (URL), too?

A: Only the organization owner can change the URL. If you're the organization owner, learn how to [change the organization URL](#).

Q: How many organization owners can I have?

A: Your organization can have only one owner. Only organization owners can [perform certain actions](#), so make sure you keep your organization owner updated.

Q: Why did you ask for extra information when I signed in?

A: If our Terms of Service have changed since you last signed in, you might be asked to agree and confirm that your information is up to date.

Q: When I change ownership from myself (as PCA) to a different user, my own account is removed from the PCA group. Is this a bug?

A: This is not a bug and is how it has been implemented. We hope to address this soon.

Q: What makes the organization owner different from other organization users?

A: The organization owner manages payments and access for organization users. The organization owner also manages billing for the organization through the [Azure classic portal](#) or the [Azure portal](#).

Organization owners also have permissions to perform the following tasks:

- Pay for users to access the organization
- Pay for additional organization services
- Rename the organization URL
- Change the organization owner

Project collection administrators can manage user access and change the organization owner, but they can't rename the organization URL.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.



Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot deleting or restoring your organization

1/31/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your **Organization settings**.

The screenshot shows the Azure DevOps organization settings page for 'FabrikamFiber'. The left sidebar lists organizations: 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. A red box highlights the 'Organization settings' button at the bottom of the sidebar. The main content area shows the 'FabrikamFiber' organization with its projects: 'Fabrikam Fiber' (selected), 'Fabrikam', and 'FabrikamFiber4.0'. The 'Projects' tab is active.

2. Find the current owner.

Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.

Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I delete my organization?

A: See [Delete your organization](#), which includes prerequisites and helpful tips.

Q: How do I restore my organization?

A: See [Recover your organization](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.

3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot setting up Visual Studio with Azure DevOps

1/31/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Visual Studio

Q: Why sign in?

A: Your Visual Studio settings, like automatic brace completion, are saved with your profile. These settings roam with your [personal Microsoft account](#), or your [work or school account](#), when you sign in to Visual Studio on any computer.

Sign in to Visual Studio during the 30-day trial period for these benefits:

- Visual Studio Enterprise: Extend your trial for 90 days. When your trial expires, learn [how to unlock Visual Studio](#).
- Visual Studio Express or Community: Continue to use this edition for free.

When you create your profile, you can also create an organization.

Learn more about [the benefits of signing in and creating a profile](#).

Q: Why can't I sign in?

A: To create a profile and save your settings, you'll need to sign in with a [personal Microsoft account](#) or a [work or school account](#) that's managed by Azure Active Directory.

Q: Which versions of Visual Studio can I use with Azure DevOps?

A: You can use:

- Visual Studio 2017
- Visual Studio 2015
- Visual Studio 2013
- Visual Studio 2012
- Visual Studio 2010, which requires [Service Pack 1](#) and [KB2662296](#)
- Visual Studio 2008 SP1, which requires a [GDR update](#)

To connect to Azure DevOps with Visual Studio 2008 through Visual Studio 2012:

1. Start Visual Studio.
2. From the **Team** menu or Team Explorer, go to **Connect to Team Foundation Server > Select Team Projects > Servers**.
3. Add your organization ({yourorganization}.visualstudio.com).
4. Select your project and finish connecting.

If you get connection errors, try choosing HTTPS as your protocol.

To connect to Azure DevOps with Visual Studio 2015 and later, learn [how to connect to team projects](#).

Q: Can I use Visual Studio 2015 with Visual Studio 2013 and 2012 on the same computer?

A: Yes, you can run all these versions on the same computer.

Q: My subscription expired. What do I do?

A: Here's [how to unlock Visual Studio](#). If you're having subscription problems, try [Subscription Support](#).

Q: I'm having problems installing or signing in to Visual Studio. How do I get help?

A: Learn more about:

- [Installing Visual Studio](#).
- [Signing in to Visual Studio](#).
- [Managing multiple user organizations](#).

Or contact [Visual Studio Support](#).

Azure DevOps Services

Q: How can I create an organization later?

A: Learn how to [sign up for Azure DevOps](#).

Q: Why won't my browser work with Azure DevOps?

A: This might happen if you're using an unsupported browser. For the best experience, make sure that you're using a [supported browser](#).

Q: Where can I find my organization name (URL)?

A: [Sign in to your Visual Studio profile](#) to find your organization list.

Q: What happens if I forget my password?

A: You can [recover your Microsoft account password](#) or [recover your work or school account password](#) if your organization turned on this feature. Otherwise, contact your Azure Active Directory administrator to recover your work or school account.

Q: Can I change my organization location?

A: Yes. For a better experience, you can change your organization's location during sign-up so that your organization is closest to most users.



Your organization's default location is selected based on the closest [Microsoft Azure region](#) where Azure DevOps is available.

Q: How do you store, secure, and protect my data?

A: Azure DevOps storage features help make sure that your data is available in case of hardware failure, service disruption, or datacenter disasters. Azure DevOps helps protect data from accidental or malicious deletion.

We follow industry best practices and have enterprise-grade security measures to help protect your code and project data. Also, all communication between your computer and the service takes place over an encrypted HTTPS connection. Learn [how your data is secured and protected](#).

Q: Do I still own my code and intellectual property? What do you do with my personal information?

A: Yes, your code and your intellectual property are yours. Please review our [terms of service](#) and [privacy policy](#).

Q: Where can I find the Azure DevOps SLA?

A: You can find it here: [Azure DevOps SLA](#).

Q: Can I change my organization name (URL) or owner?

A: Yes. If you have at least Basic access, you can do this in your organization settings. Learn how to:

- [Rename your organization](#).
- [Change the organization owner](#).

Q: Can I delete an organization that I don't need anymore?

A: Yes. See [Delete or recover your organization](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

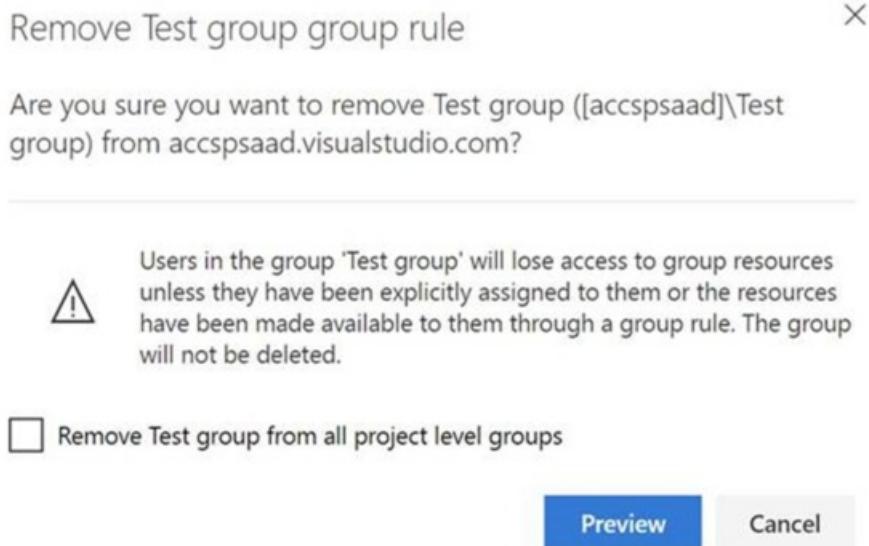
Troubleshoot managing group-based licensing

5/31/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: Will my users lose their access level and project membership if I remove a group rule?

A: Users in the group **TestGroup** lose access to group resources if the users haven't been explicitly assigned to the resources or assigned via a different group rule.



Q: Will my Azure DevOps or Azure AD group be deleted if I remove its group rule?

A: No. Your groups won't be deleted.

Q: What does the option "Remove from all project level groups" do?

A: This option removes the Azure DevOps or Azure AD group from any project-level default groups, such as **Project Readers** or **Project Contributors**.

Related articles

- [Migrate to group-based resource management](#)
- [Assign access levels and extensions to users by group membership](#)

Troubleshoot permissions and access with Azure Active Directory

6/12/2019 • 14 minutes to read • [Edit Online](#)

Azure DevOps Services

General

Q: I made changes to Azure Active Directory (Azure AD), but they didn't seem to take effect

A: Changes made in Azure AD can take up to 24 hours to be visible in Azure DevOps.

Q: Can I use Office 365 and Azure AD with Azure DevOps?

A: Yes.

- Don't have an organization yet? [Create an organization in Azure DevOps](#).
- Already have an organization? [Connect your organization to Azure AD](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: My organization uses Microsoft accounts only. Can I switch to Azure AD?

A: Yes, but before you switch, make sure that Azure AD meets your needs for sharing work items, code, resources, and other assets with your team and partners.

Learn more about the differences in how you [control access with Microsoft accounts or with Azure AD, and how to switch when you're ready](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface for managing organizations. On the left, under 'My organizations', the 'FabrikamFiber' organization is selected, indicated by a blue border around its card. Other organizations listed include 'P' (grayed out), 'fabrikamfib', and 'fabrikamfiber4'. Below this is a section for 'All projects' showing cards for 'Fabrikam' (dark green) and 'FabrikamFiber4.0' (purple). At the bottom of the left sidebar, there are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' being the one highlighted with a red box.

2. Find the current owner.



Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.



Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Understand Azure AD groups

Q: Why can't I assign Azure DevOps permissions directly to an Azure AD group?

A: Because these groups are created and managed in Azure, you can't assign Azure DevOps permissions directly or secure version control paths to these groups. You'll get an error if you try to assign permissions directly.

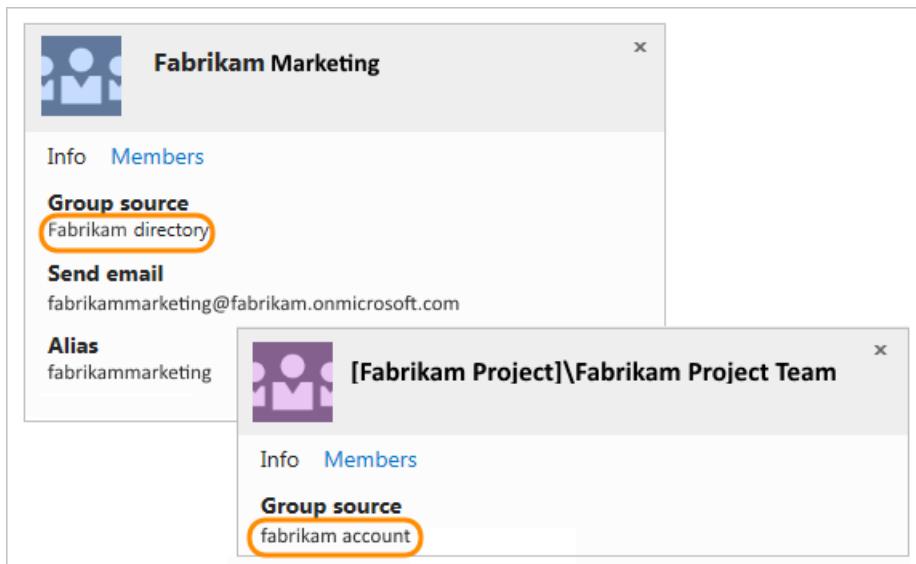
You can add an Azure AD group to the Azure DevOps group that has the permissions you want. Or, you can assign these permissions to the group instead. Azure AD group members inherit permissions from the group where you add them.

Q: Can I manage Azure AD groups in Azure DevOps?

A: No, because these groups are created and managed in Azure. Azure DevOps doesn't store or sync member status for Azure AD groups. To manage Azure AD groups, use the [Azure portal](#), Microsoft Identity Manager (MIM), or the group management tools that your organization supports.

Q: How do I tell the difference between an Azure DevOps group and an Azure AD group?

A: On the group's identity card, check the group's source.



Q: Why doesn't Users show all Azure AD group members?

A: These users have to sign in to your organization before they appear in Users.

Q: How do I assign organization access to Azure AD group members?

A: When these group members sign in to your organization for the first time, Azure DevOps assigns an access level to them automatically. If they have [Visual Studio subscriptions](#), Azure DevOps assigns the respective access level to them. Otherwise, Azure DevOps assigns them the next "best available" [access level](#), in this order: Basic, Stakeholder.

If you don't have enough access levels for all Azure AD group members, those members who sign in get a Stakeholder access.

Q: Why doesn't the Security tab show all members when I select an Azure AD group?

A: The Security tab shows Azure AD group members only after they sign in to your organization, and have an access level assigned to them.

To see all Azure AD group members, use the [Azure portal](#), MIM, or the group management tools that your organization supports.

Q: Why doesn't the team members widget show all Azure AD group members?

A: The team members widget shows only users who previously signed in to your organization.

Q: Why doesn't the team capacity pane show all Azure AD group members?

A: The team capacity pane shows only users who previously signed in to your organization. To set capacity, manually add users to your team.

Q: Why doesn't the team room show offline users?

A: The team room shows Azure AD group members, but only when they're online.

Q: Why doesn't Azure DevOps reclaim access levels from users who aren't Azure AD group members anymore?

Azure DevOps doesn't automatically reclaim access levels from these users. To manually remove their access, go to [Users](#).

Q: Can I assign work items to Azure AD group members who haven't signed in?

A: You can assign work items to any Azure AD member who has permissions for your organization. This also adds that member to your organization. When you add users this way, they'll automatically appear in Users, with the best available access level. They'll also appear in the security settings.

Q: Can I use Azure AD groups to query work items by using the "In Group" clause?

A: No, querying on Azure AD groups is unsupported.

Q: Can I use Azure AD groups to set up field rules in my work item templates?

A: No, but you might be interested in our [process customization plans](#).

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Add users to directory

[Add organization users to your Azure Active Directory](#).

Q: Can I switch current users from Microsoft accounts to work accounts in Azure DevOps?

A: No. Although you can add new work accounts to your organization, they're treated as new users. If you want to access all your work, including its history, you must use the same sign-in addresses that you used before your organization was connected to your Azure AD. You can do this by adding your Microsoft account as a member to your Azure AD.

Q: Why can't I add users from other directories to my Azure AD?

A: You must be a member or have read access in those directories. Otherwise, you can add them [using B2B collaboration through your Azure AD administrator](#). You can also add them by using their Microsoft accounts, or by creating new work accounts for them in your directory.

Q: How do I use my work or school account with my Visual Studio with MSDN subscription?

A: If you used a Microsoft account to activate a [Visual Studio with MSDN subscription](#) that includes Azure DevOps as a benefit, you can add a work or school account. The account must be managed by Azure AD. Learn [how to link work or school accounts to Visual Studio with MSDN subscriptions](#).

Q: Can I control access to my organization for external users in the connected directory?

A: Yes, but only for external users who are [added as guests through Office 365](#) or [added using B2B collaboration by your Azure AD administrator](#). These external users are managed outside the connected directory. To learn more, contact your Azure AD administrator. The following setting doesn't affect [users who are added directly to your organization's directory](#).

Before you start, make sure you have at least Basic access, not Stakeholder.

Complete the following steps to control organization access for external users added through Office 365 or Azure AD B2B collaboration.

1. Go to **Organization settings**.

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and shows 'Projects' (selected), 'My work items', and 'My pull requests'. It displays a card for 'Fabrikam Fiber' and lists other projects: 'All projects', 'Fabrikam', and 'FabrikamFiber4.0'.

2. Select **Policy** and choose to allow or deny organization access for external users added as guests.

The screenshot shows the 'Organization Settings > Policy' page. The left sidebar has sections like General (Overview, Projects, Policy selected), Users, Security, Notifications, Extensions, and Usage. The right panel is titled 'Policy' and contains two main sections: 'Application connection policies' and 'Security policies'. Under 'Application connection policies', 'Alternate authentication credentials' and 'Third-party application access via OAuth' are set to 'On'. Under 'Security policies', 'External guest access' is set to 'On' (highlighted by a red box) and 'Anonymous access to projects' is set to 'Off'.

Remove users or groups

Q: How do I remove an Azure AD group from Azure DevOps?

A: Go to your project collection or project. In the bar at the top, select the gear icon, and then select **Security**.

Find the Azure AD group, and delete it from your organization.

The screenshot shows the Azure DevOps Security interface. On the left, there's a sidebar with options like 'Create group' and 'Filter users and groups'. Below that is a list of 'Azure DevOps Services Groups' with items like 'Contributors', 'Project Administrators', and 'Project Collection Admi...'. The main area shows a group named 'Fabrikam > Project Administrators'. The 'Members' tab is selected. It lists two users: 'Project Collection Build Se... [Fabrikam Project]' and 'Christie Church'. The 'Remove' button next to the first user is highlighted with a red box.

Q: Why am I asked to remove a user from an Azure AD group when I delete that user from my organization?

A: Users can belong to your organization, both as individuals and as members of Azure AD groups that were added to Azure DevOps groups. These users can still access your organization while they're members of these Azure AD groups.

To block all access for these users, remove them from Azure AD groups in your organization, or remove these groups from your organization. Although we'd like to make it possible to block access completely or make exceptions for such users, Azure DevOps doesn't currently have this capability.

Q: If an Azure AD user is removed, will all their related PATs be revoked as well?

A: When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials.

Connect, disconnect, or change Azure AD

- [Connect your organization to Azure AD](#)
- [Disconnect your organization from your directory](#)
- [Change the directory that's connected to Azure DevOps](#)

Q: Can I connect my organization to an Azure AD created from Office 365?

A: Yes. If you can't find your Azure AD created from Office 365, see [Why don't I see the directory that I want to connect?](#).

Q: Why don't I see the directory that I want to connect to? What should I do?

A: This might happen due to any of the following circumstances:

- You don't have [organization Owner permissions](#) to manage directory connections.
- Talk to your Azure AD organization administrator and ask them to make you a member of the organization. It's possible that you're not part of the organization.

Q: Why is my organization already connected to a directory? Can I change that directory?

A: Your organization was connected to a directory when the organization owner created the organization, or sometime after that. When you create an organization with a work or school account, your organization is automatically connected to the directory that manages that work or school account. You can [disconnect your](#)

organization from this directory, and [reconnect to another directory](#). You might have to migrate some users.

Q: My alternate credentials don't work anymore. What do I do?

A: This happens after you connect your organization to a directory. [Set up your credentials](#) again for the organization that you connected.

Q: Some users are disconnected, but they have matching identities in Azure AD. What should I do?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

The screenshot shows the 'Organization Settings' page in the Azure DevOps portal. The left sidebar lists various settings categories: General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' item is highlighted with a red box. The main content area is titled 'Azure Active Directory'. It displays a message: '10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory.' Below this message is a 'Resolve' button, which is also highlighted with a red box. Further down, it states 'Your organization is connected to the Commerce Test Directory' and provides details: 'Commerce Test Directory', 'mstestvscommerceoutlook.onmicrosoft.com', and 'Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5'. A 'Disconnect directory' button is located at the bottom of this section.

- Match the identities. Select **Next** when you're done.

Resolve disconnected users



Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

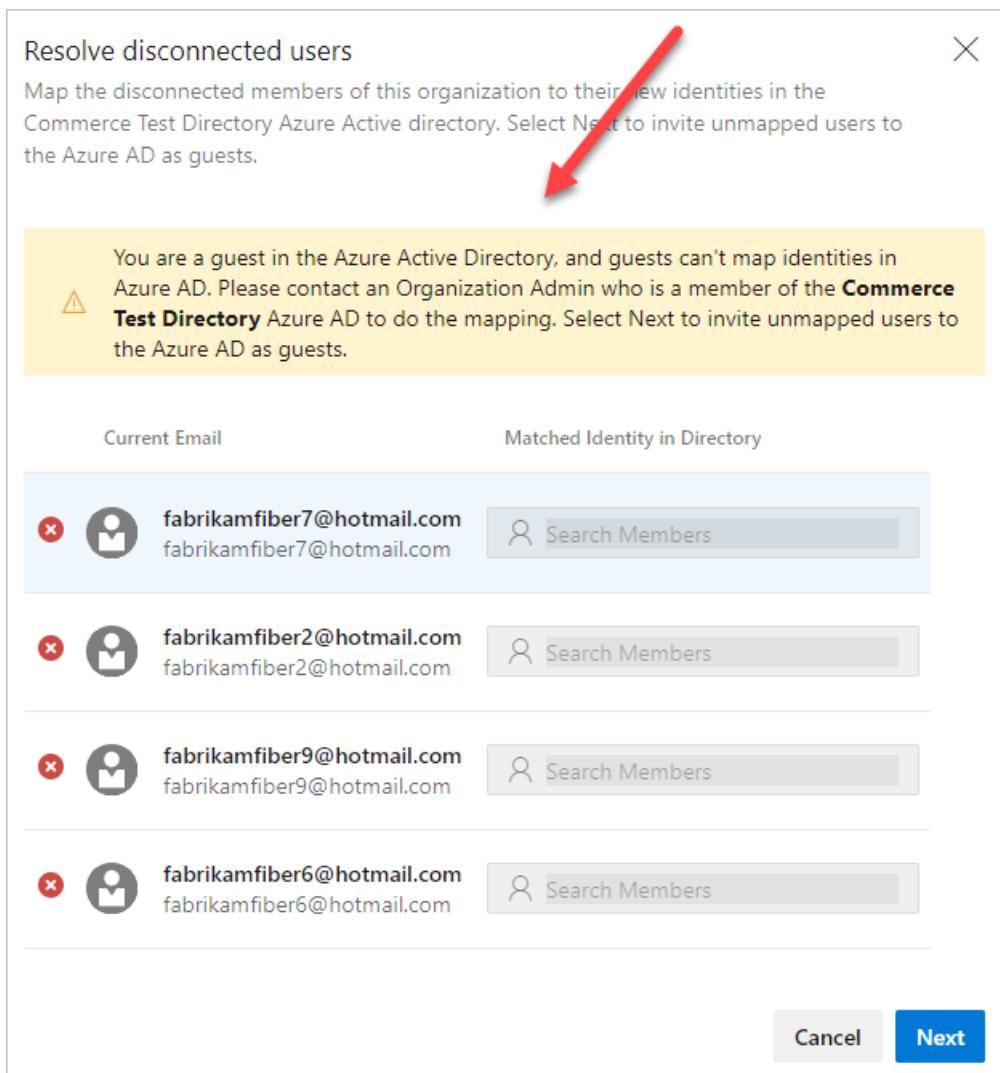
Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
CR fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: I got an error message when I was resolving disconnections. What should I do?

A:

- Try again.
- You might be a guest in Azure AD. Request that an organization administrator, who is a member of Azure AD, do the mapping. Or, request that an admin of the Azure AD convert you to a member.



- If the error message includes a user in your domain, but you don't see them active in your directory, the user likely left your company. Go to the organization user settings to remove the user from your organization.

Q: When I was trying to invite a new user to my Azure AD, I got a 403 forbidden exception. What do I do?

A: You may be a guest in Azure AD and don't have the right permission to invite users. Go to **External collaboration settings** in Azure AD and move the "Guests can invite" toggle to **Yes**. Refresh Azure AD and try again.

Q: Will my users keep their existing Visual Studio subscriptions?

A: Visual Studio subscription administrators ordinarily assign subscriptions to users' corporate email addresses, so that users can receive welcome email and notifications. If the identity and subscription email addresses match, users can access the benefits of the subscription. As you transition from Microsoft to Azure AD identities, users' benefits still work with their new Azure AD identity. But, the email addresses must match. If the email addresses don't match, your subscription administrator must [reassign the subscription](#). Otherwise, users must [add an alternate identity to their Visual Studio subscription](#).

Q: What if I'm required to sign in when I use the people picker?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: What if my email account isn't found in Azure AD?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

Organization Settings

Azure Active Directory

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory**

Your organization is connected to the **Commerce Test Directory** directory.

Commerce Test Directory
mstestvscommerceoutlook.onmicrosoft.com
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Disconnect directory

- Match the identities. Select **Next** when you're done.

Resolve disconnected users

Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	<input type="text"/> Search Members
fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	<input type="text"/> Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	<input type="text"/> Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	<input type="text"/> Search Members

Cancel **Next**

Q: What if my work items are indicating that the users aren't valid?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: Once my organization is connected to Azure AD, will it update Azure Boards work items, pull requests, and other pieces where I'm referenced in the system with my new ID?

A: Yes, all pieces in the system are updated with the new ID when a user's ID is mapped from their personal email to their work email.

Q: What if I get a warning about members who will lose access to the organization?

A: You can still connect to Azure AD, but try to resolve the mapping issue after you've connected. If you still need help, [contact support](#).

Azure Active Directory Connection

Connect your organization to a directory.

You are signed in as



Jamal Hartnett
fabrikamfiber4@hotmail.com

Azure Active Directory

Commerce Test Directory

 Commerce Test Directory
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Warning: Some members will lose access to the FabrikamFiber organization

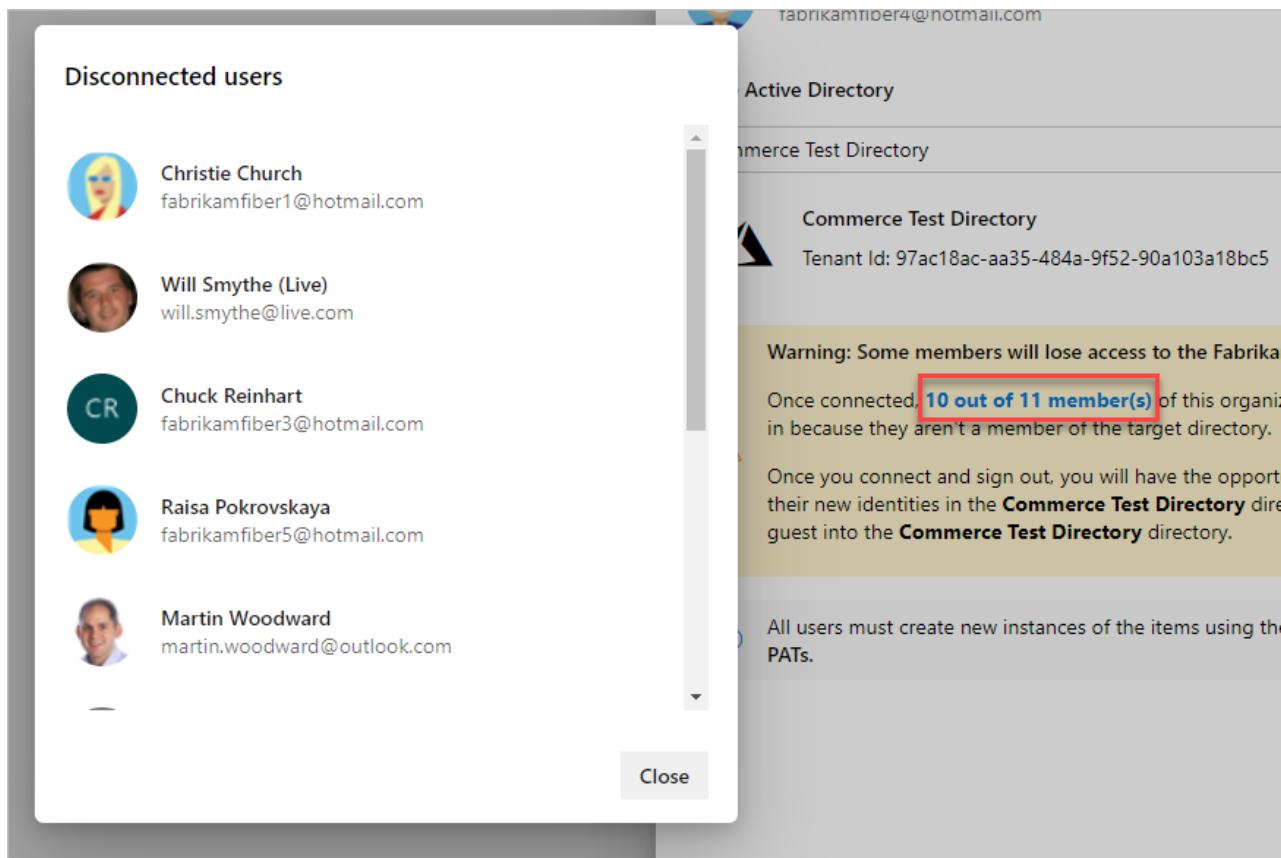
Once connected, **10 out of 11 member(s)** of this organization won't be able to sign in because they aren't a member of the target directory.

 Once you connect and sign out, you will have the opportunity to map these users to their new identities in the **Commerce Test Directory** directory, or to invite them as a guest into the **Commerce Test Directory** directory.

 All users must create new instances of the items using their work account: SSH Keys, PATs.

Cancel **Connect**

Select the bolded text to see which users are affected.



Q: What if I have over 100 users and want to connect to Azure AD?

A: If you have more than 100 users, [contact support](#).

Q: I have more than 100 members in my Azure DevOps organization, how can I connect to an Azure AD?

A: Currently, the in-app feature doesn't support connections for organizations with over 100 members. Please [contact support](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Billing

6/18/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Billing for Azure DevOps

All charges appear on your monthly Azure bill. Azure supports payment by credit card as well as invoiced billing through the Enterprise Agreement (EA), Cloud Solution Providers (CSP), and more.

- [Azure DevOps pricing](#)
- [Azure DevOps billing overview](#)

Billing for Azure DevOps Server

Make some purchases for Azure DevOps Server on your monthly Azure bill.

- [Azure DevOps Server pricing](#)
- [How to buy CALs or access to the Test Services page](#)

5-minute quickstarts

- [Set up billing](#)
- [Pay for users](#)
- [Buy Azure Pipelines](#)
- [Try Azure Test Plans for free](#)
- [Buy Basic + Test Plans access](#)

How-to guides

Billing management

- [Add user to make purchases or backup billing manager](#)
- [Change the Azure subscription your organization uses for billing](#)
- [Sign up for Azure Artifacts](#)
- [Billing FAQ](#)
- [Connect your organization to Azure Active Directory](#)

Marketplace extension management

- [Buy Basic access for users](#)
- [Approve requests for extensions](#)
- [Uninstall or disable extensions](#)

Guidance for Cloud Solution Providers

- [Buy Azure DevOps](#)
- [Buy and manage Visual Studio subscriptions](#)
- [Buy App Center resources](#)

Reference

- [Permissions](#)
- [About access levels](#)
- [Default permissions & access](#)
- [Azure DevOps data protection overview](#)

Other resources

- [Get Started using Azure DevOps](#)
- [Marketplace & Extensibility](#)
- [Azure DevOps Server Administration](#)
- [Buy Visual Studio cloud subscriptions](#)

Billing overview for Azure DevOps

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Set up [billing](#) when you need more than the *free tier* of resources in your organization, or to buy other features for your users that are offered by Microsoft or other companies.

The *free tier* includes:

- Five Azure DevOps users (Basic)
- Free tier of Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month)
- 2GB of Azure Artifacts storage
- One self-hosted CI/CD concurrent job
- 20,000 virtual user minutes of cloud-based load testing

During your first purchase for your organization, you're prompted to select the Azure subscription to use for billing. The subscription can be part of your Enterprise Agreement, Pay-As-You-Go, Cloud Solution Provider (CSP), or other types of Azure subscriptions. All services are billed via Azure. You aren't required to pay for or use any other Azure services.

The following links take you to the paid services that are offered by Microsoft:

- [Buy Basic access for users](#)
- [Buy Azure Test Plans](#)
- [Buy CI/CD](#)
- [Sign up for Azure Artifacts](#)
- [Buy cloud-based load testing](#). You're charged based on the load tests that you run. By default, paid usage is turned off for your organization.

Enable paid usage via the **Billing** tab within **Organization settings** in Azure DevOps.

NOTE

The cloud-based load testing service is deprecated. More information about the deprecation, the service availability, and alternative services can be found [here](#).

To configure costs for Azure DevOps, see the [pricing calculator](#).

Prerequisites

Ensure the following is true for the user who's [setting up billing](#) for the first time:

- User has [project collection administrator or organization owner permissions](#)
- User has [an Azure subscription that you can use to purchase](#)

To make subsequent changes to the amount of paid resources, you only need to have [access to the Azure subscription](#).

Next steps

- [Set up billing](#)
- [Add user who can make purchases or backup billing manager](#)
- [Change the Azure subscription for billing](#)

Related articles

- [Azure DevOps pricing](#)
- [Azure DevOps billing support](#)

Quickstart: Set up billing for your organization

6/27/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

In this quickstart, learn to set up billing for your organization in advance of making purchases, so that you have this in place once you're ready to buy. During that process we prompt you for an Azure subscription where charges should apply and allow you to create a new Azure subscription if you don't have one already.

All services are billed via Azure, and you're not required to use any other Azure services.

If you don't have an Azure subscription, [create one](#) before you begin. Please note that the Azure Free Trial is not supported.

To configure costs for Azure DevOps, see the [pricing calculator](#).

Prerequisites

Ensure the following is true for the user who's setting up billing for the first time:

- User has [Project Collection Administrator or organization Owner permissions](#)
- User has [an Azure subscription that you can use to set up billing](#)

Set up billing

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are links for "New organization" and "Organization settings". The "Organization settings" link is highlighted with a red box. The main content area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber", "Fabrikam", and "FabrikamFiber4.0".

3. Select **Billing**.

The screenshot shows the "Organization Settings" page. The left sidebar lists several sections: General, Overview, Projects, Users, **Billing** (which is highlighted with a red box), Global notifications, Usage, Extensions, and Azure Active Directory.

4. Select **Set up billing**.

Billing

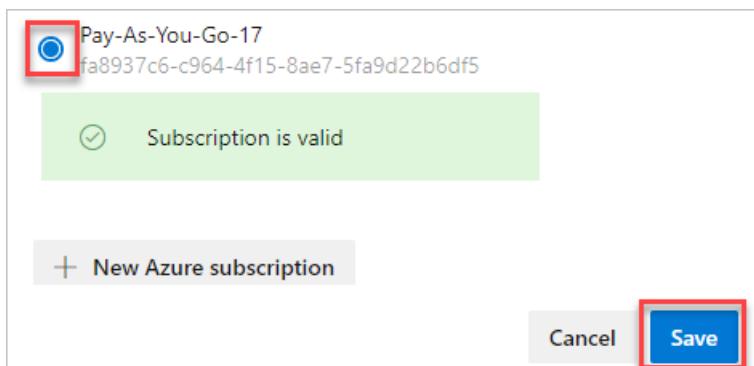
Billing has not been set up for this organization. Access will be available up to [free tier limits](#).

[Set up billing](#)

Users	Free	Paid
Repos and Boards (Basic)	5	0
Test Manager		0
Package Manager	5	0
Visual Studio Subscribers	Unlimited	
Stakeholders	Unlimited	

Resources	Free	Paid
Azure Pipelines	1800 minutes	Manage parallel jobs
Cloud-based load testing	20000 VUMs	Off Paid load testing limit

5. Select your Azure subscription, and then select **Save**.



Billing is set up.

Next steps

[Pay for users](#)

Quickstart: Buy Basic access for users

6/21/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In this quickstart, you learn how to pay for more users who need access to [Boards](#) and [Repos](#).

Visual Studio subscribers get Basic access included with their subscription, and their subscription is detected when they sign in to Azure DevOps for the first time.

To configure costs for Azure DevOps, see the [pricing calculator](#).

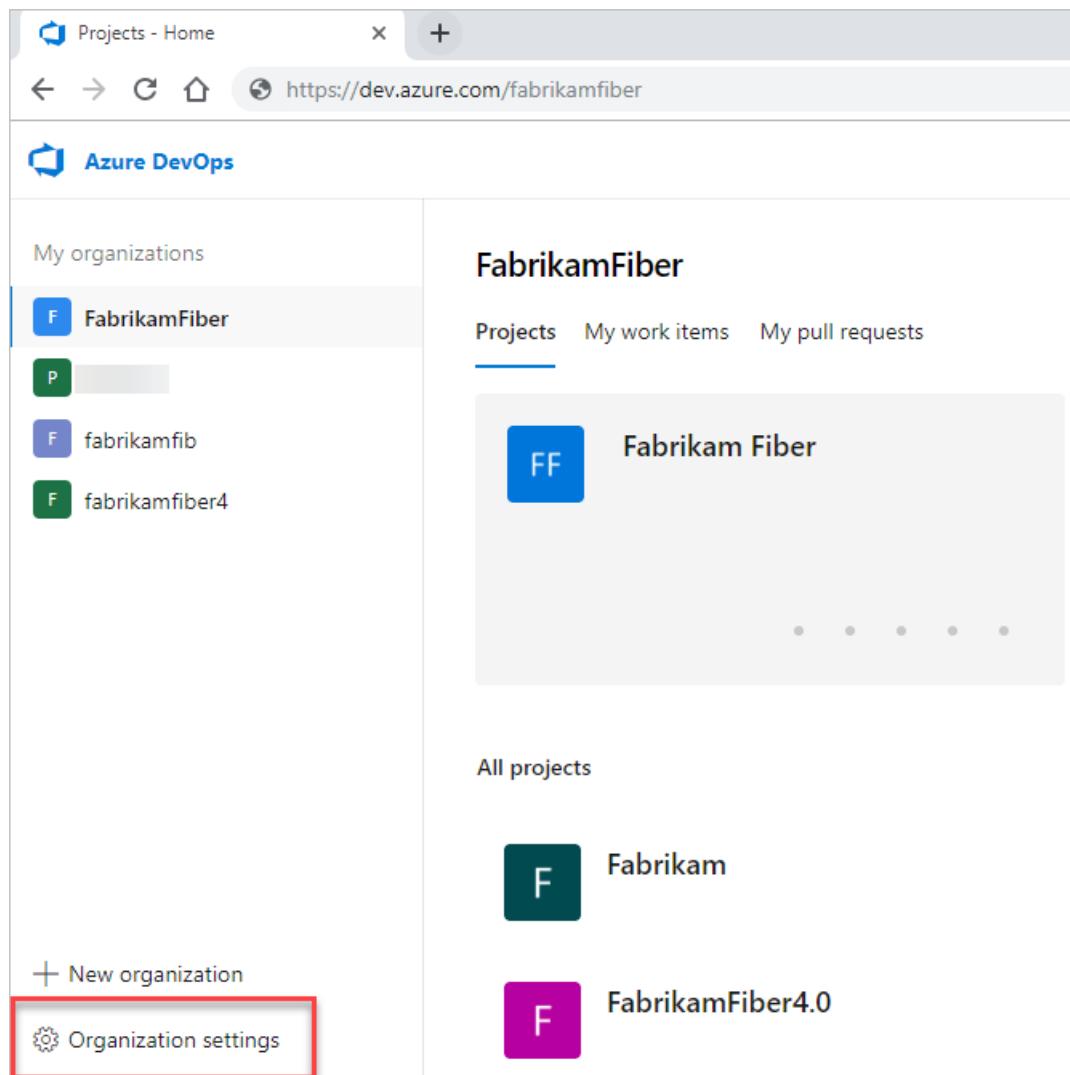
Prerequisites

Ensure the following is true:

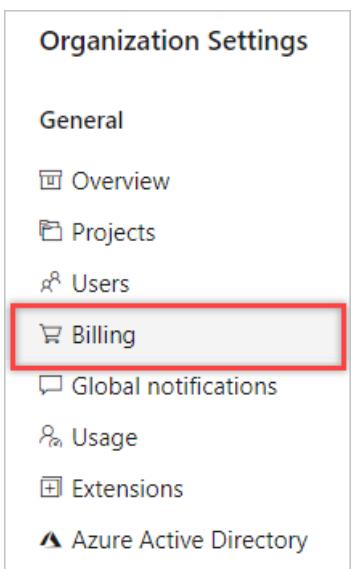
- [Billing is set up for your organization](#)
- You have [Project Collection Administrator](#) or [organization Owner](#) permissions

Increase amount of paid users

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



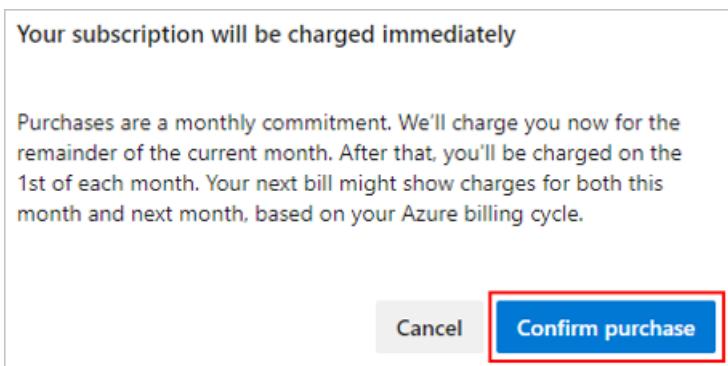
3. Select **Billing**.



4. Enter the number of **paid users**, and then choose **Save**. You also see the number of free users that are included, which is separate.

Users	Free	Paid
Basic users	5	0

5. Select **Confirm purchase**.



6. In **Organization settings**, select **Users**.

The number of users to whom you can assign Basic appears on the right side of your screen.

Settings · Users (Fabrikam) ...

https://azure.devops.com/fabrikamfiber/

Azure DevOps ...

Summary

Extensions	Access Level
Package Management	Visual Studio Enterprise
	Stakeholder
	Basic
	Early Adopter
	Basic

Users

Basic	5
5 free 0 paid 5 assigned 0 available	
Early Adopter	2
Stakeholder	1
Visual Studio Enterprise subscription	2
Visual Studio Subscriber	1
Total Users	11

Extensions

Package Management	5 free 0 paid 0 assigned 5 available
--------------------	--

The screenshot shows the 'Manage users' section of the Azure DevOps interface. On the left, there's a list of users with their names and email addresses. On the right, a summary panel displays user counts for different categories. A red box highlights the 'Basic' category, which has 5 users.

Category	Count
Basic	5
Early Adopter	2
Stakeholder	1
Visual Studio Enterprise subscription	2
Visual Studio Subscriber	1
Total Users	11

Decrease amount of paid users

As your team contracts, you can decrease the number of paid users in your organization.

NOTE

To reduce or cancel users who have paid Basic access for the next month, make your changes before the last day of the month. Your charges won't change until the next month because paid users are monthly purchases.

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

The screenshot shows the Azure DevOps 'My organizations' page. On the left, there's a sidebar with 'My organizations' and a list of organizations: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are links for 'New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area displays the 'FabrikamFiber' organization details, including its projects: 'Fabrikam Fiber', 'Fabrikam', and 'FabrikamFiber4.0'. At the bottom of the main area, there are 'All projects' and a 'More' button.

3. Select **Billing**.

The screenshot shows the 'Organization Settings' page under the 'General' section. The menu items include: Overview, Projects, Users, **Billing** (highlighted with a red box), Global notifications, Usage, Extensions, and Azure Active Directory.

4. Enter a lesser quantity of **paid users**, and then choose **Save**.

Users	Free	Paid
Basic users	5	2

Next steps

[Buy CI/CD](#)

Quickstart: Buy Basic + Test Plans access for users

6/21/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

In this quickstart, you learn how to pay for more users who need access to [Azure Repos](#), [Azure Boards](#), and [Azure Test Plans](#).

[Visual Studio Enterprise](#), [Visual Studio Test Professional](#) and [MSDN Platforms](#) subscribers have Basic + Test Plans included with their subscription, and their subscription is detected when they sign in to Azure DevOps for the first time.

To configure costs for Azure DevOps, see the [pricing calculator](#).

Prerequisites

Ensure the following is true:

- [Billing is set up for your organization](#)
- You have [Project Collection Administrator](#) or [organization Owner](#) permissions

Increase amount of paid users

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P", "fabrikamfib", and "fabrikamfiber4". Below this is a button for "New organization" and "Organization settings", which is highlighted with a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there's a card for "Fabrikam Fiber". Below this are cards for "All projects", "Fabrikam", and "FabrikamFiber4.0".

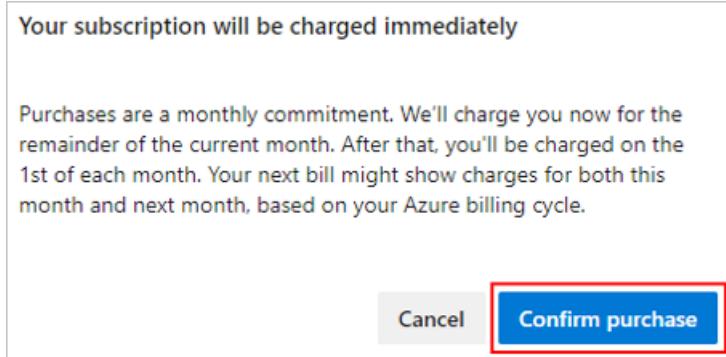
3. Select **Billing**.

The screenshot shows the "Organization Settings" page under the "General" tab. The sidebar includes links for "Overview", "Projects", "Users", "Billing" (which is highlighted with a red box), "Global notifications", "Usage", "Extensions", and "Azure Active Directory".

4. Enter the number of **paid users**, next to Basic + Test Plans, and then choose **Save**.

Users	Free	Paid
Basic users	5	0
Basic + Test Plans (was Test Manager)		0

5. Select **Confirm purchase**.



NOTE

We're moving from assignment of the Test Manager extension to assignment of the Basic + Test Plans access level, so you may have one or the other to assign, but the amount you can assign is the same for either. [Learn more](#).

Decrease amount of paid users

As your team contracts, you can decrease the number of paid users in your organization. Follow the same process as increasing the amount, only enter a lesser quantity of **paid users**, and then select **Save**.

IMPORTANT

To reduce or cancel users who have paid Basic + Test Plans access for the next month, make your changes before the last day of the month. Your charges won't change until the next month because paid users are monthly purchases.

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled 'My organizations' with icons for 'FabrikamFiber' (selected), 'P' (unselected), 'fabrikamfib' (unselected), and 'fabrikamfiber4' (unselected). Below this are buttons for '+ New organization' and 'Organization settings'. The 'Organization settings' button is highlighted with a red box. The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. Under 'Projects', there's a card for 'Fabrikam Fiber' with a blue 'FF' icon. Below it, under 'All projects', are cards for 'Fabrikam' (dark teal 'F' icon) and 'FabrikamFiber4.0' (pink 'F' icon). At the top, the browser bar shows 'Projects - Home' and the URL 'https://dev.azure.com/fabrikamfiber'.

3. Select **Billing**.

The screenshot shows the 'Organization Settings' page. On the left, there's a sidebar with sections: 'General', 'Overview', 'Projects', 'Users', 'Billing' (highlighted with a red box), 'Global notifications', 'Usage', 'Extensions', and 'Azure Active Directory'. The 'Billing' section is the active tab.

4. Enter a lesser quantity of **Basic + Test Plans users**, and then choose **Save**.

Next steps

[Buy CI/CD](#)

Quickstart: Buy CI/CD for Azure DevOps

6/21/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

In this quickstart, you learn how to buy self-hosted or Microsoft-hosted CI/CD and change your paid Azure Pipelines capacity.

With Azure Pipelines, you can run builds and deploy releases by using the Microsoft-hosted agents, your own machines, or both. We offer a *free tier* for each. The *free tier* includes:

- Free tier of Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month)
- One self-hosted CI/CD concurrent job

To estimate costs for Azure DevOps, view the [pricing calculator](#).

Microsoft-hosted CI/CD

Each organization starts out with the *free tier* of Microsoft-hosted CI/CD. This tier provides the ability to run one parallel build or release job, for up to 30 hours per month. If you need to run more than 30 hours per month, or you need to run more than one job at a time, you can switch to paid Microsoft-hosted CI/CD.

When you pay per parallel job, there are no monthly time limits for your builds and releases, and the maximum runtime for a single job is increased from 60 minutes to 6 hours. With Microsoft-hosted CI/CD, the price includes all infrastructure that Microsoft runs (virtual machines, databases, storage, and egress) to deliver this service.

NOTE

When you purchase your first Microsoft-hosted parallel job, the number of parallel jobs you have in the organization still stays at one. This purchase only removes the limits on the free parallel job that you have. To run two jobs concurrently, you need to purchase two parallel jobs.

If your pipelines are in a [public project](#), then you run up to 10 free parallel jobs with unlimited minutes on Microsoft-hosted agents. If you need more, simply [contact us](#).

Self-hosted CI/CD

Azure Pipelines also offers you a way to run the agent on machines that you manage, whether your machines are on-premises or in the cloud. Typically, you'll choose this option in either of the following situations:

- Custom software that runs in your build process is not included in the Microsoft-hosted option.
- You already have an Azure DevOps Server build server running, and you aren't ready to move your build definitions to Azure Pipelines.

Self-hosted public projects

If your pipelines are in a [public project](#), then you run up to 10 free parallel jobs with self-hosted agents. If you need more, simply [contact us](#).

Self-hosted private projects

The *free tier* is one parallel job. In addition, you get one free parallel job for each Visual Studio Enterprise subscriber that is a member of your organization. You can get more using paid self-hosted parallel jobs.

Prerequisites

Ensure the following is true:

- [Billing is set up for your organization](#)
- You have [Project Collection Administrator or organization Owner permissions](#)

Increase quantity of CI/CD

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

2. Select **Organization settings**.

The screenshot shows the Azure DevOps 'Organization settings' page. The left sidebar lists 'My organizations' with items: 'FabrikamFiber' (selected), 'P', 'fabrikamfib', and 'fabrikamfiber4'. Below this are 'New organization' and 'Organization settings'. The main area shows the 'FabrikamFiber' organization with its projects: 'Fabrikam Fiber' (selected), 'Fabrikam', and 'FabrikamFiber4.0'. The 'Organization settings' link in the sidebar is highlighted with a red box.

3. Select **Billing**.

Organization Settings

General

- Overview
- Projects
- Users
- Billing**
- Global notifications
- Usage
- Extensions
- Azure Active Directory

4. Enter the amount of Microsoft-hosted CI/CD or Self-hosted CI/CD, and then select **Save**.

Pipelines for private projects	Free	Paid
MS Hosted CI/CD	1800 minutes	<input type="text" value="0"/>
Self-Hosted CI/CD	1	<input type="text" value="0"/>

Visit [parallel jobs](#) for full details on free pipelines and public concurrency

5. Select **Confirm purchase**.

Decrease quantity of CI/CD

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

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', which is highlighted with a red box. The main area is titled 'FabrikamFiber' and shows 'Projects' (selected), 'My work items', and 'My pull requests'. It features a card for 'Fabrikam Fiber' with a blue 'FF' icon. Below it, under 'All projects', are cards for 'Fabrikam' (dark green 'F') and 'FabrikamFiber4.0' (purple 'F').

3. Select **Billing**.

The screenshot shows the 'Organization Settings' menu. It includes sections for General, Overview, Projects, Users, **Billing** (which is highlighted with a red box), Global notifications, Usage, Extensions, and Azure Active Directory.

4. Enter a lesser quantity of **Microsoft-hosted CI/CD** or **Self-hosted CI/CD**, and then select **Save**.

View parallel job details

To view your current CI/CD capacity details and consumption, complete the following steps.

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

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' organization. On the left sidebar, under 'My organizations', the 'FabrikamFiber' project is selected and highlighted with a red border. Other organizations listed are 'P', 'fabrikamfib', and 'fabrikamfiber4'. Below the sidebar, there's a section for 'All projects' displaying two items: 'Fabrikam' and 'FabrikamFiber4.0'. At the bottom of the sidebar, there are links for '+ New organization' and 'Organization settings', with 'Organization settings' also highlighted by a red border.

go to your organization toolbar, and then go to **Parallel jobs** under **Pipelines**.

<p>Organization Settings</p> <p>General</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Overview<input checked="" type="checkbox"/> Users<input checked="" type="checkbox"/> Billing<input checked="" type="checkbox"/> Auditing<input checked="" type="checkbox"/> Global notifications<input checked="" type="checkbox"/> Usage<input checked="" type="checkbox"/> Extensions<input checked="" type="checkbox"/> Azure Active Directory <p>Security</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Policies<input checked="" type="checkbox"/> Permissions <p>Boards</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Process <p>Pipelines</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Agent pools<input checked="" type="checkbox"/> Deployment pools<input checked="" type="checkbox"/> Parallel jobs<input checked="" type="checkbox"/> OAuth configurations	<h2>Overview</h2> <p>Name</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">FabrikamFiber</div> <p><input checked="" type="checkbox"/> Use the new URL: https://dev.azure.com/FabrikamFiber/ Learn more about URLs</p> <p>Privacy URL</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%; height: 40px;"></div> <p>Learn more about the Privacy URL</p> <p>Description</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">Add organization description</div> <p>Time zone</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">(UTC+00:00) Dublin, Edinburgh, Lisbon, London</div> <p>Region</p> <p>West Central US</p> <p><input type="button" value="Save"/> ⓘ Changes made will affect all projects and members of</p> <hr/> <h3>Organization owner</h3> <div style="display: flex; align-items: center;"><div style="flex-grow: 1; border: 1px solid #ccc; padding: 5px; border-radius: 5px; width: 150px; height: 40px; background-color: #f0f0f0; display: flex; align-items: center; justify-content: center;"><p>Change owner</p></div></div>
---	---

XAML build

The hosted XAML build controller is no longer supported. Organizations created on or after April 2016 don't have access to it. The hosted YAML model is our newest build model, and as a best practice, consider adopting it. Read more about it [here](#).

Important: If you have an organization where you still need to run [XAML builds](#), you should set up an [on-premises build server](#) and switch to an [on-premises build controller](#) now.

Next steps

[Try Azure Test Plans for free](#)

Sign up for Azure Artifacts

7/3/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

This article guides you through the sign-up process for Azure Artifacts. Azure Artifacts is a service where you can create package feeds to publish and consume Maven, npm, NuGet, Python, and universal packages. Azure Artifacts is billed on a consumption basis, and is free up until 2GB of storage. In the case that your organization needs more storage, you need to set up billing.

For on-premises versions, TFS 2017 and 2018, see [License Azure Artifacts](#).

Prerequisites

Ensure that the following is true:

- [Billing is set up for your organization](#)
- You have [Project Collection Administrator or organization Owner permissions](#)

Billing and free monthly usage

Azure Artifacts includes a free usage tier of 2 GB. Any usage below this level isn't billed to your subscription. Above this limit, we charge you for your actual usage. The usage limit allows you to control the maximum volume of storage that you are billed for. Once the maximum usage limit is reached, you can no longer upload artifacts. For more information on usage tiers, see the [Azure Artifacts pricing page](#).

View storage used

See and manage what your overall storage use is for Azure Artifacts.

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are 'New organization' and 'Organization settings' (which is highlighted with a red box). The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. It shows a project card for 'Fabrikam Fiber' with a blue 'FF' icon. Below it, under 'All projects', are cards for 'Fabrikam' (dark green 'F') and 'FabrikamFiber4.0' (purple 'F').

3. Select **Billing**.

The screenshot shows the 'Organization Settings' page. Under 'General', there are several sections: 'Overview', 'Projects', 'Users', 'Billing' (which is highlighted with a red box), 'Global notifications', 'Usage', 'Extensions', and 'Azure Active Directory'.

4. Find Artifacts and review your current usage.

Billing

Pipelines for private projects	Free	Paid	
MS Hosted CI/CD Link	1800 minutes	0	
Self-Hosted CI/CD Link	1	0	
Visit parallel jobs for full details on free pipelines and public concurrency			
Boards, Repos and Test Plans	Free	Paid	
Basic users Link	5	0	
Basic + Test Plans Link	Start free trial		
Resources	Free	Used	Usage limit
Artifacts Link	2 GB*	Less than 1 GB	Up to 2 GB free
Cloud-based load testing Link	20000 VUMs	0 VUMs	20,000

Pay for Artifacts

Each organization gets Azure Artifacts for free, up until they hit 2GB of storage. If you need more than that, complete the following steps to set up billing.

1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Repeat steps #2 and #3 from [View storage used](#).
3. Find Artifacts, under Resources, and increase the usage limit above the free tier, by selecting from the dropdown menu. Then, select **Save**. You are only charged for the storage you use, up to the limit.

Billing

Azure Subscription ID

8ae121ee-03b2-429b-a168-1ed367a8d0a0

Change billing

Pipelines for private projects	Free	Paid
MS Hosted CI/CD <small>1</small>	1800 minutes	0
Self-Hosted CI/CD <small>1</small>	1	0

Visit [parallel jobs](#) for full details on free pipelines and public concurrency

Boards, Repos and Test Plans	Free	Paid
Basic users <small>5</small>	5	0
Basic + Test Plans <small>1</small>		0

Resources Free Used Usage limit

Artifacts <small>1</small>	2 GB*	Less than 1 GB	Up to 2 GB free
----------------------------	-------	----------------	-----------------

Cloud-based load testing <small>1</small>	20000 VUMs	0 VUMs	Up to 2 GB free
---	------------	--------	-----------------

*Organizations created before May 6, 2019 receive free storage for 12 months.

- Up to 12 GB
- Up to 52 GB
- Up to 102 GB
- Up to 1002 GB
- No limit, pay for what you use

[Save](#)

NOTE

If you have reached your storage limit and are blocked from making additional uploads, it can take up to 1 hour after increasing your limit for uploads to be re-enabled.

FAQs

Q: Which artifacts count towards my storage total?

A: Currently, the following get counted towards your storage total:

- All npm, NuGet, Python, Maven, and universal packages (including those stored from upstream sources)
- All symbols

Pipeline Artifacts, Build Artifacts, and Pipeline Caching are included in Azure Pipelines and do not count towards your storage total in Azure Artifacts as of today.

Q: Why do I see 0GB of storage, even though I am storing artifacts?

A: Currently, the billing page only shows integers of storage (0GB, 1GB, 2GB, etc.). It is likely that even though you have artifacts stored, you haven't gotten to 1GB yet, which is our lowest granularity right now.

Q: How can I control how long artifacts are stored?

A: Azure Artifacts retention is controlled by feed retention policy settings. Symbols also contribute to Azure Artifacts storage usage. Symbols retention is controlled by build retention policy.

For more information on how to set the feed retention policy, see how to [automatically delete old package versions with retention policies](#).

Q: How long does it take for deleted artifacts to affect the amount of used storage?

A: Deletion of artifacts doesn't register immediately. It can take up to 24 hours for the usage level to be updated. If

you're blocked from uploading artifacts, you can temporarily increase your usage level to continue publishing artifacts, and then reduce the level once the storage metrics are updated.

Usage is updated once per day, so when you delete Artifacts, it may not reflect immediately. For more information, see [Delete and recover packages in Azure Artifacts](#).

Q: What happens if I remove my Azure Subscription from my Azure DevOps organization?

A: If you remove your Azure Subscription from your Azure DevOps organization, you will only have access to the free tier of storage (< 2GB). If you have above 2GB of storage used, you will be able to read packages but will no longer be able to push until you either get your usage below 2GB, or reconnect an Azure Subscription to your organization and increase your storage tier appropriately.

Q: What about customers who were using Artifacts before May 6, 2019 under the previous per user model?

A: Customers before May 6, 2019 won't be charged for Artifacts storage until May 6, 2020. These customers can opt in to the new storage model by setting a paid limit above the amount of storage they are currently using. Then, starting on May 6, 2020, you're charged under the new storage model.

Quickstart: Try Azure Test Plans for free

7/1/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

In this quickstart, you learn how to try [Azure Test Plans](#) for 30 days free.

Prerequisites

Ensure you have [Project Collection Administrator](#) or [organization Owner](#) permissions.

Try Azure Test Plans

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

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. At the bottom of this sidebar are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area shows the 'FabrikamFiber' organization with tabs for 'Projects', 'My work items', and 'My pull requests'. Below this are sections for 'Fabrikam Fiber' (with a large blue 'FF' icon) and 'All projects' (showing 'Fabrikam' and 'FabrikamFiber4.0').

3. Select **Billing**.

Organization Settings

General

- [Overview](#)
- [Projects](#)
- [Users](#)
- [Billing](#)
- [Global notifications](#)
- [Usage](#)
- [Extensions](#)
- [Azure Active Directory](#)

4. Select **Start 30-day Test Plans trial**.

Boards, Repos and Test Plans	Free	Paid
Basic users ?	5	0
Basic + Test Plans ?	Start 30-day Test Plans trial	

5. Select **Start free trial**.

Boards, Repos and Test Plans	Free
Basic users ?	5
Basic + Test Plans ?	Start free trial

Next steps

[Create a test plan](#)

Quickstart: Buy cloud-based load testing for Azure DevOps

6/21/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

NOTE

The cloud-based load testing service is deprecated. More information about the deprecation, the service availability, and alternative services can be found [here](#).

In this quickstart, you learn how to enable paid load testing in Azure DevOps.

Azure DevOps offers a cloud-based solution for [load testing your apps](#). You can create load tests by using Visual Studio Ultimate 2013, Visual Studio Enterprise 2015, or later versions. Then you can run these tests in Azure DevOps.

Load tests are measured and billed in virtual user minutes (VUMs) as described in this Q&A: [What are VUMs?](#) [How many minutes will my load test use?](#)

If you don't have an Azure subscription, [create a subscription](#) before you begin.

To configure costs for Azure DevOps, see the [pricing calculator](#).

Prerequisites

[Set up billing for your organization](#).

Enable paid load testing

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber" (blue icon), "Fabrikam" (dark teal icon), and "FabrikamFiber4.0" (purple icon). At the bottom of the main area, it says "All projects".

3. Select **Billing**.

The screenshot shows the "Organization Settings" page. On the left, there's a sidebar with the following menu items: "General", "Overview", "Projects", "Users", "Billing" (which is highlighted by a red box), "Global notifications", "Usage", "Extensions", and "Azure Active Directory".

4. Select the dropdown menu for Cloud-based load testing, and then select **On**.

You can set a monthly limit on the virtual user minutes that you use by selecting an amount from the **PAID LOAD TESTING LIMIT** drop-down menu. When you're done, choose **Save**.

The screenshot shows the Azure portal's settings interface for cloud-based load testing. At the top, there are tabs for 'Cloud-based load testing' and '20000 VUMs'. Below these are dropdown menus for 'On' (set to 'On') and 'Paid load testing limit'. The 'Paid load testing limit' dropdown is currently open, displaying a list of options: 'No Limit' (which is highlighted), 50,000, 100,000, 500,000, 1,000,000, 5,000,000, 10,000,000, and 20,000,000. A 'Save' button is located at the bottom left of the settings area.

Cloud-based load testing is enabled for your organization.

Billing and free monthly usage

You're charged for only the virtual user minutes of cloud-based load testing used above the *free tier* of user minutes per month. The *free tier* includes:

- Five Azure DevOps users (Basic)
- Free tier of Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month)
- 2GB of Azure Artifacts storage
- One self-hosted CI/CD concurrent job
- 20,000 virtual user minutes of cloud-based load testing
- The *free tier* resets on the first day of the month.
- Visual Studio subscriptions don't include any additional virtual user minutes. The free amounts are per organization, not per user.
- For cloud-based load testing, you're charged for each [virtual user minute](#) that exceeds the free monthly usage.
- Graduated discounts for cloud-based load testing are calculated based on your Azure subscription billing cycle.

Limits on load test runs

There's a limit on the duration for each test run. For cloud-based load testing, the limit depends on where you run your test. For details, see [this Q&A](#).

Next steps

[Load test your app](#)

Add a user who can set up billing for Azure DevOps

6/7/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

In this article, learn how to let a user [set up billing](#) or [change billing](#) for your organization. Go to the **Subscriptions** tab and add **owner**, **contributor**, **service admin**, or **co-admin** roles to users in the Azure subscription that your organization uses for Azure DevOps billing.

1. [Sign in to the Azure portal](#) as the Azure subscription administrator.
2. Enter *subscriptions* in the search box, and then select **Subscriptions** from the drop-down menu. If more than one subscription is listed, choose the subscription to modify.

The screenshot shows the Microsoft Azure Subscriptions blade. On the left is a navigation sidebar with options like 'Create a resource', 'All services', 'FAVORITES' (which includes 'Resource groups', 'Azure Active Directory', 'Dashboard', 'All resources', 'App Services', 'Function Apps', and 'SQL databases'). The main area is titled 'Subscriptions' under 'Commerce Test Directory'. It shows a table with columns: SUBSCRIPTI..., SUBSCRIPTION ID, MY ROLE, and CURRE... . A single row is selected, showing 'Jamal Hartnett...' as the name, '266640fb-5c34-44df-8db1-3f4f5628e5ae' as the Subscription ID, 'Owner' as the My Role, and '\$0.00' as the current value. This selected row is highlighted with a red box.

3. Choose **Access control (IAM)**.

The screenshot shows the 'Access control (IAM)' section of the Azure Subscriptions blade for 'Jamal Hartnett's Pay-As-You-Go'. The left sidebar has links for 'Overview', 'Access control (IAM)' (which is highlighted with a red box), 'Diagnose and solve problems', 'Security (Preview)', 'Events', 'Cost Management', and 'Cost analysis'. The main pane displays subscription details: 'Subscription ID' (266640fb-5c34-44df-8db1-3f4f5628e5ae), 'Subscription name' (Jamal Hartnett's), 'Directory' (Commerce Test Directory (mstestvsocom...)), 'Current billing period' (Not available), 'My role' (Owner), 'Currency' (USD), 'Offer' (Pay-As-You-Go), 'Status' (Disabled), and 'Offer ID' (MS-AZR-0003P).

4. Choose **Add**.

Home > Subscriptions > Jamal Hartnett's Pay-As-You-Go > Access Control - Role assignment

Access Control - Role assignment

Jamal Hartnett's Pay-As-You-Go

+ Add Remove Refresh Help

Manage

Role assignment Roles

Name i:
Type i: All
Role i: 2 selected
Scope i: All scopes
Group by i: Role
2 items (2 Users)

5. In the drop-down menus, select the *role* to add members to and select an *assignment type*.

Role i: Contributor
Assign access to i: Azure AD user, group, or application

6. Select a user or group by entering their *name* or *email alias*. (Select a device by entering its *name*.)

Search by name or email address

Selected members:

 Christie Church fabrikamfiber1@hotmail.com Remove

Save Discard

7. If your update is complete, choose **Save**.

A user who can [set up](#) or [change billing](#) is added to your organization.

NOTE

To give access to a user who's not in your directory, the user must accept the invitation that's received via email before they can access the Azure subscription.

Related articles

- [Set up billing](#)
- [Change the Azure subscription for billing](#)
- [Azure DevOps pricing](#)
- [Azure DevOps billing support](#)

Change or remove the Azure subscription that your organization uses for billing

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

In this article, learn how to change the Azure subscription that your organization uses for billing or remove your billing subscription at any time.

To configure costs for Azure DevOps, see the [pricing calculator](#).

Prerequisites

- To change or remove your billing subscription, you must be a member of the [Project Collection Administrators group](#) or be the [organization owner](#).
- To change your Azure billing subscription, you must be added [as an Owner or Contributor to an Azure subscription](#) that you can use to purchase.

Change your subscription

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this are buttons for "+ New organization" and "Organization settings", with "Organization settings" highlighted by a red box. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests", with "Projects" selected. A card for the "Fabrikam Fiber" project is shown, featuring its logo (blue square with FF) and name. Below this, under "All projects", are cards for "Fabrikam" (dark teal square with F) and "FabrikamFiber4.0" (purple square with F).

3. Select **Billing**.

The screenshot shows the "Organization Settings" page. It has a sidebar with sections: "General", "Overview", "Projects", "Users", "Billing" (highlighted by a red box), "Global notifications", "Usage", "Extensions", and "Azure Active Directory".

4. Select **Change Billing**.

Organization Settings

- General
- Overview
- Projects
- Users
- Billing
- Global notifications

Billing

Azure Subscription ID

8ae121ee-03b2-429b-a168-1ed367a8d0a0

[Change billing](#)

5. Select your Azure subscription, and then select **Save**.

Pay-As-You-Go-17
fa8937c6-c964-4f15-8ae7-5fa9d22b6df5

Subscription is valid

[+ New Azure subscription](#)

[Cancel](#) Save

Remove your billing subscription

NOTE

When you remove the billing subscription from your organization, any paid quantities of Basic, Azure Artifacts users, Azure Test Plans users, Microsoft-hosted CI/CD, and self-hosted CI/CD you've paid for this month continue uninterrupted until the 1st of next month, but your organization reverts immediately to the Free Tier for [cloud-based load testing](#). Removing the subscription also cancels any non-Microsoft paid extensions without refund or credit.

1. Sign in to your organization, choose **Organization settings**, choose **Billing**, and then choose **Change billing** following steps 1 through 4 provided in the [Change the subscription](#) section.
2. Choose **Remove billing** and then choose **Save**.

Remove billing

Your organization will go back to the free organization limits immediately. CI/CD parallel jobs and features purchased for your users are valid until the end of the month. Any non-Microsoft extensions will be canceled without a refund or credit.

[+ New Azure subscription](#)

[Cancel](#) Save

Related articles

- [Buy Basic access for users](#)
- [Buy Azure Test Plans](#)
- [Buy CI/CD](#)
- [Sign up for Azure Artifacts](#)

Buy access to Azure DevOps Server or Azure Test Plans

6/18/2019 • 3 minutes to read • [Edit Online](#)

[Azure Pipelines](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

For [Azure DevOps Server](#), you pay per user for [Basic](#) features like Code or Agile Planning. Users who have a [Visual Studio subscription](#) are free to add because Basic features are included in their subscription as a benefit. It's also free to add [Stakeholders](#), which provides access to a limited set of features.

Paid users are entitled access to Basic features in your company's Azure DevOps Server. Paying monthly for users is a great alternative to buying User CALs, which typically have a 3-year commitment term. When you buy access in this way, you aren't required to use Azure DevOps Services (although you can use Azure DevOps Services in addition to Azure DevOps Server).

You can also buy [Basic + Test Plans](#) for your users monthly. This method is an alternative way to buy a Visual Studio subscription that's entitled to use Azure Test Plans in Azure DevOps Server.

To learn more about the requirements to access Azure DevOps Server or Azure Test Plans, see [Change access levels](#). For more information about licensing, see the [pricing page](#). To configure costs for Azure DevOps, see the [pricing calculator](#).

Buy monthly access to Azure DevOps Server for your users

1. [Sign up for an organization](#), if you don't have one already.
2. You can use Azure DevOps Server features, like Basic or Azure Test Plans up to your total entitlements across Visual Studio subscription purchases, Azure DevOps Server CALs, and paid users in Azure DevOps. Based on your number of users, [pay for users](#).
3. [Add users](#) to your organization so you can more easily track these users.

These users are invited to your organization, but you're not required to use Azure DevOps.

4. As the Azure DevOps Server administrator, [add these same users to Azure DevOps Server](#). Give them the necessary access.

NOTE

Azure DevOps Server doesn't detect what happens in Azure DevOps Services. Make sure to add these users to Azure DevOps Server and assign them the Basic access level.

If you stop paying for these users within your organization, your administrator should remove the users from Azure DevOps Server or buy Azure DevOps Server CALs for them.

Buy monthly access to Azure Test Plans

1. [Sign up for an organization](#), if you don't have one already.
2. Based on the amount of users who need Azure Test Plans access in Azure DevOps Server, [buy Basic + Test Plans](#).

Test Plans installs automatically in Azure DevOps Server.

3. [Add users](#) to your organization. Assign them Basic + Test Plans so you can track these users.

These users are invited to your organization, but are not required to use Azure DevOps Services. By assigning Basic + Test Plans or Microsoft Test Manager within your organization, your users can also run Visual Studio Test Professional 2015 or [2017](#). If you only add the users to Azure DevOps Server, they can't run Test Professional.

NOTE

These users must sign in to Visual Studio Test Professional with the same credentials that they used to join your organization.

4. As the Azure DevOps Server administrator, [add these same users](#). Give them Basic + Test Plans access so they can use Azure Test Plans.

1. [Sign up for an organization](#), if you don't have one already.

2. Based on the amount of users who need Azure Test Plans access in Azure DevOps Server, [buy Basic + Test Plans access](#).

Test Plans installs automatically in Azure DevOps Server.

3. [Add users](#) to your organization. Assign them Basic + Test Plans access so you can track these users.

4. As the Azure DevOps Server administrator, [add these same users](#). Give them Advanced access so they can use Azure Test Plans.

NOTE

Azure DevOps Server doesn't detect what happens in Azure DevOps Services.

If you stop paying for these users, your administrator should remove those users from Azure DevOps Server.

Q&A

Q: Why should I pay via Azure DevOps Services for my Azure DevOps Server users?

A: You get many benefits, for example:

- Paying via Azure DevOps Services gives your users the flexibility to access both Azure DevOps Server and Azure DevOps Services for the same price.
- You can pay monthly for users who need temporary access.
- You get all the purchasing capabilities that Azure offers like payment via credit card, through a Cloud Solution Provider (CSP) partner, through the Enterprise Agreement, and more.

Q: Where can I learn more about Azure DevOps Server CALs and access levels for Azure Test Plans?

A: See [Change access levels](#).

Related articles

- [Azure DevOps pricing](#)
- [Azure DevOps billing support](#)

Billing FAQs

7/1/2019 • 8 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

In this article, you can find answers to frequently asked questions about billing for your organization.

Make sure to review [Azure DevOps pricing](#) and the [billing overview](#).

You need to set up billing when you need more than the *free tier* of resources in your organization:

- Five Azure DevOps users (Basic)
- Free tier of Microsoft-hosted CI/CD (one concurrent job, up to 30 hours per month)
- 2GB of Azure Artifacts storage
- One self-hosted CI/CD concurrent job
- 20,000 virtual user minutes of cloud-based load testing

NOTE

The cloud-based load testing service is deprecated. More information about the deprecation, the service availability, and alternative services can be found [here](#).

You also need to [set up billing](#) to buy other features (for your users) that are offered by Microsoft or by other companies.

To configure costs for Azure DevOps, see the [pricing calculator](#).

Q: Can I buy Azure DevOps by using a purchase order?

A: No. Azure DevOps must be purchased through an Azure subscription. (Think of it as your Azure billing account.)

Q: What types of Azure subscriptions can be used to buy Azure DevOps?

A: Almost all Azure subscriptions can be used. We support Azure subscriptions connected to your [Enterprise Agreement \(EA\)](#), Azure subscriptions set up by Cloud Solution Providers (CSPs), Azure subscriptions set up through Microsoft Open License resellers, and Pay-As-You-Go Azure subscriptions. You can even buy using Azure subscriptions that Visual Studio subscribers set up as a subscriber benefit. (But no, you can't use your monthly credit to pay for more Visual Studio subscriptions.)

The only notable exclusion is that you can't use the [Azure free trial](#), Government, or National clouds.

Q: Can I use the monthly Azure credits from my Visual Studio subscription to buy Azure DevOps?

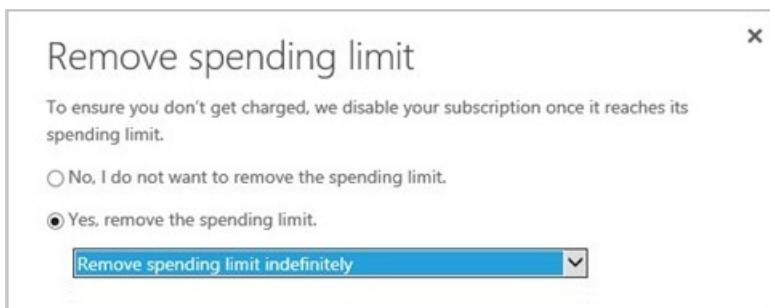
A: No, you can't use the monthly Azure credits from [Visual Studio subscriptions](#) to pay for Azure DevOps. Before you make purchases by using this type of Azure subscription, you must [remove your spending limit](#).

[Continue](#)

This subscription has a spending limit. Create a new Azure subscription or [remove your spending limit](#) to continue.

NOTE

Remove your spending limit indefinitely. This prevents disabling your Azure subscription when your recurring monthly charges are billed the next month. Otherwise, all resources billed to this subscription are suspended, including virtual machines and all other workloads.



Q: What's the difference between daily pro-rated charges instead of monthly committed purchases?

A: With **monthly billing**, purchases are a monthly commitment. With any updates, we charge you for the remainder of the current month. After that, you're charged on the 1st of each month. With **daily billing**, purchases are billed daily on a pro-rated basis. Changes to purchased quantities are reflected in usage billed to your Azure subscription by the following day.

Q: Am I required to buy other Azure services?

A: Not at all. If you only want to buy Azure DevOps via Azure, you can do that.

Q: Can tags be applied to organizations from the Azure portal?

A: No, but this feature is in our backlog to add in the future.

Q: How are paid extensions changing in the Azure DevOps Marketplace in July 2019?

A: Microsoft is ending support for purchasing 3rd party paid Azure DevOps extensions through your Azure bill on July 1st, 2019. Going forward, we're encouraging our publishers to offer paid access to their services directly. We're working closely with publishers to help existing customers transition to the new model and will communicate to specific customers as publishers are ready.

Q: Do I need to pay to add "Package Management" users in Team Foundation Server 2017 and 2018?

A: As of June 1st, 2019, on-premises Azure Artifacts (ie. Package Management) is now included with the Basic license. For Azure DevOps Server 2019, purchase a Basic license and assign it to the user. For TFS 2017 and 2018, no additional purchase is required, but you still need to [assign users the Package Management extension license](#) to use the feature.

Enterprise Agreement customers

Q: Can I use an Enterprise Agreement to buy Azure DevOps?

A: Yes, you can. You need to be an owner or contributor for an Azure subscription that was created for your EA.

Q: How can I tell whether I have the necessary privileges to buy services through my organization's Enterprise Agreement?

A: The easiest approach to determine if you have the right privileges is to select the **Buy** button for a service. You need to select an Azure subscription (which is a billing account) from a presented list of Azure subscriptions that are currently linked to your sign-in. Because the name of the Azure subscription defaults to the type of billing account (for example, "Pay-As-You-Go" or "Enterprise Agreement"), it's often clear if the Azure subscription is part of your Enterprise Agreement.

Another approach is to try to visit the [Azure Enterprise Portal](#). If you can reach it successfully, then you already have either the enterprise admin or the organization owner role. Only organization owners can set up new Azure billing in an Enterprise Agreement.

If you can't access the Azure Enterprise Portal, inquire within your organization to find out who your Enterprise Admin is, and ask that person to add you as an organization owner within the Azure Enterprise Portal. If you can't find this person, you can [submit a support ticket](#) and request the contact information. You need your organization's name and your Enterprise Agreement enrollment number for the support ticket.

Q: Can I use the Azure Monetary Commitment funds from my Enterprise Agreement to buy Azure DevOps?

A: Yes, you can use these prepaid funds for all Azure DevOps services that Microsoft offers. Make sure to choose an Azure subscription that was created for your EA when you [set up billing for your organization](#).

The only exclusion is for extensions offered by partners. These charges appear on your next "overage" invoice. Typically this happens monthly, but due to historical rules for some EA customers, an overage invoice might not be issued for several months. Please consult a licensing specialist for your EA if you need to know what amount of additional purchases (purchases that aren't eligible for Azure Monetary Commitment funds) trigger an overage invoice.

How charges are processed

Q: How are user charges (Azure DevOps User/Basic, Basic + Test Plans, and Azure Artifacts) and CI/CD concurrent job charges (for both Microsoft-hosted and self-hosted CI/CD) processed?

A: At the first purchase, we bill a prorated quantity to cover the remaining days in the current month. For instance, if a purchase of 10 Basic + Test Plans users happens on April 15, then we charge 5 units because 50% of the month remains (15 days of a 30-day month). On the first of May, and each month thereafter until you cancel, the full 10 units is billed.

When you increase the paid quantity later, we also prorate the increased units to cover the remaining days in the current month. So if you buy 1 more Basic + Test Plans user on May 10, we would bill roughly 0.677 units (21 days remaining in the 31-day month of May).

Q: How do reductions or cancellations work?

A: When you reduce or cancel user charges or CI/CD charges, you're canceling automatic renewal. The features and/or CI/CD capacity continue through the end of the current calendar month, taking effect on the first day of the next month.

Changes in Azure subscription status

Q: What happens if I cancel my Azure subscription or my credit card expires?

A: When the Azure subscription used for billing on your organization is not in active status - for example, because you cancel it or the credit card used for billing expires - your organization reverts to the free tier of service. But you'll keep any paid users or paid CI/CD concurrent jobs until next month.

NOTE

You must keep your Azure subscription in good standing to avoid interruptions in paid services.

Q: Where can I check my bill or update billing details on my Azure subscription?

A: If you're the owner or contributor for the Azure subscription used for billing your organization, you can view your billing details in the Billing tab of your Organization settings in Azure DevOps.

Other questions

Q: Why do I no longer see Team Projects in the Azure portal?

A: Starting September 28th, 2018 you can no longer create Team Projects or view them in the Azure portal. You can continue to **access** any Team Projects you have created via the Azure portal through your organization URL (<https://dev.azure.com/{yourorganization}>) and you can always [create new organizations and projects from visualstudio.com](#). Going forward, the best way for Azure users to get started using Azure DevOps is to [create a project](#).

Q: Why is my organization already linked to an Azure subscription?

A: This happens if someone already [set up billing](#) for your organization. Each organization can use only one Azure subscription for billing. Charges can't be split across multiple Azure subscriptions.

Q: Can I use the same Azure subscription for billing across multiple organizations?

A: Yes, you can use the same Azure subscription for billing across multiple organizations. But you can't link a single organization to multiple Azure subscriptions.

Q: Can I buy Azure DevOps from my software reseller?

A: Yes you can, if your reseller participates in the Cloud Solution Provider program. Just ask them.

Buy Azure DevOps now

- [Azure DevOps Users/Basic](#)
- [Microsoft-hosted CI/CD](#) (formerly hosted pipelines)
- [Self-hosted CI/CD](#) (formerly private pipelines)
- [Azure Test Plans](#) (formerly Test Manager)
- [Azure Artifacts](#)

Related articles

- [Set up billing](#)
- [Add backup billing managers](#)
- [Change the Azure subscription for billing](#)
- [Azure DevOps pricing](#)
- [Azure DevOps billing support](#)

Cloud Solution Providers: Buy Azure DevOps

5/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Partners in the Cloud Solution Provider (CSP) program can enable their customers to [pay for Azure DevOps](#) by using a CSP-based Azure subscription.

Prerequisites

To enable your customer to purchase Azure DevOps by using a CSP-based Azure subscription, confirm the following statements are true:

- The customer has [Project Collection Administrator \(PCA\) or organization Owner permissions](#)
- The customer has [Contributor or Owner role permissions](#) to the CSP-based Azure subscription

When your customer gains access to the CSP-based Azure subscription, they can [set up billing](#) or [change billing](#) for their Azure DevOps organization and further charges are billed to the CSP subscription.

Change billing to CSP Azure subscription

CSP steps

1. Sign in to the [Azure portal](#) as CSP.
2. Assign your selected user Contributor access to the CSP Azure subscription.

Customer steps

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

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with a list of organizations: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this is a button for "New organization" and a highlighted "Organization settings" button. The main area is titled "FabrikamFiber" and contains tabs for "Projects", "My work items", and "My pull requests". Under "Projects", there are cards for "Fabrikam Fiber", "Fabrikam", and "FabrikamFiber4.0".

3. Select **Billing**.

The screenshot shows the "Organization Settings" page. The left sidebar lists several options: "General", "Overview", "Projects", "Users", "Billing" (which is highlighted with a red box), "Global notifications", "Usage", "Extensions", and "Azure Active Directory".

4. Select **Change billing**.

Organization Settings

- General
- Overview
- Projects
- Users
- Billing
- Global notifications

Billing

Azure Subscription ID

8ae121ee-03b2-429b-a168-1ed367a8d0a0

[Change billing](#)

5. Select your CSP Azure subscription that you want to be billed with, and then select **Save**.

Cloud Solution Providers: Buy Visual Studio App Center resources

1/25/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Partners in the Cloud Solution Provider (CSP) program can enable their customers to purchase [Visual Studio App Center resources](#) by using a CSP-based Azure subscription. Resources include build pipelines, test device concurrencies, and advanced push notifications.

To enable the customer to purchase App Center resources by using a CSP-based Azure subscription, confirm the following:

- The customer has organization admin rights in App Center, which grants them access to the Billing tab.
- The customer has owner role permissions to the CSP-based Azure subscription in order to make purchases. Learn more about [how to add users with co-owner permissions](#).

Security & Identity

7/1/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

For anyone to access a project, you must add them to a security group. For a quick look at what permissions are assigned to the default security groups, see [Default permissions and access assignments](#).

5-minute quickstarts

- [View permissions](#)
- [Look up the organization owner or a project administrator](#)
- [Add users to a project or team](#)
- [Set Git or TFVC repository permissions](#)
- [Add administrators or set permissions at the project or collection level](#)

Tutorials

- [Set up Active Directory or Azure Active Directory](#)
- [Add AD/Azure AD security groups to built-in security groups](#)
- [Change individual permissions, grant select access to specific functions](#)
- [Grant or restrict permissions to select tasks](#)
- [Remove user accounts](#)

Concepts

- [About permissions and groups](#)
- [About security roles](#)
- [About access levels](#)
- [Azure Active Directory groups \(Azure DevOps\)](#)
- [Active Directory groups \(on-premises\)](#)
- [Security glossary](#)

How-to guides

- [Set Git branch permissions](#)
- [Set build and release permissions](#)
- [Set permissions and access for work tracking](#)
- [Change access levels \(on-premises\)](#)
- [Authenticate with personal access tokens](#)
- [Revoke user PATs - for admins](#)

Reference

- [Default permission and access assignments](#)
- [Permissions lookup guide](#)
- [Permissions and groups reference](#)

- [Azure DevOps Services data protection](#)
- [Authentication guidance for REST APIs](#)
- [Add IP addresses and URLs to allow list](#)

Resources

- [REST API, Permissions](#)
- [Server Administration \(on-premises\)](#)

About security and identity

5/31/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Azure DevOps Services, our cloud-hosted application, is based on the capabilities of Azure DevOps Server 2019 (formerly known as Team Foundation Server), with additional cloud services. Both support software development projects, from planning through deployment. Azure DevOps uses Microsoft Azure's Platform as a Service infrastructure and many of Azure's services, including Azure SQL databases, to deliver a reliable, globally available service for your development projects.

This article introduces the main security concepts employed by Azure DevOps. To learn more about the steps Microsoft takes to keep your projects in Azure DevOps safe, available, secure, and private, see this white paper, [Azure DevOps Services Data Protection Overview](#).

The main security concepts to understand are

- Authentication
- Authorization
- Security groups
- Security roles
- Permission levels and permissions
- Access levels

Authentication

Authentication verifies a user's identify based on the credentials provided when they sign into Azure DevOps. These systems integrate with and rely upon the security features provided by these additional systems:

- Azure Active Directory (Azure AD)
- Microsoft account (MSA)
- Active Directory (AD)

Azure AD and MSA support cloud authentication. We recommend Azure AD when you need to manage a large group of users. Otherwise, if you have a small user base accessing your organization in Azure DevOps, you can simply use Microsoft accounts. For additional information, see [Access Azure DevOps with Azure Active Directory \(Azure AD\)](#).

For on-premises deployments, AD is recommended when managing a large group of users. For additional information, see [Set up groups for use in on-premises deployments](#).

Authentication methods, integrating with other services and apps

Other applications and services can integrate with Azure DevOps services and resources. To access your account without asking for user credentials multiple times, apps can use these authentication methods:

- [Alternate credentials](#) as a single set of credentials across all tools that don't have plug-in, extension, or native support. For example, you can use basic authentication to access [REST APIs for Azure DevOps](#), but you must turn on alternate credentials.
- [Personal access tokens](#) to generate tokens for:
 - Accessing specific resources or activities, like builds or work items

- Clients like Xcode and Nuget that require usernames and passwords as basic credentials and don't support Microsoft account and Azure Active Directory features like multi-factor authentication
- Accessing [Azure DevOps REST APIs](#)
- [OAuth](#) to generate tokens for accessing [REST APIs](#). The [Accounts](#) and [Profiles](#) APIs support only OAuth.
- [SSH authentication](#) to generate encryption keys when you use Linux, macOS, or Windows running [Git for Windows](#) and can't use [Git credential managers](#) or [personal access tokens](#) for HTTPS authentication.

By default, your account or collection allows access for all authentication methods. You can limit access, but you must specifically restrict access for each method. When you deny access to an authentication method, no app can use that method to access your account. Any app that previously had access gets an authentication error and can't access your account.

To learn more about how we store your credentials, see [Credential storage for Azure DevOps](#).

To learn more about how to choose the right authentication mechanism, see [Guidance for authentication](#).

Authorization

Authorization verifies that the identity which is attempting to connect has the necessary permissions to access a service, feature, function, object, or method.

Authorization always occurs after successful authentication. If a connection is not authenticated, it fails before any authorization checking is performed. If authentication of a connection succeeds, a specific action might still be disallowed because the user or group did not have authorization to perform that action.

Authorization is based on users and groups, and the permissions assigned directly to both those users and groups and permissions those users and groups might inherit by belonging to one or more Azure DevOps security groups. These users and groups can be Azure AD or AD users and groups. For on-premises deployments, they can also be local Windows users and groups.

Also, for select features, users and groups may need to belong to an access level that grants them access to a feature.

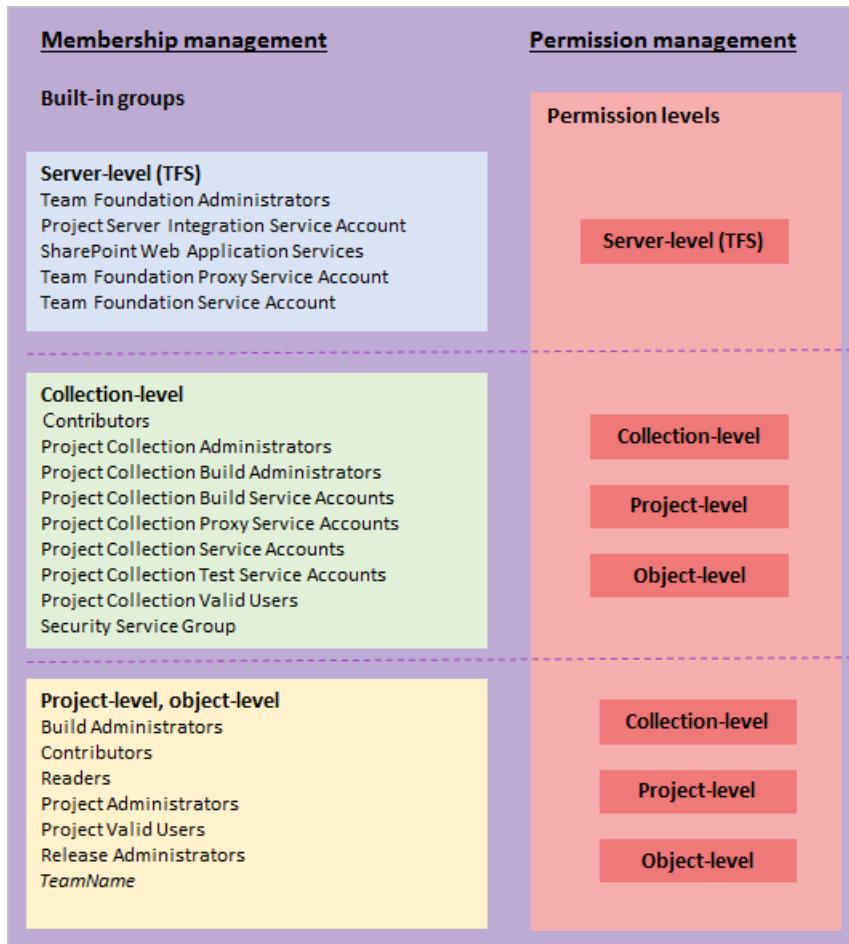
Security groups and permissions

Azure DevOps is pre-configured with default security groups. Default permissions are assigned to the default security groups.

SECURITY AREA	GROUPS, LEVELS, AND STATES
Security groups	<ul style="list-style-type: none"> ● Project-level ● Organization or collection level ● Server-level (Azure DevOps Server and TFS only)
Permission levels	<ul style="list-style-type: none"> ● Object-level ● Project-level ● Organization or collection level ● Server-level (Azure DevOps Server and TFS only)

<p>Permission states</p>	<p>User or group has permissions to perform a task:</p> <ul style="list-style-type: none"> • Allow • Inherited allow <p>User or group doesn't have permission to perform a task:</p> <ul style="list-style-type: none"> • Deny • Inherited deny • Not set
--------------------------	---

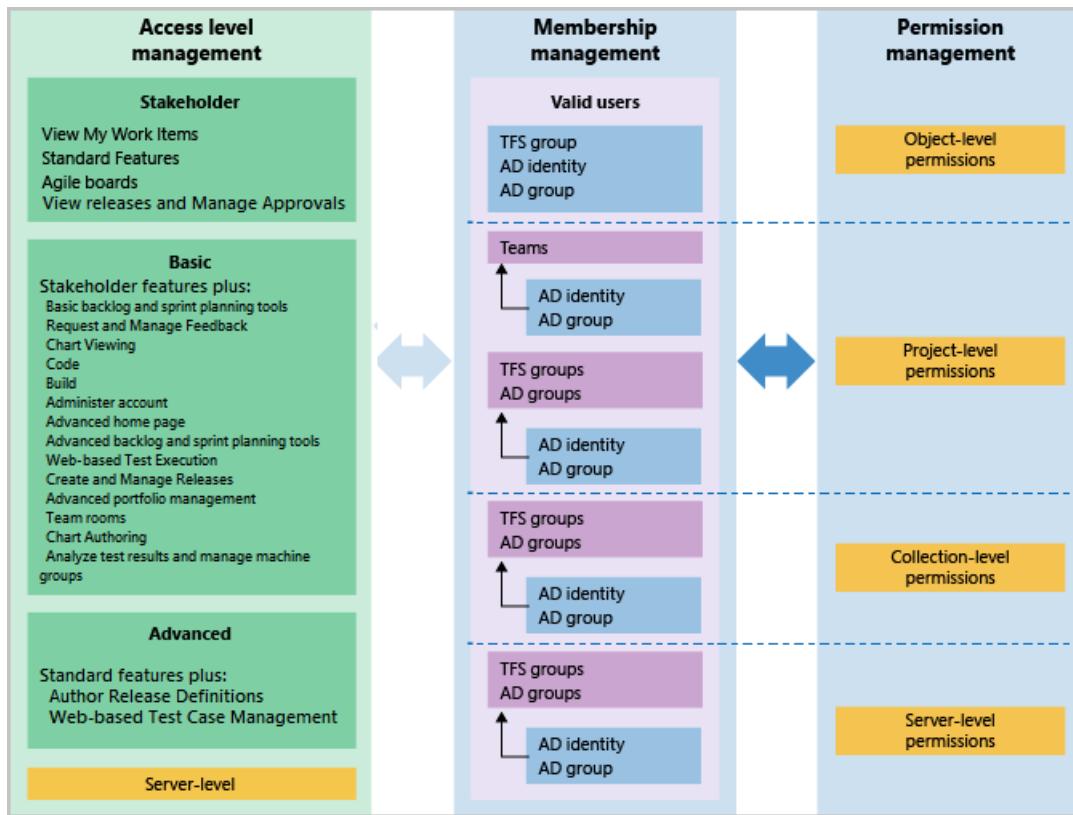
You can populate these groups by using individual users. However, for ease of management, it's easier if you populate these groups by using Azure AD or AD security groups. This method enables you to manage group membership and permissions more efficiently across multiple computers.



Azure DevOps controls access through these three inter-connected functional areas:

- **Membership management** supports adding individual Windows user accounts and groups to default security groups. Also, you can create Azure DevOps security groups. Each default group is associated with a set of default permissions. All users added to any security group are added to the Valid Users group. A valid user is someone who can connect to the project.
- **Permission management** controls access to specific functional tasks at different levels of the system. Object-level permissions set permissions on a file, folder, build pipeline, or a shared query. Permission settings correspond to **Allow**, **Deny**, **Inherited allow**, **Inherited deny**, and **Not set**. To learn more about inheritance, see [About permissions and groups](#).
- **Access level management** controls access to features provided via the web portal, the web application for Azure DevOps. Based on what has been purchased for a user, administrators set the user's access level to Basic, VS Enterprise (previously Advanced), or Stakeholder.

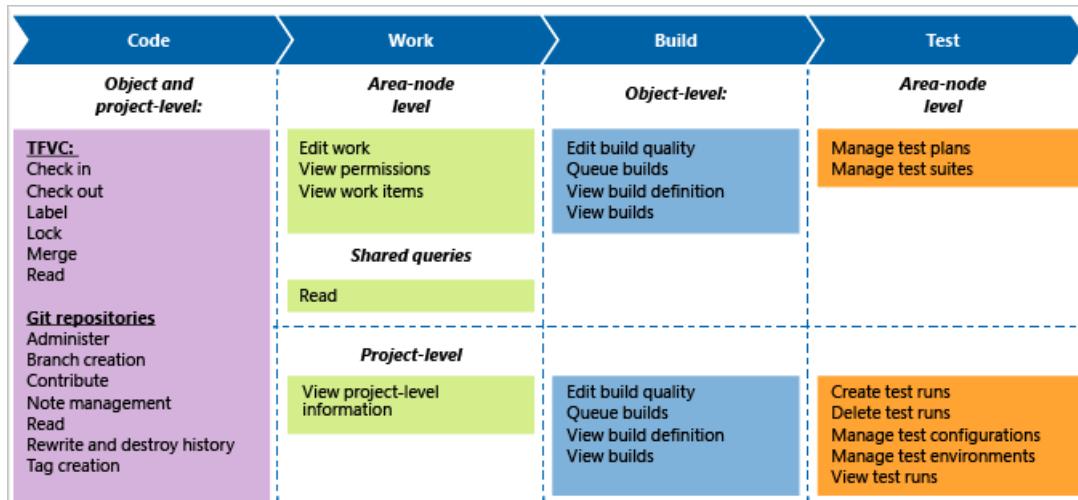
Each functional area uses groups to simplify management across the deployment. You add users and groups through the web administration context. Permissions are automatically set based on the security group that you add users to, or based on the object, project, collection, or server level to which you add groups. On the other hand, access level management controls access for all users and groups at the server level.



You can create local groups or Active Directory (AD) [groups to manage your users](#). If you decide to use groups, make sure that membership in those groups is limited to valid users. Because group membership can be altered by their owners at any time, if those owners did not consider Azure DevOps Server access when they created those groups, their changes to membership can cause unwanted side effects within the server.

Default permissions set for the Contributors group

The following image shows the default permission assignments made to the Contributors group.



To learn more about other groups and their permission assignments, see [Permissions and groups reference](#).

Security roles

There are a number of artifacts whose permissions are managed by role. These include the following artifacts and features.

SECURITY LEVEL	FUNCTIONAL AREA
Object-level	<ul style="list-style-type: none"> Deployment groups Secure files Variable groups
Project-level	<ul style="list-style-type: none"> Agent queues Service connections Team administration
Collection-level	<ul style="list-style-type: none"> Agent pools Deployment pools Marketplace extensions

To learn more, see [About security roles](#).

Access levels

Certain features are only available to users who have the appropriate licensing level for those features. Access to those features is not controlled by permissions but by membership in an access level. To learn more, see [Access levels](#).

Related articles

- [Permissions and groups reference](#)
- [Default permissions and access for Azure DevOps](#)
- [Access with Azure Active Directory \(Azure AD\)](#)
- [Set up groups for use in on-premises deployments](#)
- [Setting up HTTPS with Secure Sockets Layer \(SSL\)](#)

View permissions for yourself or others

6/13/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

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

Permissions are set at the collection, project, and object level as described in [About permissions and groups](#). So to view the permissions you have, you need to open the permissions at the object, project, or collection level.

Prerequisites

- You must have a project to connect to. If you don't have a project yet, [create one](#).
- You must be a member of the Project Valid Users Group or Project Collection Valid Users Group to view permissions.

NOTE

This article shows how to view permissions assigned to a user at the project-level or collection-level. However, the steps are similar when you work from the Security dialog of an object.

View project-level permissions

1. Choose **Project Settings** and then **Security**.

To see the full image, click to expand.

The screenshot shows the 'Project Settings' page for the 'Fabrikam Fiber' project. On the left, there's a sidebar with various project management tabs: Overview, Work, Code, Build and release, and Packages. Below these is the 'Project settings' button, which is highlighted with a red box and the number '1'. In the main content area, the 'Security' tab is selected, indicated by a red box and the number '2'. The 'General' section contains links for Overview, Services, Teams, Notifications, Service hooks, and Dashboards. Under the 'Teams' section, a 'Create group' dialog is open, showing a list of existing teams: Customer Service, Email, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. There's also a section for 'Azure DevOps Groups' with options like Build Administrators, Contributors, Deployment Group Administrators, Disallow access group, Endpoint Administrators, Endpoint Creators, Project Administrators, Project Collection Valid Users, and Security Service Group.

2. Begin entering the name into the *Filter users and groups* box. The system automatically shows the names that begin with the characters you enter.

This screenshot shows the 'Create group' dialog with the search term 'Jamal' entered into the 'Filter users and groups' input field. The search results list one item: 'Jamal Hartnett' (fabrikamfiber4@hotmail.com). The 'Showing 1 result' message is highlighted with a red box. To the right, a list of permissions is shown for the 'Customer Service' team, including 'Members' and 'Member of' sections, and specific permissions for work item updates, process change, tag definition, test runs, and work item deletion.

Permission	Setting
Members	Not set
Member of	Not set
Change process of team project.	Not set
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set

3. Choose the name you want. The project-level permissions you have set are based on the groups you belong to or the permissions set for your account.

Create group

Jamal



Jamal Hartnett

fabrikam > Jamal Hartnett | Edit... ▾



Permissions Member of

Bypass rules on work item updates	Not set
Change process of team project.	Not set
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set
Delete shared Analytics views	Allow (inherited)
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Edit shared Analytics views	Allow (inherited)
Manage project properties	Not set
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Not set
Permanently delete work items	Not set
Rename team project	Not set
Suppress notifications for work item updates	Not set
Update project visibility	Not set
View analytics	Allow (inherited)
View project-level information	Allow (inherited)
View test runs	Allow (inherited)

[Clear explicit permissions](#)

[Save changes](#) [Undo changes](#)

- Choose **Member of** to see which security groups the user belongs to.

Here we see that *Jamal Hartnett* belongs to several teams and the Project Collection Administrators group.

Create group

Jamal



Jamal Hartnett

fabrikam > Jamal Hartnett | Edit... ▾



Permissions **Member of**

[+ Add...](#) | [⟳](#) | [Search](#)

Display Name	Username Or Scope
 Customer Service	[Fabrikam Fiber]
 Fabrikam Fiber Team	[Fabrikam Fiber]
 Web	[Fabrikam Fiber]
 Project Collection Administrators	[fabrikam]
 Project Administrators	[MyFirstProject]

- Open **Project Settings**. Choose the gear settings icon, and choose **Security**.

The screenshot shows the Microsoft Teams navigation bar. The 'Security' tab is highlighted with a red box. Other tabs visible include Overview, Work, Version Control, Policies, Agent queues, Notifications, and Service Hooks.

2. Begin entering the name into the *Filter users and groups* box. The system automatically shows the names that begin with the characters you enter.

The screenshot shows the 'Create group' dialog. A red box highlights the search results for 'Jam'. The results list 'Jamal Hartnett' with a small profile icon and the email 'fabrikamfiber4@hotmail.com'. Below the list, it says 'Showing 1 result'. To the right, the 'Permissions' section for 'Customer Service' is shown, listing various permissions with their current status (e.g., Allow (inherited), Not set).

Permission	Status
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Manage project properties	Not set

3. Choose the name you want. The project-level permissions you have set are based on the groups you belong to or the permissions set for your account.

The screenshot shows the 'Create group' dialog with 'Jamal' entered in the search box. The results list 'Jamal Hartnett' with a small profile icon. To the right, the 'Permissions' section for 'Jamal Hartnett' is shown, listing various permissions with their current status.

Permission	Status
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Manage project properties	Not set
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Not set
Permanently delete work items	Not set
Rename team project	Not set
View project-level information	Allow (inherited)
View test runs	Allow (inherited)

For a description of each permission, see [Permissions and groups reference](#).

4. Choose **Member of** to see which security groups the user belongs to.

Here we see that *Jamal Hartnett* belongs to several teams and the Project Collection Administrators group.

The screenshot shows the 'Member of' tab selected for the user 'Jamal'. The table lists the groups he belongs to:

Display Name	Username Or Scope	
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Project Collection Administrators	[fabrikam]	

For a description of each group, see [Permissions and groups reference](#).

View organization or collection-level permissions

Open admin settings for the organization or a project collection.

1. Choose the to open **Projects**. Then choose **Admin settings**.



2. Choose **Security**, the **Project Collection Administrators** group, and then **Members**.

The screenshot shows the 'Members' tab selected for the 'Project Collection Administrators' group. The table lists the members:

Display Name	Username Or Scope
Christie Church	fabrikamfiber1@hotmail.com
Jamal Hartnett	fabrikamfiber4@hotmail.com
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com

3. Follow steps 2 through 4 in the procedure outlined previously for view project-level permissions.

1. Choose the and select **Organization settings** or **Collection settings**.



2. Choose **Security**, **Project Collection Administrators** group, and then **Members**.

The screenshot shows the Azure DevOps interface. At the top, there's a navigation bar with 'fabrikam' and dropdown menus for 'Projects', 'My favorites', 'My work items', 'My pull requests', and '...'. On the far right is a gear icon. Below the navigation is a secondary menu with 'Overview', 'Settings', 'Security' (which is highlighted with a red box), 'Users', 'Process', 'Build and Release', 'Agent Pools', and 'Notifications'. A 'Create group' button is also present. To the left, a sidebar lists 'Azure DevOps Groups' with 'Project Collection Administrators' selected (also highlighted with a red box). The main content area shows the 'Members' tab for 'Project Collection Administrators'. It includes a header with 'Permissions', 'Members' (highlighted with a red box), and 'Member of'. Below is a table with columns 'Display Name' and 'Username Or Scope'. The table lists three users: 'Project Collection Service ...' (username obscured), 'Christie Church' (fabrikamfiber1@hotmail.com), 'Jamal Hartnett' (fabrikamfiber4@hotmail.com), and 'Raisa Pokrovskaya' (fabrikamfiber5@hotmail.com). There are buttons for '+ Add...', 'Edit', and 'Search'.

3. Follow steps 2 through 4 in the procedure outlined previously for view project-level permissions.

View object-level permissions

You can define the security or permissions for a number of objects. You access them from the context menu of the object.

From the web portal, open the Security dialog for the object whose permissions you want to set. For specific instructions, see the following articles:

AREA	TASK
Wiki & Dashboard permissions	<ul style="list-style-type: none">README & WikiDashboards
DevOps (code, build, test, release) permissions	<ul style="list-style-type: none">Git branchGit repositoryTFVCBuildsRelease pipeline securityApprovals and approvers
Work tracking permissions	<ul style="list-style-type: none">Area and iteration pathsWork item query and folderPlan permissions

Next steps

[Look up the organization owner or a project administrator](#)

Look up administrators and organization owner

Look up administrators

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

When you need to have your permissions changed or you need to get access to select features or functions, you may need to find out who can grant them. Usually it is an administrator or the account owner.

For an overview of built-in security groups and default permission assignments, see [Default permissions and access](#).

Prerequisites

- You must have a project. If you don't have a project yet, [create one](#).
- You must be a member of the Project Valid Users Group or Project Collection Valid Users Group to view permissions.

Show members of the Project Administrators group

If you aren't a project administrator, and you need to be, find someone who is, and have them add you. You can find who is a member of the Project Administrators group by choosing that group from the **Project Settings>Security** page and seeing who are members.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose **Project Settings** and then **Security**.

To see the full image, click to expand.

The screenshot shows the 'Project Settings' page for the 'Fabrikam Fiber' project. On the left, there's a sidebar with icons for Overview, Work, Code, Build and release, and Packages. Below the sidebar is a 'Project settings' button, which is highlighted with a red box and a red circle containing the number '1'. The main area is titled 'Project Settings' and has a 'General' section expanded. Under 'General', there are links for Overview, Services, Teams, Security (which is highlighted with a red box and a red circle containing the number '2'), Notifications, Service hooks, and Dashboards. To the right of the 'General' section is a 'Create group' panel. This panel includes a 'Filter users and groups' input field and a 'Teams' section containing a list of groups: Customer Service, Email, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. Below the 'Teams' section is another section for 'Azure DevOps Groups' with a list of groups: Build Administrators, Contributors, Deployment Group Administrators, Disallow access group, Endpoint Administrators, Endpoint Creators, Project Administrators, Project Collection Valid Users, and Security Service Group.

3. Choose the **Members** tab.

The screenshot shows the 'Create group' page for the 'Project Administrators' group under the 'Fabrikam Fiber' project. The 'Members' tab is selected and highlighted with a red box. The page displays a table with columns for 'Display Name', 'Username Or Scope', and 'Remove'. There are three entries: Christie Church (fabrikamfiber1@hotmail.com), Jamal Hartnett (fabrikamfiber4@hotmail.com), and Raisa Pokrovskaya (fabrikamfiber5@hotmail.com). To the left of the table is a sidebar with sections for 'Teams' and 'Azure DevOps Groups'. Under 'Teams', there are links for Customer Service, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. Under 'Azure DevOps Groups', there are links for Build Administrators, Contributors, and Project Administrators (which is highlighted with a red box). At the bottom of the sidebar is a link for Project Valid Users.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open **Project Settings**.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. The 'Files' tab is selected. In the top right corner, there is a gear icon. A red arrow points from this icon to the 'Project settings' option in a dropdown menu that appears when the gear icon is clicked. The dropdown menu also includes other options like 'Overview', 'Work', 'Security', 'Version Control', 'Policies', 'Agent Queues', 'Notifications', 'Service Hooks', 'Services', 'Test', 'Release', 'Dashboards', and 'Organization settings'.

3. Choose the **Security** page, **Project Administrators** group, and the **Members** tab.

The screenshot shows the 'Create group' interface in Azure DevOps. On the left, there is a sidebar with a 'Create group' button at the top, followed by a 'Filter users and groups' input field. Below that are sections for 'Teams' and 'Azure DevOps Groups'. Under 'Teams', several groups are listed: Customer Service, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. Under 'Azure DevOps Groups', Build Administrators, Contributors, and Project Administrators are listed. The 'Project Administrators' group is highlighted with a red box. On the right, the main area shows the 'Fabrikam Fiber > Project Administrators' page. It has tabs for 'Permissions', 'Members' (which is selected and highlighted with a red box), and 'Member of'. Below the tabs is a control bar with '+ Add...', a refresh icon, and a 'Search' input field. The 'Members' table lists three users:

Display Name	Username Or Scope	Action
Christie Church	fabrikamfiber1@hotmail.com	Remove
Jamal Hartnett	fabrikamfiber4@hotmail.com	
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

Show members of the Project Collection Administrators group

If you need elevated permissions, you'll have to request them from a member of the [Project Collection Administrators group](#). Project collection administrators manage features and functions that impact all projects.

To find out who is a member, check the **Security** settings at the collection level.

1. Choose the Azure DevOps logo to open **Projects**. Then choose **Admin settings**.



2. Choose **Security**, the **Project Collection Administrators** group, and then **Members**.

The screenshot shows the 'Create group' page for 'Project Collection Administrators'. On the left, there's a sidebar with 'Create group' and 'Filter users and groups' options. Below that is a list of 'Azure DevOps Groups' under 'Project Collection Administrators', which is highlighted with a red box. Other groups listed include 'Project Collection Build Administrators', 'Project Collection Build Service Accounts', 'Project Collection Proxy Service Accounts', 'Project Collection Service Accounts', 'Project Collection Test Service Accounts', 'Project Collection Valid Users', and 'Security Service Group'. On the right, the 'fabrikam > Project Collection Administrators' page is shown with tabs for 'Permissions', 'Members' (which is selected and highlighted with a red box), and 'Member of'. It includes buttons for '+ Add...', 'Search', and a refresh icon. The table lists members with columns for 'Display Name', 'Username Or Scope', and profile icons. Members listed are 'Project Collection Service ...' (username obscured), 'Christie Church' (fabrikamfiber1@hotmail.com), 'Jamal Hartnett' (fabrikamfiber4@hotmail.com), and 'Raisa Pokrovskaya' (fabrikamfiber5@hotmail.com).

1. Choose the settings icon and select **Organization settings** or **Collection settings**.



2. Choose **Security**, **Project Collection Administrators** group, and then **Members**.

The screenshot shows the 'Security' tab for 'Project Collection Administrators'. At the top, there's a navigation bar with 'fabrikam', 'Projects', 'My favorites', 'My work items', 'My pull requests', '...', and a gear icon (Admin settings) which is highlighted with a red box. Below the navigation bar is the 'Create group' section with 'Filter users and groups' and a list of 'Azure DevOps Groups' including 'Project Collection Administrators' (highlighted with a red box). On the right, the 'fabrikam > Project Collection Administrators' page is shown with tabs for 'Permissions', 'Members' (selected and highlighted with a red box), and 'Member of'. It includes buttons for '+ Add...', 'Search', and a refresh icon. The table lists members with columns for 'Display Name', 'Username Or Scope', and profile icons. Members listed are 'Project Collection Service ...' (username obscured), 'Christie Church' (fabrikamfiber1@hotmail.com), 'Jamal Hartnett' (fabrikamfiber4@hotmail.com), and 'Raisa Pokrovskaya' (fabrikamfiber5@hotmail.com).

Show who is the organization owner

1. Choose the Azure DevOps logo to open **Projects**. Then choose **Admin settings**.



2. Choose **Overview** to find the current owner.

Organization settings

Organization information

Organization URL

<https://.visualstudio.com/> 

This organization is not backed by Azure Active Directory. [Learn more](#)

Organization owner

 Jamal Hartnett



Time zone

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



Region

North Central US

Description

To change the owner, see [Change organization owner](#).

Try this next

[Add users to a project or team](#)

Add users to a project or team

6/13/2019 • 7 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

In this quickstart, you learn how to add users to a project or specific team. For anyone to access a project, they must be added to one of the default security groups or a custom group. Usually you add them to the Contributors group. For a quick look at what permissions are assigned to the default groups, see [Permissions and access](#).

The easiest way to add a number of users to a project is to add groups defined in [Azure Active Directory \(Azure AD\)](#) or [Active Directory \(AD\)](#).

IMPORTANT

If you're adding users to an organization in Azure DevOps and you don't use Azure AD, then you need to [add their "personal" Microsoft accounts to your account or project](#). After you've added them to one project, you can add them to additional projects using the procedures provided in this article.

Once users have been added to a project, you can browse for their display name or user name (email alias). Also, you can [add them to a specific team](#). To add a team, see [Add a team](#).

Prerequisites

- You must have a project. If you don't have a project yet, [create one](#).
- To add users to a project, you must be a member of the [Project Administrators group](#) or have your [Edit project-level information](#) set to Allow. You can add Stakeholders to the Project Administrators group and then they can add users to an organization or project.
- To add users to a team, you must be [added as a team administrator](#), or you must be a member of the Project Administrators Group, or have your [Edit project-level information](#) set to Allow.

Add users to a project

If you are adding a user to Azure DevOps for the first time, see [Add account users for Azure DevOps](#).

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose **Project Settings** and then **Security**.

To see the full image, click to expand.

The screenshot shows the 'Project Settings' page for the 'Fabrikam Fiber' project. On the left, there's a navigation bar with icons for Overview, Work, Code, Build and release, Packages, and Project settings. The 'Project settings' icon has a red box around it and a red circle with the number '1' over it. The main area is titled 'Project Settings' and contains a 'General' section with links to Overview, Services, Teams, Notifications, Service hooks, Dashboards, Boards, Build and release, Code, Test, and Extensions. The 'Security' tab is highlighted with a red box and a red circle with the number '2' over it. To the right of the tabs is a 'Create group' button and a 'Filter users and groups' input field. Below these are sections for 'Teams' (Customer Service, Email, Fabrikam Fiber Team, Management team, Phone, Voice, Web) and 'Azure DevOps Groups' (Build Administrators, Contributors, Deployment Group Administrators, Disallow access group, Endpoint Administrators, Endpoint Creators, Project Administrators, Project Collection Valid Users, Security Service Group).

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

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

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

Here we choose the **Contributors** group.

Fabrikam Fiber > Contributors | Edit... ▾

Permissions Members Member of

+ Add... | Refresh | Search

Display Name	Username Or Scope	
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Management team	[Fabrikam Fiber]	
Phone	[Fabrikam Fiber]	
Voice	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Jia-hao Tseng	fabrikamfiber9@hotmail.com	

Teams

- Customer Service
- Fabrikam Fiber Team
- Management team
- Phone
- Voice
- Web

Azure DevOps Groups

- Build Administrators
- Contributors
- Project Administrators
- Project Valid Users
- Readers

By default, the default team group and any other teams you add to the project, are 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.
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 meet your requirements.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

Chris

Christie Church
fabrikamfiber1@hotmail.com

Showing 1 result

Save changes Cancel

NOTE

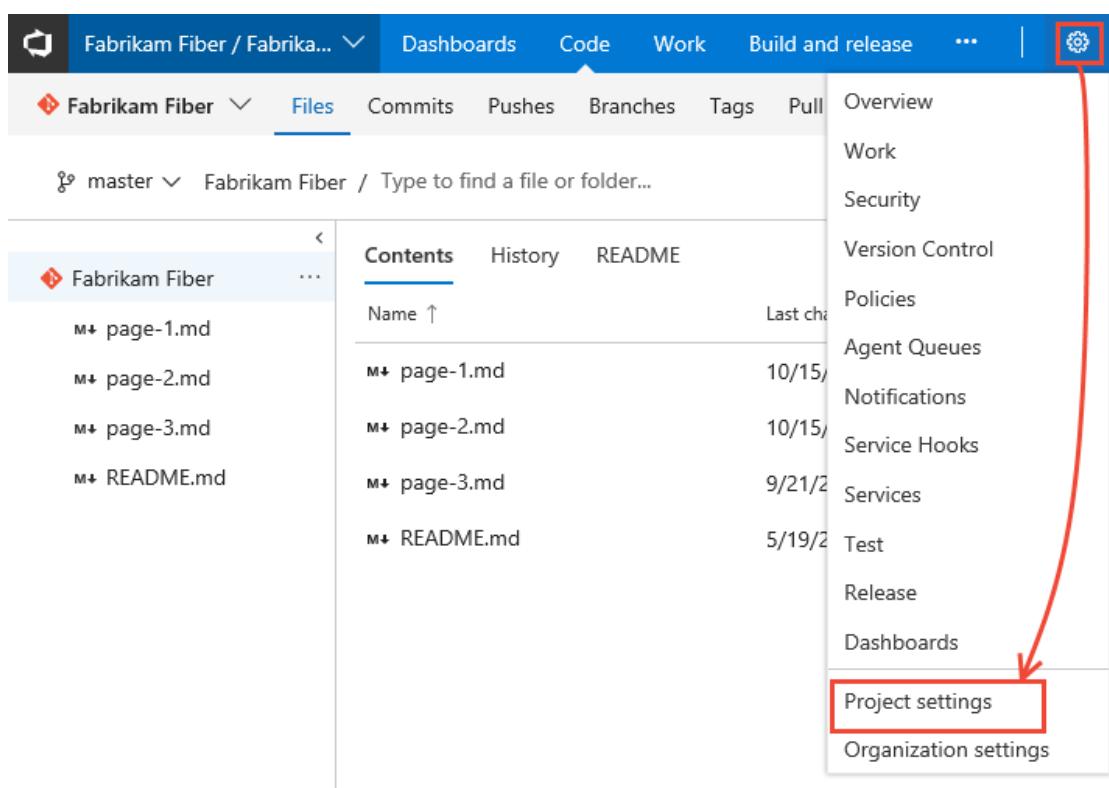
The first time you add a user or group to Azure DevOps, you can't browse to it or check the friendly name. After the identity has been added, you can just enter the friendly name.

7. In **Identities**, specify the name of the user or group you want to add.
8. Depending on the user, you may customize their permissions for other functionality in the project. For example, in [areas and iterations](#) or [shared queries](#).

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open the administrative context.



3. Choose **Security** and under **Groups**, choose one of the following options:
 - To add users who require read-only access to the project, choose **Readers**.
 - To add users who contribute fully to this project, choose **Contributors**.
 - For users who need to administrate the project, choose **Project Administrators**. To learn more, see [Set permissions at the project-level or project collection-level](#).
4. Next, choose the **Members** tab.

Here we choose the Contributors group.

Fabrikam Fiber > Contributors | Edit... ▾

Permissions Members Member of

+ Add... | Refresh | Search

Display Name	Username Or Scope	
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Management team	[Fabrikam Fiber]	
Phone	[Fabrikam Fiber]	
Voice	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Jia-hao Tseng	fabrikamfiber9@hotmail.com	

Teams

- Customer Service
- Fabrikam Fiber Team
- Management team
- Phone
- Voice
- Web

Azure DevOps Groups

- Build Administrators
- Contributors
- Project Administrators
- Project Valid Users
- Readers

TIP

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

By default, the default team group and any other teams you add to the project, are 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.

- Choose + **Add** to add a user or a user group.
- 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.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

Chris

Christie Church
fabrikamfiber1@hotmail.com

Showing 1 result

Save changes Cancel

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.

7. In **Identities**, specify the name of the user or group you want to add.
8. You may want to customize user permissions for other functionality within the project, such as [areas](#) and [iterations](#) or [shared queries](#).

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

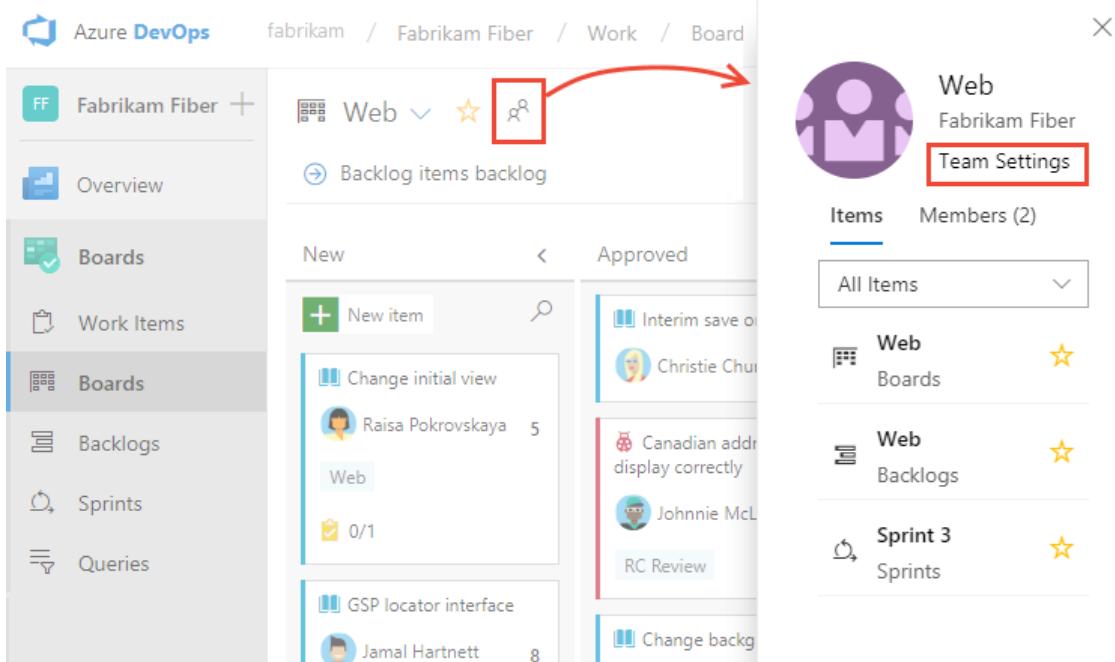
Add users to a team

Several Agile tools, like capacity planning, team alerts, and dashboard widgets are team-scoped. That is, they automatically reference the user accounts added as members of a team to support planning activities or sending alerts. To learn more, see [About teams and Agile tools](#).

You add team members from **Project Settings>Work>Team configuration**. You can quickly navigate to it from a team work tracking backlog, board, or dashboard.

1. Open a backlog or board for a team and choose the  team profile icon. Then choose **Team Settings**.

Here we open the Board for the Web team and from there the team profile.



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

Project Settings > Team configuration > **Web** ▾

- Work
- General Iterations
- Backlogs
- See only the backlog
- Backlog navigation
- Epics
- Features
- Backlog items

Phone (Fabrikam Fiber) ★

Voice (Fabrikam Fiber) ★

Web (Fabrikam Fiber)

Customer Service (Fabrikam Fiber)

Fabrikam Fiber Team (Fabrikam F...)

Management team (Fabrikam Fib...)

More teams

Email (Fabrikam Fiber)

3. Choose **Add**.

Team Profile

Web

Members

+ Add...

Display Name	Username Or Scope	Remove
Jamal Hartnett	fabrikamfiber4@hotmail.com	Remove
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

Name
Web

Description
Enter a description

Administrators
~~Jamal Hartnett~~
~~Raisa Pokrovskaya~~

[+ Add](#)

4. Enter the sign-in addresses or display name for each account you want to add. Add them one at a time or all at the same time. You can enter several identities into the text box, separated by commas.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group: Chris

	Christie Church fabrikamfiber1@hotmail.com	
--	---	--

Showing 1 result

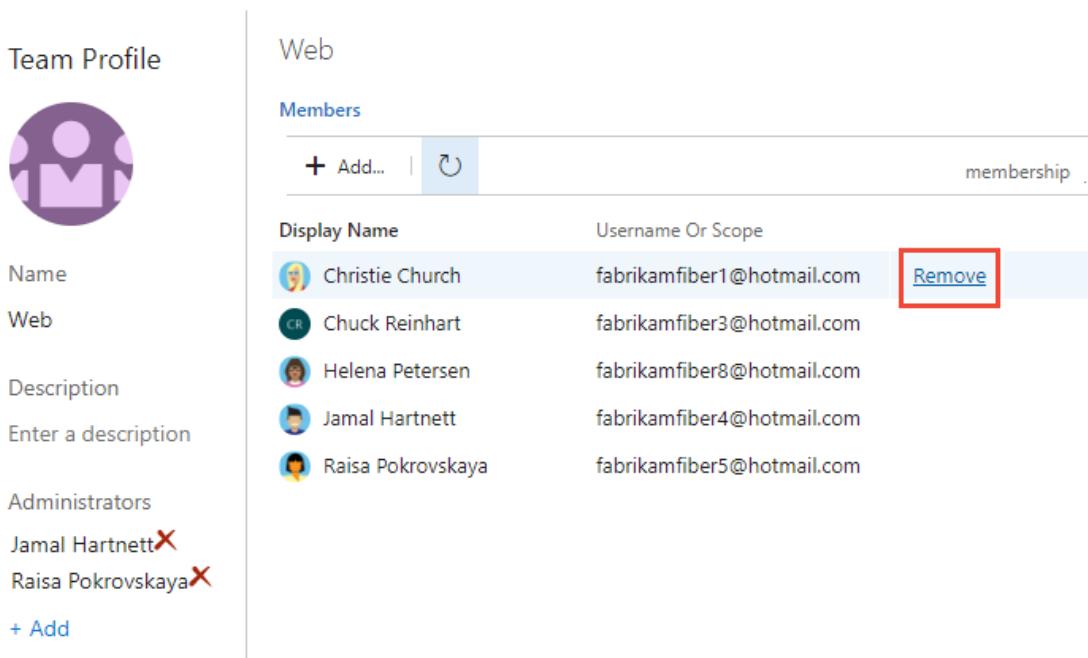
Save changes **Cancel**

TIP

You must enter user and group names one at a time. However, after entering a name, the account is added to the list, and you can enter another name in the Identities text box before choosing to save your changes.

You may need to choose the  refresh icon to see your updates.

5. To remove members, return to this page, highlight the user name and choose **Remove**.

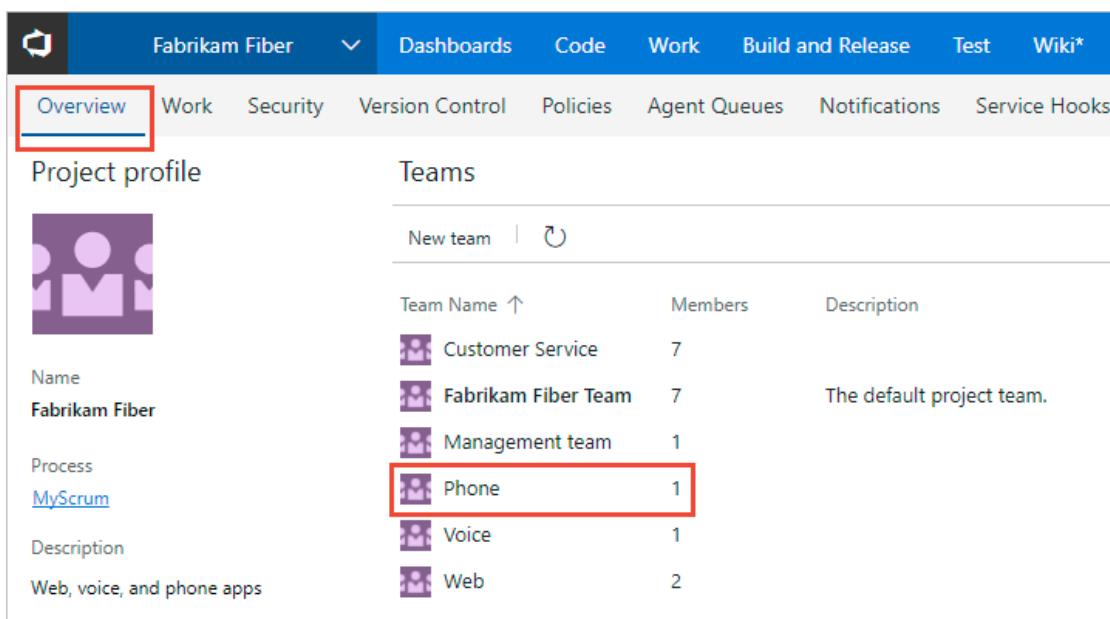


Display Name	Username Or Scope	Action
Christie Church	fabrikamfiber1@hotmail.com	Remove
Chuck Reinhart	fabrikamfiber3@hotmail.com	
Helena Petersen	fabrikamfiber8@hotmail.com	
Jamal Hartnett	fabrikamfiber4@hotmail.com	
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

NOTE

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

6. To add an account as a team administrator, choose **Add** located in the Team Profile page. For details, see [Add a team administrator](#).
1. From the project admin context, open the **Overview** page, and then choose the team you want to add team members to.



Team Name ↑	Members	Description
Customer Service	7	
Fabrikam Fiber Team	7	The default project team.
Management team	1	
Phone	1	
Voice	1	
Web	2	

- Choose the **+ Add** to add a user or a user group.
- Enter the sign-in addresses or display name for each user you want to add. Add them one at a time or all at the same time. You can enter several identities into the text box, separated by commas.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

 Christie Church	fabrikamfiber1@hotmail.com	
---	----------------------------	---

Showing 1 result

Save changes **Cancel**

TIP

You must enter user and group names one at a time. However, after entering a name, it is added to the list, and you can enter another name in the Identities text box before choosing to save your changes.

You may need to choose the  refresh icon to see your updates.

- To remove members, return to this page, highlight the user name, and then choose **Remove**.

Team Profile

Phone

Members

+ Add... | 

Display Name	Username Or Scope	
 Christie Church	fabrikamfiber1@hotmail.com	
 Chuck Reinhart	fabrikamfiber3@hotmail.com	
 Cristina Potra	fabrikamfiber6@hotmail.com	
 Jamal Hartnett	fabrikamfiber4@hotmail.com	
 Johnnie McLeod	fabrikamfiber2@hotmail.com	
 Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

Name
Customer Service
Description
Enter a description
Administrators
Cristina Potra 
+ Add

NOTE

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

- To add an account as a team administrator, choose **Add** located in the Team Profile page. For details, see [Add a team administrator](#).

Add users or groups to an access level

For on-premises deployments, you may need to set the access level for a user or group, particularly if those groups don't belong to the default access level. To learn more, see [Change access levels](#).

Add users or groups to SQL Server Reports

If your on-premises deployment is integrated with SQL Server Reports, you need to manage membership for those products separately from their websites. See [Grant permissions to view or create SQL Server reports in Azure DevOps](#).

Add users or groups to SharePoint or SQL Server Reports

If your on-premises deployment is integrated with a SharePoint product or SQL Server Reports, you need to manage membership for those products separately from their websites.

- [Set SharePoint site permissions](#)
- [Grant permissions to view or create SQL Server reports in Azure DevOps Server](#)

Next steps

[Add administrators or set permissions at the project or collection level](#)

Related articles

- To view permissions for yourself or another user, see [View permissions](#).
- [Set Git or TFVC repository permissions](#)
- [Set Git branch permissions](#)
- [Set build and release permissions](#)
- [Set permissions and access for work tracking](#)

Set repository permissions for Git or TFVC

6/26/2019 • 6 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

By default, members of the project Contributors group have permissions to contribute to a repository. However, to create and manage permissions for a repository, you must be a member of the Project Administrators group. You can grant or restrict access to a repository by setting the permission state to **Allow** or **Deny** for a single user or a security group.

Prerequisites

- You must have a project. If you don't have a project yet, create one in [Azure DevOps](#) or set one up in an [on-premises TFS](#).
- You must be a member of the [Project Administrators Group](#) or have your **Manage permissions** set to **Allow** for Git repositories or the TFVC repository.

Default repository permissions

To contribute to the source code, you must be granted **Basic** access level or greater. Users granted **Stakeholder** access for private projects have no access to source code. Users granted **Stakeholder** access for public projects have the same access as Contributors and those granted **Basic** access. To learn more, see [About access levels](#).

To contribute to the source code, you must be granted **Basic** access level or greater. Users granted **Stakeholder** access have no access to source code. To learn more, see [About access levels](#).

For a description of each security group and permission level, see [Permissions and group reference](#).

Git

You can use Git repositories to host and collaborate on your source code. For an overview of code features and functions, see [Git](#).

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

TASK	READERS	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Clone, fetch, contribute to pull requests, and explore the contents of a repository	✓	✓	✓	✓
Contribute to a repository, create branches, create tags, manage notes		✓	✓	✓
Create, delete, and rename repositories				✓
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)				
--	--	--	--	--

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

By default, the project-level Readers groups have read-only permissions.

TASK	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Branch Creation: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓
Contribute: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓
Note Management: Can push and edit Git notes to the repository. They can also remove notes from items if they have the Force permission.	✓	✓	✓
Tag Creation: Can push tags to the repository, and can also edit or remove tags if they have the Force permission.	✓	✓	✓
Administer: Delete and rename repositories If assigned to the top-level Git repositories entry, can add additional repositories. At the branch level, users can set permissions for the branch and unlock the branch. The Administer permission set on an individual Git repository does not grant the ability to rename or delete the repository. These tasks require Administer permissions at the top-level Git repositories entry.			✓
Rewrite and destroy history (force push): Can force an update to a branch and delete a branch. A force update can overwrite commits added from any user. Users with this permission can modify the commit history of a branch.			✓

The Project Collection Build Service can read from all repositories by default. Any pipeline which runs with project collection scope can potentially read any repository in the organization/collection. You can remove this permission for a repository: set "Read" to "Deny" for the Project Collection Build Service.

TFVC

[Team Foundation Version Control \(TFVC\)](#) provides a centralized version control system to manage your source control.

TASK	READERS	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Contribute to a centralized version control, including Code Review (Check in, label, lock, merge, pend a change)	Read only	✓	✓	✓

Check in, revise, undo, or unlock other users' changes					✓
Manage branches, manage permissions					✓

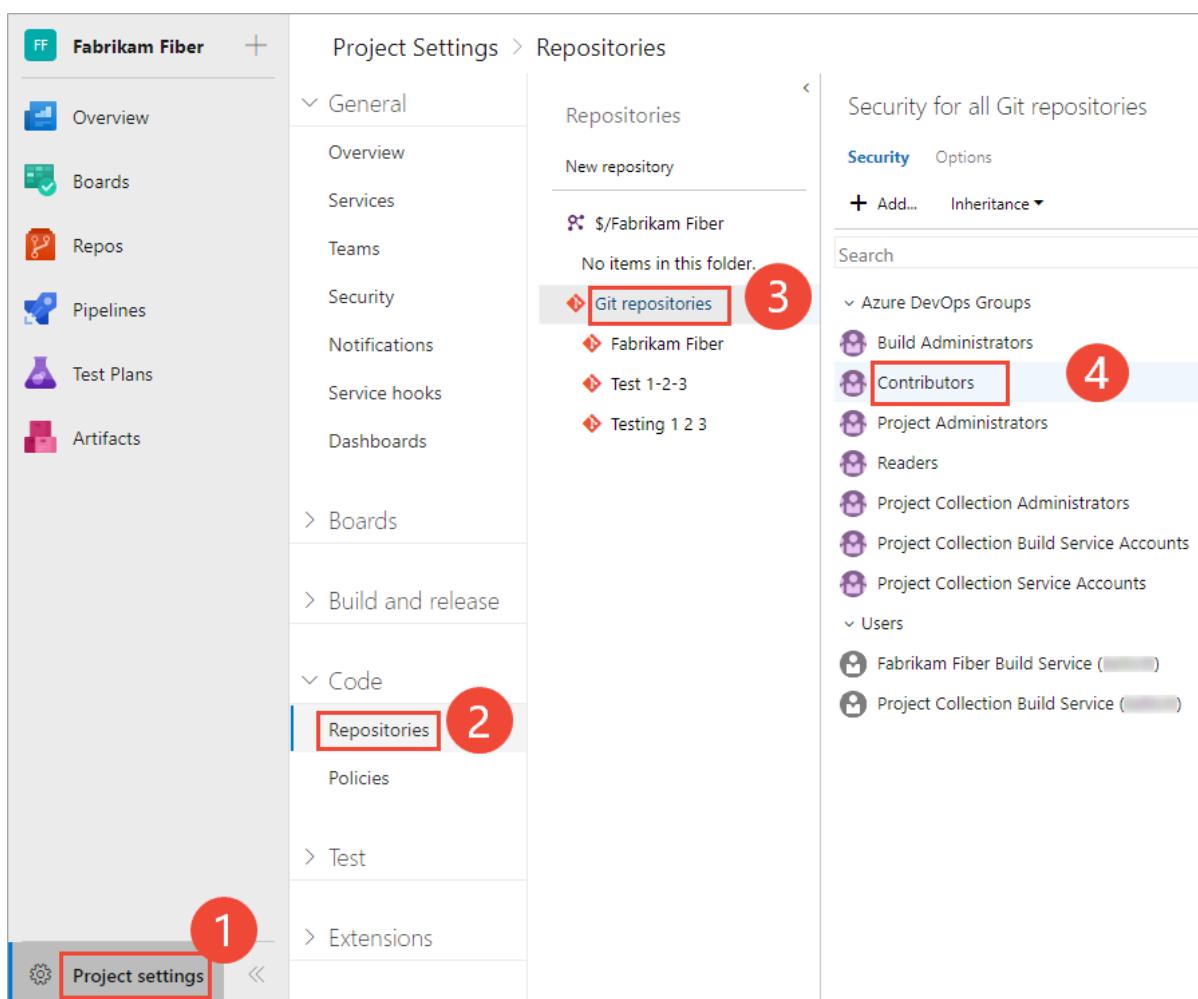
Set Git repository permissions

You can set the permissions for all Git repositories for a project, or for a single repository.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. To set the permissions for all Git repositories for a project, choose **Git Repositories** and then choose the security group whose permissions you want to manage.

For example, here we choose (1) **Project Settings**, (2) **Repositories**, (3) **Git repositories**, (4) the **Contributors** group, and then (5) the permission for **Create repository**.

To see the full image, click to expand.



Otherwise, choose a specific repository and choose the security group whose permissions you want to manage.

NOTE

If you add a user or group, and don't change any permissions for that user or group, then upon refresh of the permissions page, the user or group you added no longer appears.

3. When done, choose **Save changes**.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open the administrative context.

The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber / Fabrika...' project. At the top, there's a navigation bar with 'Dashboards', 'Code', 'Work', 'Build and release', and a three-dot menu. A red box highlights the gear icon in the top right corner of the header. Below the header, a dropdown menu is open, listing various administrative options: Overview, Work, Security, Version Control, Policies, Agent Queues, Notifications, Service Hooks, Services, Test, Release, Dashboards, Project settings (which is highlighted with a red box), and Organization settings. The main content area shows a file list for the 'master' branch of the 'Fabrikam Fiber' repository, containing files like 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md'.

3. Choose **Version Control**.

4. To set the permissions for all Git repositories for a project, (1) choose **Git Repositories** and then (2) choose the security group whose permissions you want to manage.

Otherwise, choose a specific repository and choose the security group whose permissions you want to manage.

5. Choose the setting for the permission you want to change.

Here we grant permissions to the Contributors group to (3) create repositories.

The screenshot shows the 'Version Control' section of the Azure DevOps interface. On the left, under 'Repositories', the 'Git repositories' section is selected (marked with a red box and '1'). A specific repository named 'Contributors' is selected (marked with a red box and '2'). On the right, the 'ACCESS CONTROL SUMMARY' table lists various permissions. The 'Create branch' permission is highlighted with a red box and '3', indicating it is being modified. The 'Allow' button for this permission is also highlighted.

Action	Setting
Contribute	Allow
Create branch	Allow
Create repository	
Create tag	Allow
Delete repository	Not set
Edit policies	Not set
Exempt from policy enforcement	Not set
Force push (rewrite history and delete branches)	Not set
Manage notes	Allow
Manage permissions	Not set
Read	Allow
Remove others' locks	Not set
Rename repository	Not set

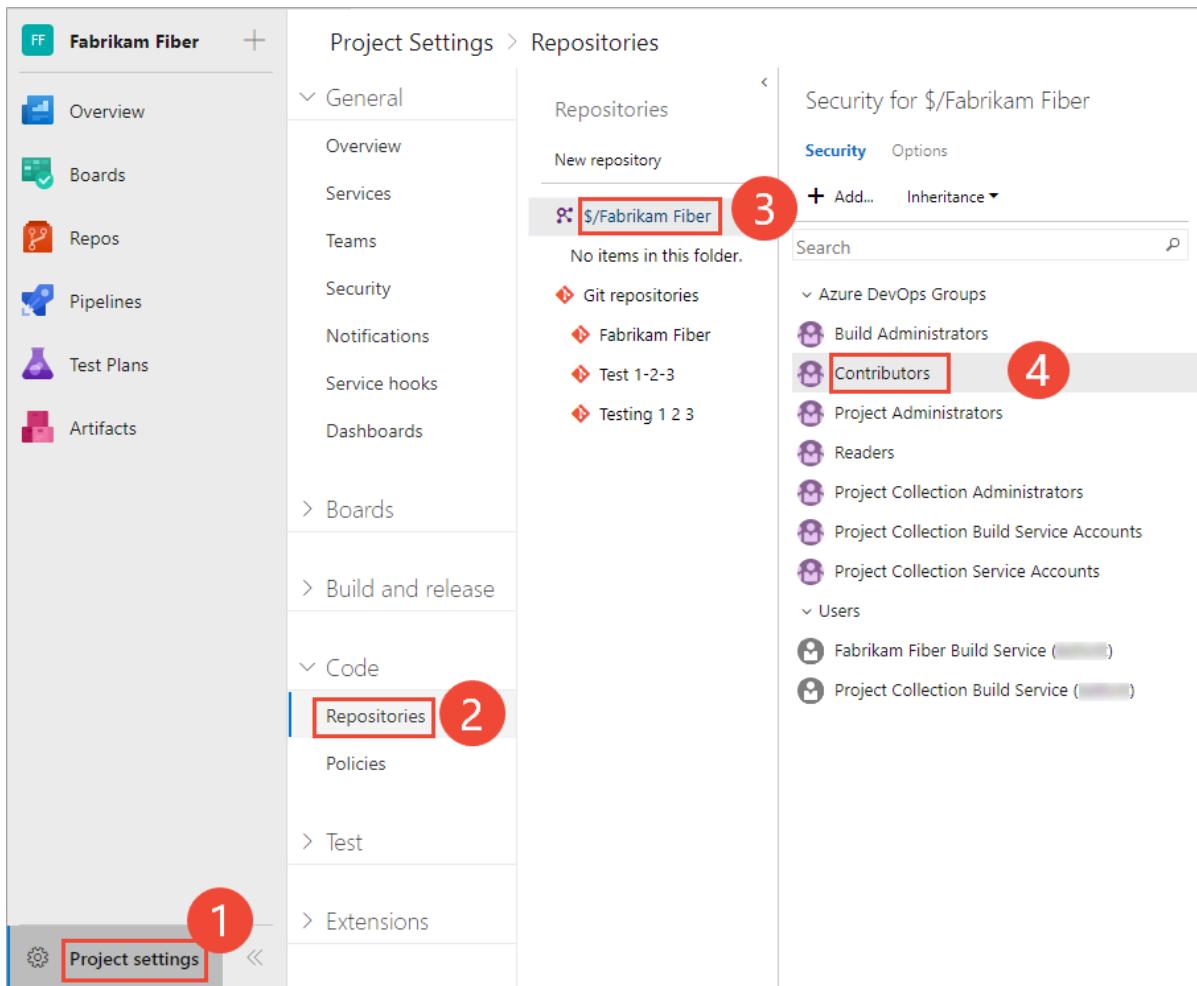
- When done, choose **Save changes**.

Set TFVC repository permissions

- To set the set the permissions for the TFVC repository for a project, choose **TFVC Repository** and then choose the security group whose permissions you want to manage.

For example, here we choose (1) **Project Settings**, (2) **Repositories**, (3) the **TFVC repository**, (4) the **Contributors** group, and then (5) the permission for **Manage branch**.

To see the full image, click to expand.



NOTE

If you add a user or group, and don't change any permissions for that user or group, then upon refresh of the permissions page, the user or group you added no longer appears.

2. Save your changes.

1. From the web portal, open the admin context by choosing the gear Settings icon and choose **Version Control**.
2. Choose the TFVC repository for the project and then choose the security group whose permissions you want to manage.
3. Change the permission setting to **Allow** or **Deny**.

For example, here we change the **Manage branch** permission to Allow for all members of the **Contributors** group.

The screenshot shows the TFS interface for managing version control. On the left, under 'Repositories', the path '\$/Fabrikam Fiber' is selected (marked with a red box and number 1). In the center, the 'Version Control' tab is active, displaying 'Security for \$/Fabrikam Fiber'. The 'Contributors' group is selected (marked with a red box and number 2). On the right, the 'ACCESS CONTROL SUMMARY' table lists various permissions with their current status (e.g., 'Not set', 'Allow'). A red box and number 3 highlights the 'Allow' button for the 'Manage branch' permission.

ACCESS CONTROL SUMMARY	
Administrator labels	Not set
Check in	Allow
Check in other users' changes	Not set
Label	Allow
Lock	Allow
Manage branch	Allow (highlighted with a red box and number 3)
Manage permissions	Not set
Merge	Allow
Pend a change in a server workspace	Allow
Read	Allow
Revise other users' changes	Not set
Undo other users' changes	Not set
Unlock other users' changes	Not set

4. Save your changes.

Related articles

- [Default Git permissions](#)
- [Default TFVC permissions](#)
- [Default permissions and access](#)
- [Permissions and groups reference](#)

Set permissions at the project- or collection-level

6/14/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Several permissions are set at the project or at the organization/project collection level. You can grant these permissions by adding a user or group to one of the default security groups listed here. Or, you can create a custom security group within a level and add members to that group. You can then change the default permission settings.

An organization is the container for several projects that share resources. For more information about projects and project collections, see [Plan your organizational structure](#).

A project collection is the container for several projects that share resources. For more information about projects and project collections, see [About projects and scaling your organization](#).

PROJECT LEVEL	ORGANIZATION/COLLECTION LEVEL
<ul style="list-style-type: none">- Build Administrators- Contributors- Project Administrators- Project Valid Users- Readers- Release Administrators- <i>TeamName</i> Team	<ul style="list-style-type: none">- Project Collection Administrators- Project Collection Build Administrators- Project Collection Build Service Accounts- Project Collection Proxy Service Accounts- Project Collection Service Accounts- Project Collection Test Service Accounts- Project Collection Valid Users- Security Service Group

NOTE

The above list indicates the latest groups defined for Azure DevOps and TFS 2017 and later versions. For earlier versions of TFS, the list may differ. Only add service accounts to [TFS service account groups](#). To understand valid user groups, see [About permissions and groups](#), [Valid user groups](#).

For a description of each group and each permission, see [Permissions and groups reference](#), [Groups](#).

TIP

For users tasked with managing project-level features —such as, teams, area and iteration paths, repositories, service hooks, and service end points—add them to the Project Administrators group. For users tasked with managing organization or collection-level features —such as, projects, policies, processes, retention policies, agent and deployment pools, and extensions—add them to the Project Collection Administrators group. To learn more, see [About user, team, project, and organization-level settings](#).

Prerequisites

- You must be a member of a project. If you don't have a project yet, create one in [Azure DevOps](#). If you haven't been added as a team member, [get added now](#).
- You must be a member of a project. If you don't have a project yet, create one in an [on-premises TFS](#). If you haven't been added as a team member, [get added now](#).
- To manage permissions or groups at the project level, you must be a member of the Project Administrators Group or have your **Edit project-level information** set to Allow. If you created the project, you are automatically added as a member of this group.
- To manage permissions or groups at the collection or instance level, you must be a member of the Project Collection Administrators Group or have your **Edit instance-level information** set to Allow. If you created the organization or collection, you are automatically added as a member of this group.

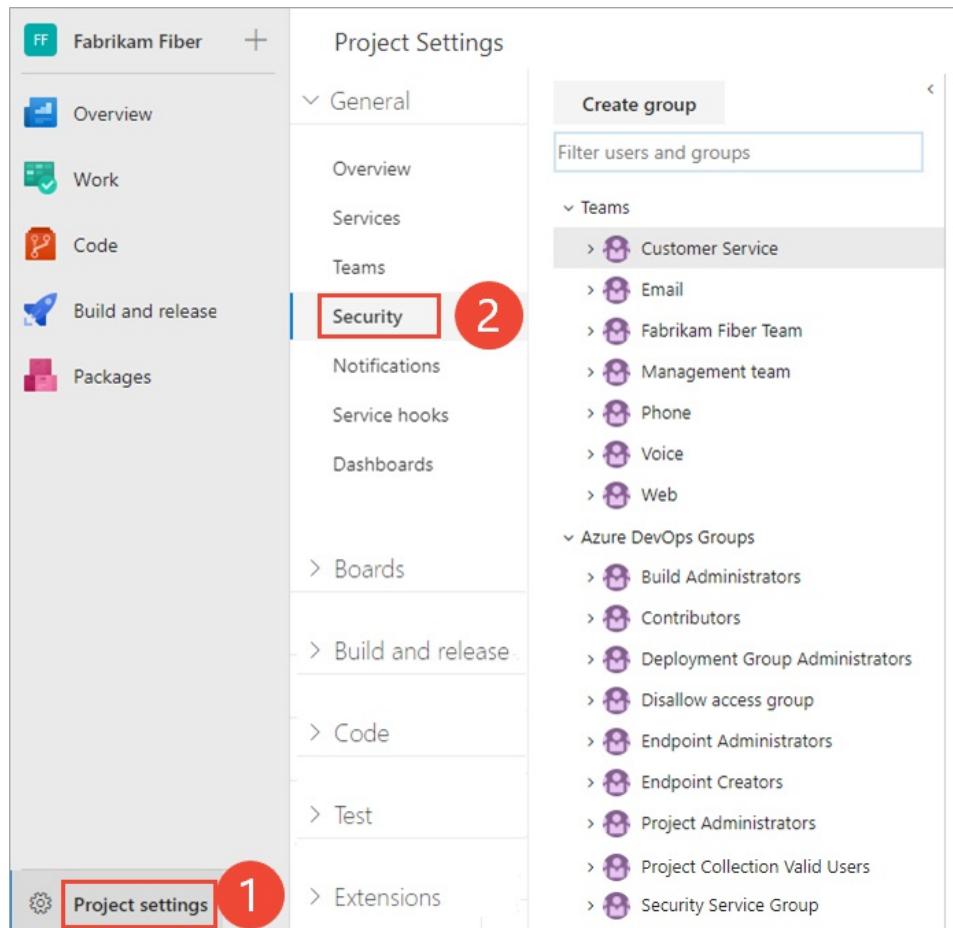
Add a user or group to a security group

As roles and responsibilities change, you might need to change the permission levels for individual members of a project. The easiest way to do that is to add the user or a group of users to a pre-defined security group.

Here we show how to add a user to the built-in Project Administrators group. The method is similar to adding an Azure Active Directory or Active Directory group.

1. Open the web portal and choose the project where you want to add users or groups.
To choose another project, see [Switch project, repository, team](#).
2. Choose **Project Settings** and then **Security**.

To see the full image, click to expand.



3. Choose **Project Administrators** group, **Members**, and then **Add**.

The screenshot shows the 'Create group' interface. On the left, there's a sidebar with sections like 'Teams' and 'Azure DevOps Groups'. Under 'Azure DevOps Groups', 'Project Administrators' is selected and highlighted with a grey background. On the right, the 'Members' tab is active, showing a list of users. Two users are listed: 'Jamal Hartnett' and 'Raisa Pokrovskaya'. Each user has a small profile icon, a display name, a username or scope, and a 'Remove' link. Below the list is a search bar. At the top right, there's an 'Edit...' button.

4. 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 choice.

The screenshot shows the 'Add users and groups' dialog box. In the 'User or group' input field, the text 'Chris' is typed. Below the input field, a search result for 'Christie Church' is displayed, showing her profile picture, name, and email address ('fabrikamfiber1@hotmail.com'). At the bottom of the dialog, there are 'Save changes' and 'Cancel' buttons.

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

5. Choose **Save changes**. Choose the refresh icon to see the additions.
1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open the administrative context.

Fabrikam Fiber / Fabrika... Dashboards Code Work Build and release ...

Fabrikam Fiber Files Commits Pushes Branches Tags Pull Overview

master Fabrikam Fiber / Type to find a file or folder...

Contents History README

Name ↑ Last change

- M+ page-1.md 10/15/2023
- M+ page-2.md 10/15/2023
- M+ page-3.md 9/21/2023
- M+ README.md 5/19/2023

Version Control Policies Agent Queues Notifications Service Hooks Services Test Release Dashboards

Project settings

Organization settings

3. Choose **Security, Project Administrators** group, **Members**, and then **Add**.

Create group

Filter users and groups

Teams

- Customer Service
- Fabrikam Fiber Team
- Management team

Azure DevOps Groups

- Build Administrators
- Contributors
- Disallow access group
- Project Administrators** (highlighted)
- Project Valid Users
- Readers
- Release Administrators
- Team Admins

Permissions Members Member of

+ Add... | Search

Display Name	Username Or Scope	Remove
Jamal Hartnett	fabrikamfiber4@hotmail.com	Remove
Raisa Pokrovskaya	fabrikamfiber5@hotmail.com	

4. 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 choice.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group: Chris

Christie Church	fabrikamfiber1@hotmail.com	
-----------------	----------------------------	--

Showing 1 result

Save changes Cancel

NOTE

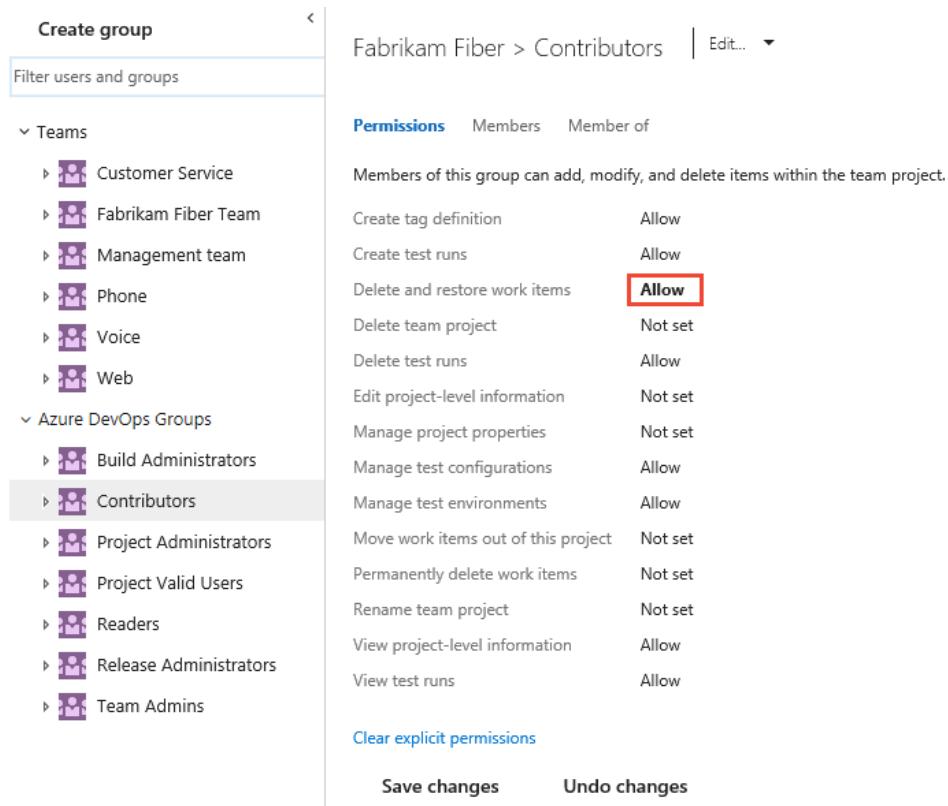
Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

5. Choose **Save changes**. Choose the  refresh icon to see the additions.

Change the permission level for a project-level group

1. From the **Security** page, choose the group whose permissions you want to change.

For example, here we grant permission to the Contributors group to delete and restore work items.



The screenshot shows the 'Create group' interface. On the left, there's a sidebar with a tree view of 'Teams' and 'Azure DevOps Groups'. Under 'Teams', 'Customer Service', 'Fabrikam Fiber Team', 'Management team', 'Phone', 'Voice', and 'Web' are listed. Under 'Azure DevOps Groups', 'Build Administrators', 'Contributors' (which is selected and highlighted in grey), 'Project Administrators', 'Project Valid Users', 'Readers', 'Release Administrators', and 'Team Admins' are listed. On the right, the main area shows 'Fabrikam Fiber > Contributors' with 'Edit...' and a dropdown arrow. Below this is a table of permissions:

Permission	Setting
Create tag definition	Allow
Create test runs	Allow
Delete and restore work items	Allow (highlighted with a red box)
Delete team project	Not set
Delete test runs	Allow
Edit project-level information	Not set
Manage project properties	Not set
Manage test configurations	Allow
Manage test environments	Allow
Move work items out of this project	Not set
Permanently delete work items	Not set
Rename team project	Not set
View project-level information	Allow
View test runs	Allow

At the bottom, there are buttons for 'Clear explicit permissions', 'Save changes', and 'Undo changes'.

TIP

In general, if you add a user to the Contributors group, they can add and modify work items. You can restrict permissions of users or user groups to add and modify work items based on the area path. For details, see [Set permissions and access for work tracking](#), [Modify work items under an area path](#).

For a description of each permission, see [Permissions and groups reference](#), [project-level permissions](#).

NOTE

You can't change the permission settings for the Project Administrators group. This is by design.

2. Choose **Save changes**.

Add a group and change its permissions at the organization or collection-level group

1. From your project web portal, choose the  Azure DevOps icon, and then select  **Organization settings**.

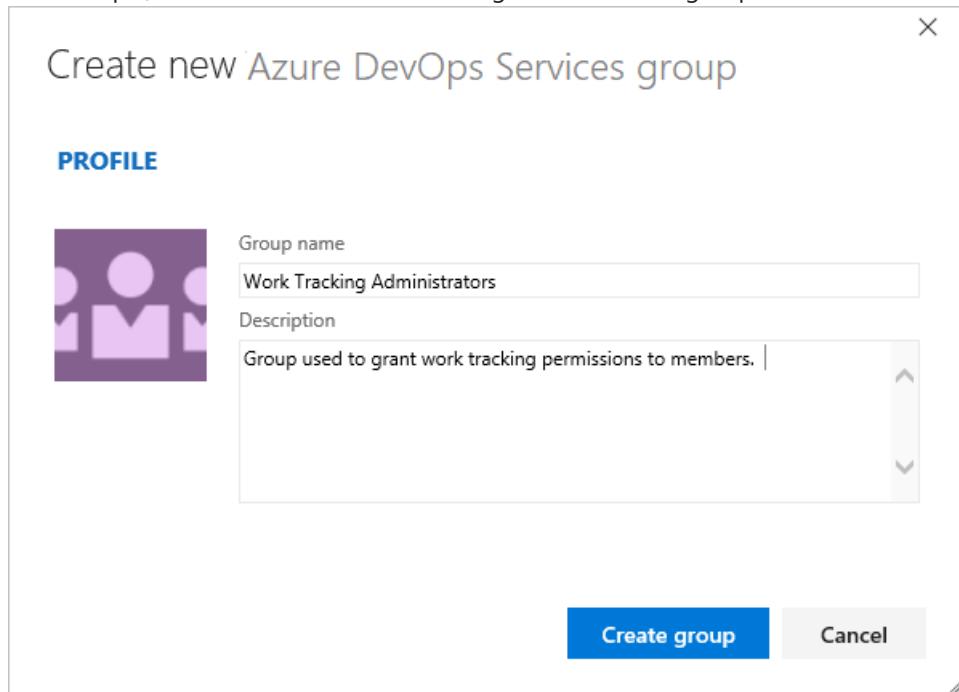


2. Choose **Security**, and then choose **Create group** to open the dialog for adding a group.



3. Enter a name for the group, and optionally a description.

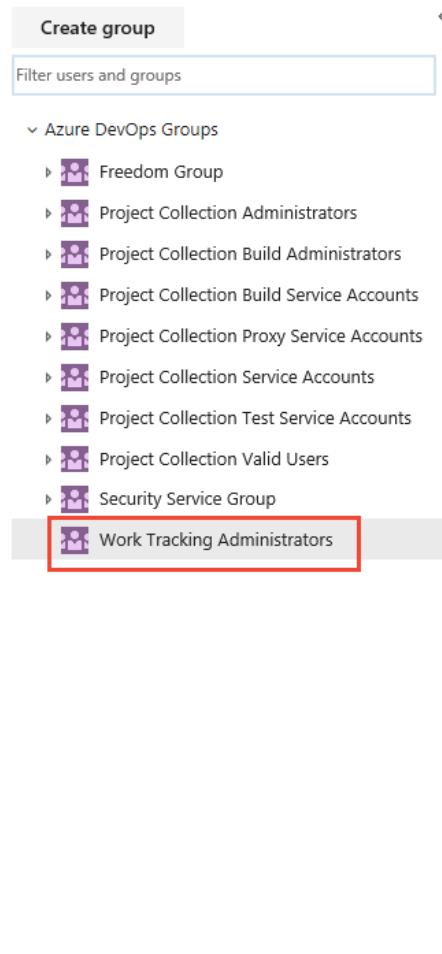
For example, here we define a Work Tracking Administrators group.



For a description of each permission, see [Permissions and groups reference](#), [collection-level permissions](#).

4. Choose the group name you just created and change the permission levels.

Here we grant this group permissions to [manage customizations for the Inheritance process model](#).



The screenshot shows the 'Create group' dialog. On the left, under 'Azure DevOps Groups', several groups are listed: Freedom Group, Project Collection Administrators, Project Collection Build Administrators, Project Collection Build Service Accounts, Project Collection Proxy Service Accounts, Project Collection Service Accounts, Project Collection Test Service Accounts, Project Collection Valid Users, Security Service Group, and Work Tracking Administrators. The 'Work Tracking Administrators' option is highlighted with a red box. On the right, the 'Permissions' tab is selected in the 'fabrikam > Work Tracking Administrators' view, showing a detailed list of permissions with their current status.

	Permissions	Members	Member of
Group used to grant work tracking permissions to members.			
Administer build resource permissions	Not set		
Administer process permissions	Allow		
Administer shelved changes	Not set		
Administer workspaces	Not set		
Alter trace settings	Not set		
Create a workspace	Allow (inherited)		
Create new projects	Not set		
Create process	Allow		
Delete field from account	Allow		
Delete process	Allow		
Delete team project	Not set		
Edit instance-level information	Not set		
Edit process	Allow		
Make requests on behalf of others	Not set		
Manage build resources	Not set		
Manage test controllers	Not set		
Trigger events	Not set		
Use build resources	Not set		
View build resources	Allow (inherited)		
View instance-level information	Allow (inherited)		
View system synchronization information	Not set		

5. Choose **Save changes**.

NOTE

You can't change the permission settings for the Project Collection Administrators group. This is by design.

1. Choose the  settings icon and select **Organization settings** (Azure DevOps) or **Collection settings** (on-premises).



2. Choose **Security**, and then choose **Create group** to open the dialog for adding a group.



The screenshot shows the 'Create group' dialog. The 'Create group' button at the top left is highlighted with a red box. Below it is a search bar labeled 'Filter users and groups'. On the right, the 'fabrikam > Project Collection Administrators' view is shown.

3. Enter a name for the group, and optionally a description.

For example, here we define a Work Tracking Administrators group.

Create new Azure DevOps Services group

PROFILE



Group name
Work Tracking Administrators

Description
Group used to grant work tracking permissions to members.

Create group **Cancel**

For a description of each permission, see [Permissions and groups reference](#), [collection-level permissions](#).

4. Choose the group name you just created and change the permission levels.

Here we grant this group permissions to [manage customizations for the Inheritance process model](#).

Permissions	Members	Member of
Group used to grant work tracking permissions to members.		
Administer build resource permissions	Not set	
Administer process permissions	Allow	
Administer shelved changes	Not set	
Administer workspaces	Not set	
Alter trace settings	Not set	
Create a workspace	Allow (inherited)	
Create new projects	Not set	
Create process	Allow	
Delete field from account	Allow	
Delete process	Allow	
Delete team project	Not set	
Edit instance-level information	Not set	
Edit process	Allow	
Make requests on behalf of others	Not set	
Manage build resources	Not set	
Manage test controllers	Not set	
Trigger events	Not set	
Use build resources	Not set	
View build resources	Allow (inherited)	
View instance-level information	Allow (inherited)	
View system synchronization information	Not set	

Create group

Filter users and groups

- ✓ Azure DevOps Groups
 - ↳ Freedom Group
 - ↳ Project Collection Administrators
 - ↳ Project Collection Build Administrators
 - ↳ Project Collection Build Service Accounts
 - ↳ Project Collection Proxy Service Accounts
 - ↳ Project Collection Service Accounts
 - ↳ Project Collection Test Service Accounts
 - ↳ Project Collection Valid Users
 - ↳ Security Service Group
 - ↳ Work Tracking Administrators**

5. Choose **Save changes**.

NOTE

You can't change the permission settings for the Project Collection Administrators group. This is by design.

On-premises deployments

For on-premises deployments, see these additional topics:

- [Add a user as a TFS server administrator](#)
- [TFS service account groups](#)

If your on-premises deployment is integrated with SQL Server Reports, you'll need to manage membership for those products separately from their websites. See [Grant permissions to view or create SQL Server reports in TFS](#).

If your on-premises deployment is integrated with a SharePoint product or SQL Server Reports, you'll need to manage membership for those products separately from their websites.

- [Set SharePoint site permissions](#)
- [Grant permissions to view or create SQL Server reports in TFS](#)

Next steps

[Manage projects](#)

Related articles

- [About permissions and groups](#)
- [Permissions lookup reference](#)
- [Permissions and groups reference](#)
- [Manage teams and configure team tools](#)

Set up Active Directory or Azure Active Directory

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

The method we recommend for managing a large set of user accounts is to use Azure Active Directory (Azure AD) for Azure DevOps Services and Active Directory (AD) for Azure DevOps Server or Team Foundation Server (TFS). By managing your user base using AD/Azure AD, you simplify the maintenance of managing permissions across your organization.

If you only have to manage a small set of users, then you can skip this step. However, if you foresee that your organization may grow, you may want to set up AD or Azure AD. Also, if you plan on paying for extra services, you'll need to set up Azure AD for use with Azure DevOps to support billing.

Use this topic to access articles that show you how to:

- Set up Azure Active Directory for use with Azure DevOps Services
- Manage organizational access with Azure AD

Use this topic to access articles that show you how to:

- Set up Active Directory for use with TFS

NOTE

Without Azure AD, all Azure DevOps users must sign in using Microsoft accounts, and you must manage account access by individual user accounts. Even if you manage account access using Microsoft accounts, you need to set up an [Azure subscription in order to manage billing](#).

Set up Azure Active Directory for use with Azure DevOps Services

- [Access Azure DevOps with Azure Active Directory \(Azure AD\)](#)

Manage organizational access with Azure AD

- [Add Azure DevOps users to your Azure AD](#)
- [Connect Azure DevOps organization to Azure AD](#)
- [Disconnect Azure DevOps organization from Azure AD](#)
- [Delete users from Azure DevOps connected to Azure AD](#)
- [Troubleshoot access with Azure Active Directory](#)

Set up Active Directory for use with Azure DevOps Server

Use these resources to learn about installing Active Directory. Typically, you should install Active Directory prior to installing TFS.

- [Install Active Directory Domain Services \(Level 100\)](#)
- [Step-By-Step: Setting up Active Directory in Windows Server 2016](#)

Set up Active Directory for use with an on-premises TFS

Use these resources to learn about installing Active Directory. Typically, you should install Active Directory prior to installing TFS.

- [Install Active Directory Domain Services \(Level 100\)](#)
- [Step-By-Step: Setting up Active Directory in Windows Server 2016](#)

Next steps

[Add AD/Azure AD security groups to built-in security groups](#)

Related articles

- [About security and identity](#)
- [How billing works](#)
- [Set up billing to pay for users, pipelines, and cloud-based load testing in Azure DevOps](#)
- [What is Azure Active Directory?](#)
- [Get started with Azure AD](#)

Add AD/Azure AD users or groups to a built-in security group

6/21/2019 • 3 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

As described in [About security and identity](#), there are two main types of built-in security groups: project-level and collection-level. In general, you add users and groups to a project-level group such as Contributors and Readers. For users that need to administrate select features and functions, add them or associated groups to the Build Administrators or Project Administrators groups.

Review [Default permissions and access](#) to gain insight into the default permissions provided to the built-in, project-level security groups.

In this topic you'll learn how to:

- Add an AD/Azure AD user or group to a built-in security group

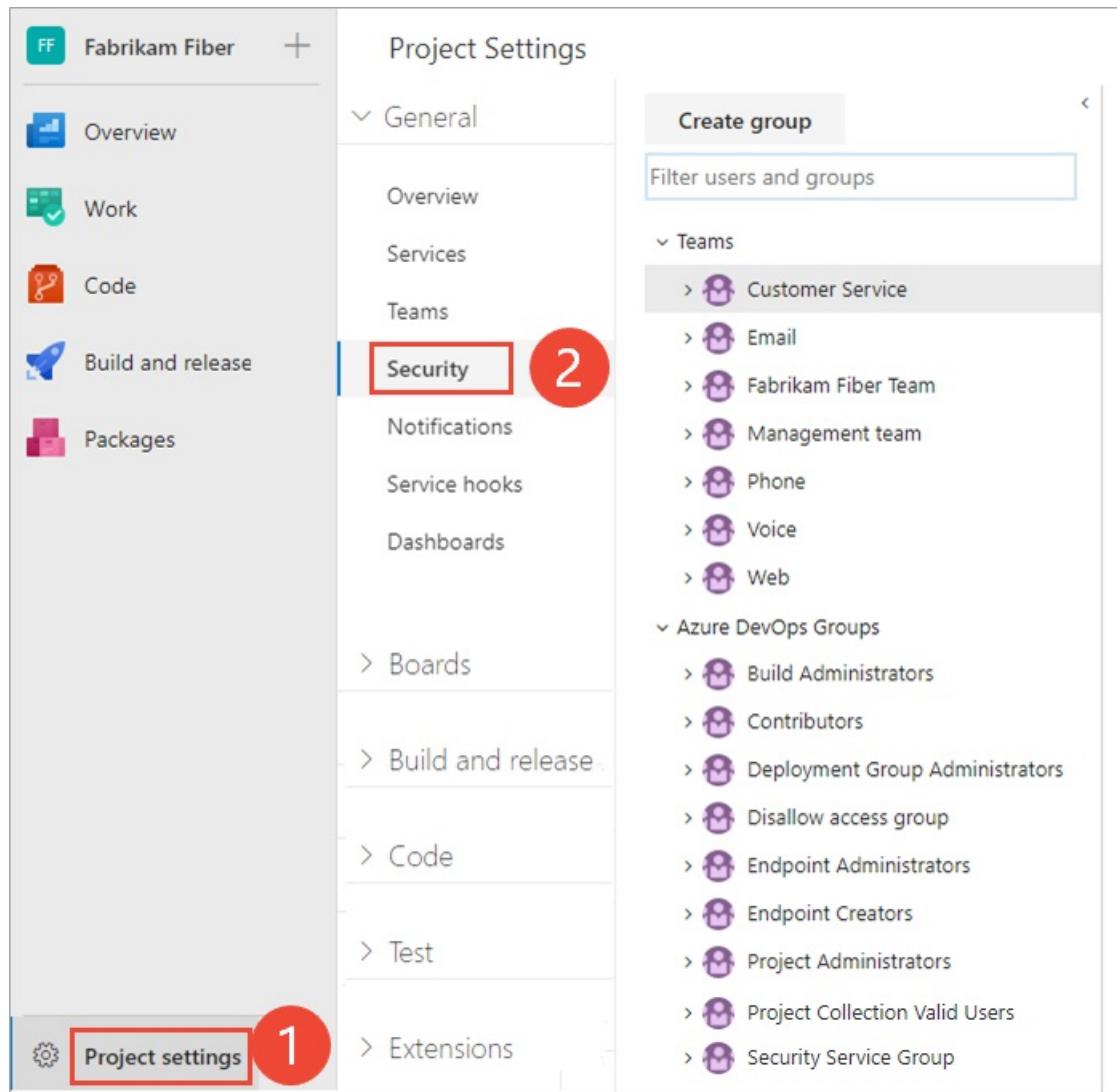
The method for adding a user or group to a built-in security group is the same, no matter at what level you add them.

Add an AD/Azure AD user or group to a built-in security group

IMPORTANT

If you are adding a user to Azure DevOps for the first time, see [Add users for Azure DevOps](#). To manage the permissions of an Azure AD group in Azure DevOps, you must first add the Azure AD group to a built-in security group. Once you complete this task, you can then manage your Azure AD group permissions throughout Azure DevOps.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose **Project Settings** and then **Security**.



3. Open **Security** and under the **Groups** section, choose one of the following:

- To add users who require read-only access to the project, choose **Readers**.
- To add users who need to contribute fully to the project or who have been granted Stakeholder access, choose **Contributors**.
- For users who need to administrate the project, choose **Project Administrators**.

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

Here we choose the **Contributors** group.

The screenshot shows the 'Contributors' group members page. The 'Members' tab is selected. The left sidebar shows a tree view of groups: 'Teams' (Customer Service, Fabrikam Fiber Team, Management team, Phone, Voice, Web) and 'Azure DevOps Groups' (Build Administrators, Contributors, Project Administrators, Project Valid Users, Readers). A red box highlights the 'Contributors' item under 'Azure DevOps Groups'. The main area lists members with their display names, usernames or scopes, and a 'Remove' link.

Display Name	Username Or Scope	
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Management team	[Fabrikam Fiber]	
Phone	[Fabrikam Fiber]	
Voice	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Jia-hao Tseng	fabrikamfiber9@hotmail.com	

By default, the default team group and all other teams you add to the project are included as members of the Contributors group. So, you can choose to [add a new user as a member of a team](#) instead, and the user would automatically inherit Contributor permissions.

5. Choose **+ Add** to add a user or a user group.
6. Enter the name of the user 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 choice.

The screenshot shows the 'Add users and groups' dialog box. The 'User or group' input field contains 'Chris'. Below it, a search result for 'Christie Church fabrikamfiber1@hotmail.com' is shown, with a small profile picture and the email address. At the bottom are 'Save changes' and 'Cancel' buttons.

NOTE

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

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open **Project Settings**.

The screenshot shows the 'Fabrikam Fiber' project in the Azure DevOps interface. A red arrow points from the gear icon in the top right corner down to the 'Project settings' option in the dropdown menu.

Project settings

- Overview
- Work
- Security
- Version Control
- Policies
- Agent Queues
- Notifications
- Service Hooks
- Services
- Test
- Release
- Dashboards
- Project settings**
- Organization settings

3. Open **Security** and under the **Groups** section, choose one of the following:

- To add users who require read-only access to the project, choose **Readers**.
- To add users who need to contribute fully to the project or who have been granted Stakeholder access, choose **Contributors**.
- For users who need to administrate the project, choose **Project Administrators**.

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

Here we choose the **Contributors** group.

The screenshot shows the 'Contributors' group page in the Azure DevOps interface. A red box highlights the 'Contributors' link in the left navigation bar. Another red box highlights the 'Members' tab at the top of the main content area. The table lists the members of the group:

Display Name	Username Or Scope	Action
Customer Service	[Fabrikam Fiber]	Remove
Fabrikam Fiber Team	[Fabrikam Fiber]	
Management team	[Fabrikam Fiber]	
Phone	[Fabrikam Fiber]	
Voice	[Fabrikam Fiber]	
Web	[Fabrikam Fiber]	
Jia-hao Tseng	fabrikamfiber9@hotmail.com	

By default, the default team group and all other teams you add to the project are included as members of the Contributors group. So, you can choose to [add a new user as a member of a team](#) instead, and the user

automatically inherits Contributor permissions.

5. Choose **+ Add** to add a user or a user group.
6. Enter the name of the user 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 meet your choice.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group

 Christie Church fabrikamfiber1@hotmail.com	Edit
---	----------------------

Showing 1 result

Save changes **Cancel**

NOTE

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

Next steps

[Change individual permissions, grant select access to specific functions](#)

Related articles

- [About permissions and groups](#)
- [Set permissions at the project-level or project collection-level](#)
- [About security and identity](#)

Change individual or group permissions

6/14/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

The standard way to set permissions is by adding them to one or more built-in security groups. However, sometimes you may want to grant additional permissions to select users, where not all permissions are assigned to the security group. For example, if you want to give some users the ability to add or edit area and iteration paths, but don't want them to have all permissions available to members of the Project Administrators group.

You can change individual permissions in one of the following three ways:

- Create a custom Azure DevOps security group, define permissions for that group, add the user account to the group
- For object-level permissions: Add the user account and set permissions
- For project or collection-level permissions: Search for the user account and selectively change their permission assignments

In this article you learn how to do the following tasks:

- Create a custom security group
- Set permissions for a custom security group
- Add members to a custom security group
- Change the permission assignments for an individual user

If you're new to managing permissions and groups, review [About permissions and groups](#) to learn about permission states and inheritance.

NOTE

The images you see from your web portal may differ from the images you see in this article. These differences result from updates made to Azure DevOps Services or your on-premises deployment. However, the basic functionality available to you remains the same unless explicitly mentioned.

Create a custom security group

Create a custom security group at the project-level or the collection-level. The method for creating a custom security group is the same, no matter at what level you add it.

To create a project-level security group, open the web portal and choose the project where you want to add users or groups.

1. Choose **Project Settings > Security**.

To see the full image, click to expand.

The screenshot shows the 'Project Settings' page for the 'Fabrikam Fiber' project. On the left, there's a sidebar with icons for Overview, Work, Code, Build and release, and Packages. Below this is the 'Project settings' button, which is highlighted with a red box and a red circle containing the number '1'. The main area is titled 'Project Settings' and has a 'General' section expanded. Under 'General', there are links for Overview, Services, Teams, Security (which is highlighted with a red box and a red circle containing the number '2'), Notifications, Service hooks, and Dashboards. To the right of the General section is a 'Create group' dialog box. This dialog has a 'Filter users and groups' input field and a list of groups under 'Teams' and 'Azure DevOps Groups'. The 'Customer Service' group is selected in the 'Teams' list.

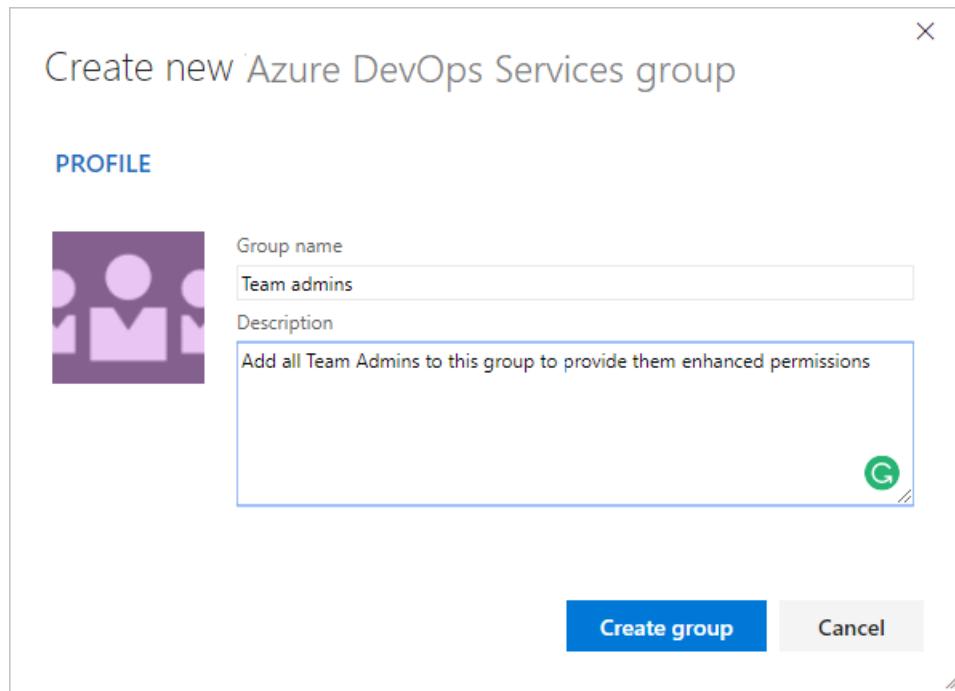
2. Choose **Create group** to open the dialog for adding a group.

The screenshot shows the 'Create group' dialog for the 'Customer Service' group. The title bar says 'Create group' and 'Fabrikam Fiber > Customer Service'. There's an 'Edit...' button with a dropdown arrow. The dialog has a 'Filter users and groups' input field. On the left is a tree view of groups under 'Teams' and 'Azure DevOps Groups'. The 'Customer Service' group is selected and expanded, showing its permissions. On the right, there are three tabs: 'Permissions', 'Members', and 'Member of'. The 'Permissions' tab displays a list of permissions with their current status ('Not set' or 'Allow (inherited)').

Permission	Status
Bypass rules on work item updates	Not set
Change process of team project.	Not set
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set
Delete shared Analytics views	Allow (inherited)
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Edit shared Analytics views	Allow (inherited)
Manage project properties	Not set
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Not set
Permanently delete work items	Not set

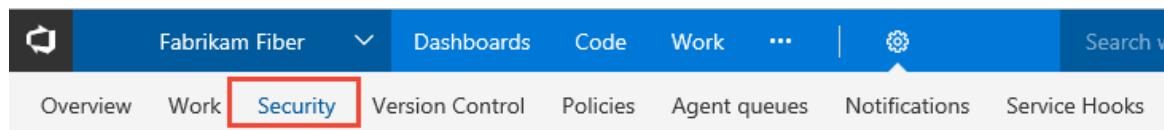
3. Enter a name for the group, and optionally a description.

For example, here we define a Team Admins group.



4. Choose **Create group**.

1. Open **Project Settings**. Choose the gear settings icon, and choose **Security**.



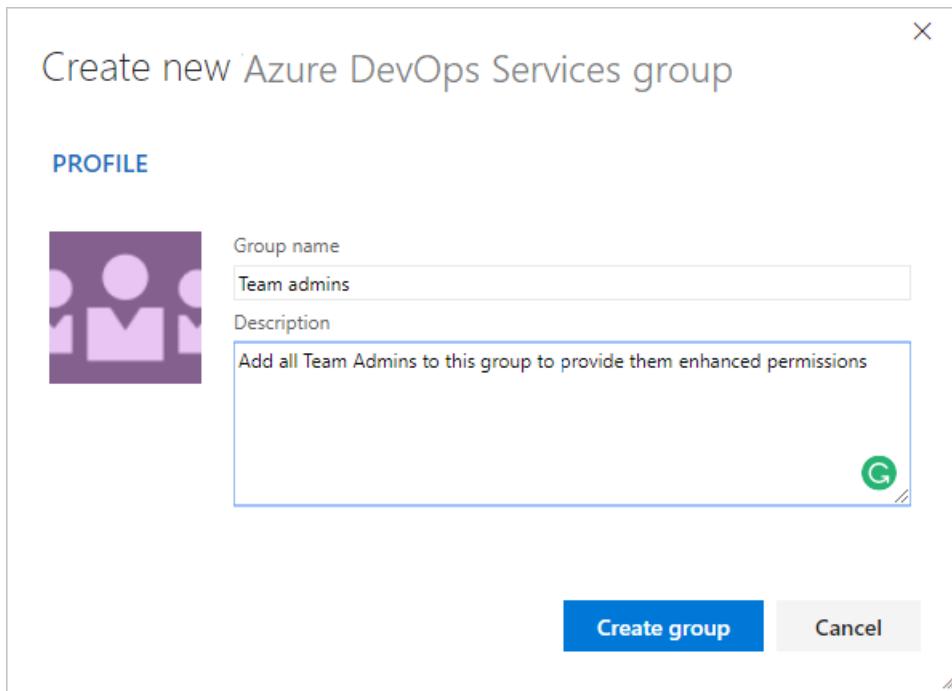
2. Choose **Create group** to open the dialog for adding a group.

The screenshot shows the 'Create group' dialog on the left and the 'Customer Service' security settings page on the right. The 'Create group' dialog has a red box around the 'Create group' button. The security settings page lists permissions for the Customer Service team, such as 'Bypass rules on work item updates' (Not set) and 'Change process of team project' (Not set).

Permission	Setting
Bypass rules on work item updates	Not set
Change process of team project	Not set
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Not set
Delete shared Analytics views	Allow (inherited)
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Edit shared Analytics views	Allow (inherited)
Manage project properties	Not set
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Not set
Permanently delete work items	Not set

3. Enter a name for the group, and optionally a description.

For example, here we define a Team Admins group.



4. Choose **Create group**.

Set permissions for a custom security group

1. To set permissions for the custom group you created, choose the group name and then set one or more permissions.

The screenshot shows the 'Security' tab selected in the top navigation bar. A custom security group named 'Team Admins' is selected. The left sidebar lists various groups under 'Azure DevOps Groups'. The 'Team Admins' item is highlighted with a red box. The main pane displays a table of permissions with their current status (Allow, Deny, Not set). At the bottom are 'Save changes' and 'Undo changes' buttons.

Permission	Status
Bypass rules on work item updates	Allow
Create tag definition	Allow
Create test runs	Allow
Delete and restore work items	Allow
Delete team project	Deny
Delete test runs	Not set
Edit project-level information	Not set
Manage project properties	Deny
Manage test configurations	Allow
Manage test environments	Allow
Move work items out of this project	Allow
Permanently delete work items	Allow
Rename team project	Deny
Suppress notifications for work item updates	Not set
View analytics	Allow (inherited)
View project-level information	Allow
View test runs	Allow

For a description of each permission, see [Permissions and groups reference](#), [project-level permissions](#).

- Choose **Save changes**.

Add members to a custom security group

You add members to a custom security group in the same way you add users to a built-in group.

- Choose the security group, choose **Members**, and then choose **Add**.

The screenshot shows the 'Team Admins' members page. The 'Members' tab is selected. A red box highlights the '+ Add...' button. The search bar shows 'No identities found in current scope.'

2. Enter the user identity 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 choice.

The screenshot shows the 'Add users and groups' dialog box. The 'User or group' input field contains 'Chris'. A search result for 'Christie Church' is shown, with a red box highlighting the user card. The card displays the name 'Christie Church' and the email 'fabrikamfiber1@hotmail.com'. Below the card, it says 'Showing 1 result'. At the bottom right are 'Save changes' and 'Cancel' buttons.

NOTE

Users that have limited access, such as Stakeholders, won't be able to access select features even if granted permissions to those features. To learn more, see [Permissions and access](#).

Change individual permission at the project-level

1. From the project-level **Security** page, enter the user identity in the **Filter users and groups** box. Then, select the account whose permissions you want to change.

The screenshot shows the 'Contributors' members page. The 'Members' tab is selected. A red box highlights the search bar containing 'Rais' and the user card for 'Raisa Pokrovskaya'. The card displays the name 'Raisa Pokrovskaya' and the email 'fabrikamfiber5@hotmail.com'. Below the card, it says 'Showing 1 result'. At the bottom right are 'Edit...' and 'Search' buttons.

2. Change the permission, setting a permission as **Allow** or **Deny**.

The screenshot shows the 'Create group' dialog for a user named 'Raisa Pokrovskaya'. The left sidebar lists 'Permissions' and 'Member of'. The main area displays a table of permissions with their current status. The 'Move work items out of this project' row has its 'Allow' value highlighted with a blue border.

Permission	Status
Bypass rules on work item updates	Not set
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Allow
Delete team project	Not set
Delete test runs	Allow (inherited)
Edit project-level information	Not set
Manage project properties	Allow
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Allow
Permanently delete work items	Allow
Rename team project	Not set
Suppress notifications for work item updates	Not set
View analytics	Allow (inherited)
View project-level information	Allow (inherited)
View test runs	Allow (inherited)

[Clear explicit permissions](#)

[Save changes](#) [Undo changes](#)

For a description of each permission, see [Permissions and groups reference, project-level permissions](#).

3. Choose **Save changes**.

Change individual permission at the collection-level

1. Open the user-level or collection-level **Security** admin page and follow the instructions provided in the previous section for project-level permissions.

For a description of each collection-level permission, see [Permissions and groups reference, collection-level permissions](#).

Change individual permission at an object-level

From the web portal, open the Security dialog for the object whose permissions you want to set. For specific instructions, see the following articles:

AREA	TASK
Wiki & Dashboard permissions	<ul style="list-style-type: none">• README & Wiki• Dashboards

DevOps (code, build, test, release) permissions	<ul style="list-style-type: none"> • Git branch • Git repository • TFVC • Builds • Release pipeline security • Approvals and approvers
Work tracking permissions	<ul style="list-style-type: none"> • Area and iteration paths • Work item query and folder • Plan permissions

1. From the Security dialog, choose **Add**.

Permission	Status
Contribute	Allow (inherited)
Edit policies	Not set
Exempt from policy enforcement	Not set
Force push (rewrite history, delete branches and tags)	Not set
Manage permissions	Not set
Remove others' locks	Not set

2. Enter the user ID, choose search, and then make your selection in the left pane.
3. Update the permission setting to **Allow** or **Deny** for specific permissions.

Security for features/hello-world branch in Fabrikam Fiber

+ Add... Inheritance ▾

Search ⚙

✓ Azure DevOps Groups

- Build Administrators
- Contributors
- Project Administrators
- Readers
- Project Collection Administrators
- Project Collection Build Service Accou...
- Project Collection Service Accounts

✗ Users

- Raisa Pokrovskaya
- Fabrikam Fiber Build Service (fabrikam)
- Project Collection Build Service (fabrikam)

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Contribute	Allow (inherited)
Edit policies	Allow (inherited)
Exempt from policy enforcement	Allow
Force push (rewrite history, delete branches and tags)	Allow (inherited)
Manage permissions	Allow (inherited)
Remove others' locks	Allow (inherited)

Clear explicit permissions

Remove Save changes Undo changes

Close

The screenshot shows the 'Security' dialog for a specific branch in a project. On the left, there's a sidebar with 'Add...', 'Inheritance', and a search bar. Below that is a tree view of 'Azure DevOps Groups' and 'Users'. Under 'Users', 'Raisa Pokrovskaya' is selected. On the right, the 'ACCESS CONTROL SUMMARY' section displays various permissions with their current status: Contribute (Allow (inherited)), Edit policies (Allow (inherited)), Exempt from policy enforcement (Allow), Force push (Allow (inherited)), Manage permissions (Allow (inherited)), and Remove others' locks (Allow (inherited)). A blue box highlights the 'Allow' button for the 'Exempt from policy enforcement' permission. At the bottom, there are 'Remove', 'Save changes', and 'Undo changes' buttons, and a 'Close' button.

For a description of specific permissions, see [Permissions and groups reference](#).

4. Choose **Save changes**.

Next steps

[Grant or restrict access to select features](#)

Related articles

- [Permissions lookup guide](#)
- [About permissions and groups](#)
- [Permissions and groups reference](#)
- [Set permissions at the project-level or project collection-level](#)

Grant or restrict access

5/24/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You can grant or restrict access to resources that you manage in Azure DevOps. You may want to open up or close down access to a select set of features and for a select set of users. While the built-in security groups provide a standard set of permission assignments, you may need additional security requirements not met by these assignments.

If you're new to administrating permissions and groups, review [About permissions and groups](#) to learn about permission states and inheritance.

In this article you learn how to do the following tasks:

- Recommended method for granting and restricting permissions
- Delegate tasks by assigning select permissions to specific roles
- Restrict access to view or modify objects
- Restrict modification of work items based on a user or group

TIP

Because you set many permissions at an object-level, such as repositories and area paths, how you structure your project determines the areas you can open up or close down.

Recommended method for granting and restricting permissions

For maintenance purposes, we recommend you use either the built-in security groups or [custom security groups to manage permissions](#).

You can't change the permission settings for the Project Administrators group or the Project Collection Administrators group, which is by design. However, for all other groups, you can change the permissions.

If you manage a small number of users, then you may find changing individual permissions a valid option. However, custom security groups allow you to better track roles and permissions assigned to those roles.

Delegate tasks to specific roles

As an administrator or account owner, it's a good idea to delegate administrative tasks to those team members who lead or manage an area. Several of the main built-in roles that come with default permissions and role assignments are:

- Readers
- Contributors
- Team Administrator (role)
- Project Administrators
- Project Collection Administrators

For a summary of permissions for the above roles, see [Default permissions and access](#), or for the Project Collection Administrators, see [Add administrators](#)

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 (TFVC)	Manage repository and branches	Administer labels, Manage branch, and Manage permissions See Set repository permissions for Git or TFVC .
Software architect (Git)	Manage repositories	Create repositories, Force push, and Manage permissions See Set repository permissions for Git or TFVC .
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 Add administrators, set permissions at the project-level or project collection-level .
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 Add administrators, set permissions at the project-level or project collection-level .
Process template manager (Hosted XML process model)	Work tracking customization	Edit collection-level information, See Add administrators, set permissions at the project-level or project collection-level .
Project management (On-premises XML process model)	Work tracking customization	Edit project-level information, See Add administrators, set permissions at the project-level or project collection-level .

Permissions manager	<p>Manage permissions for a project, account, or collection</p>	<p>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 grant permissions, See Add administrators, set permissions at the project-level or project collection-level.</p> <p>You can also grant permissions to manage permissions for the following objects:</p> <ul style="list-style-type: none"> • Manage Git or TFVC repository permissions • Manage Git branch permissions • Administer build and release permissions • Manage Wiki permissions.
---------------------	---	---

Restrict access to view or modify objects

Azure DevOps is designed to enable all valid users to view all objects defined in the system. You can restrict access to resources by setting the permission state to **Deny**. You can set permissions for members that belong to a custom security group or for an individual user. To learn more about how to set these types of permissions, see [Change individual permissions, grant select access to specific functions](#).

Area to restrict	Permissions to set to Deny
View or contribute to a repository	<p>View, Contribute See Set repository permissions for Git or TFVC.</p>
View, create, or modify work items within an area path	<p>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.</p>
View or update select build and release pipelines	<p>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.</p>
Edit a dashboard	<p>View dashboards See Set dashboard permissions.</p>

Restrict modification of work items based on a user or group

For [On-premises XML process model](#), you can customize work item types to support these restriction requests:

- Restrict who can create or modify a work item
- Restrict who can create specific work item types, such as Epics or Features

You can restrict modification of work items by adding a rule to the work item type, usually within the **WORKFLOW** section. To learn more, see [Add a rule to a work item type](#), [Apply or ignore rules based on user or group](#).

NOTE

These restriction types aren't available for organizations in Azure DevOps and the [Inheritance process model](#).

Next steps

[Remove user accounts](#)

Related articles

- [Default permissions and access](#)
- [Permission lookup guide](#)
- [About permissions and groups](#)
- [Permissions and groups reference](#)
- [Set permissions at the project-level or project collection-level](#)

Remove user accounts

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

When a user with access to Azure DevOps leaves a company, an administrator would typically remove them from Azure Active Directory or Active Directory. This automatically voids their user account and remove their ability to access or connect to Azure DevOps.

If you manage your Azure DevOps users with Microsoft Service Accounts (MSA), then you'll need to [remove their account](#).

In this topic you'll find:

- A checklist to review when removing user accounts
- Options for removing users from organizations in Azure DevOps
- Links to topics for removing user accounts from AD or Azure AD

In this topic you'll find:

- A checklist to review when removing user accounts
- Links to topics for removing user accounts from AD or Azure AD

Consider when removing users

- Have you granted users any paid extensions? You'll want to [transfer those extensions to another user](#).
- Do users have any tokens that you need to revoke?
- Have you granted individual user accounts special permissions that need to be revoked?
- Have you reassigned work users you are removing to current team members?

Remove users from an organization in Azure DevOps

If your organization uses MSA accounts, then to you must remove users from the organization as you have no other way to prevent access. When you do so, you'll not be able to create a query for work items assigned to the removed user account. To learn more, see [Delete users from Azure DevOps](#).

If your organization is backed by Azure AD, then you can disable or delete the Azure AD user account while leaving their Azure DevOps account active. In this way, you can continue to query their work item history using their account name.

Remove users from AD or Azure AD

For information on removing users from AD or Azure AD, see one of these topics:

- [Delete users from Azure AD](#)
- [Delete a User Account from Active Directory](#)

Reduce the number of paid users, reassign paid extensions

- [Change number of users who have paid Basic access](#)
- [Assign paid extension access to users](#)

NOTE

To manage users, you must be a member of the [Project Collection Administrator group](#).

Related articles

- [About permissions and groups](#)
- [Set permissions at the project-level or project collection-level](#)
- [About security and identity](#)

Get started as a Stakeholder

6/14/2019 • 9 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

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. Stakeholder access is one of several supported access levels. To understand the full set of features Stakeholders have access to, see [About access levels](#).

NOTE

For public projects, Stakeholder access gives users greater access to work tracking features. To learn more, see [Default roles and access for public projects](#).

With Stakeholder access, you can add and modify work items, view and approve pipelines, and view dashboards. You can check project status and provide direction, feedback, feature ideas, and business alignment to a team. Stakeholder access is one of several supported access levels. To understand the full set of features Stakeholders have access to, see [About access levels](#).

With Stakeholder access, you can add and modify work items. You can check project status and provide direction, feedback, feature ideas, and business alignment to a team. Stakeholder access is one of several supported access levels. To understand the full set of features Stakeholders have access to, see [About access levels](#).

Use this tutorial to learn how to do the following tasks:

- Sign in to a project
- Add a work item
- View the product backlog and add new work to it
- View work in progress on the Kanban board
- Find work assigned to you, or query for other work items

For information about working with pipelines, see these articles:

- [Build your GitHub repository](#)
- [Build OSS repositories](#)

First time signing in

1. Choose the link provided in the email invitation you should have received. Or, open a browser window and enter the URL for the web portal.

`http://dev.azure.com/OrganizationName/ProjectName`

`http://ServerName:8080/tfs/DefaultCollection/ProjectName`

For example, to connect to the server named *FabrikamPrime* and project named *Contoso*, enter

`http://FabrikamPrime:8080/tfs/DefaultCollection/Contoso`.

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.

View and add work items

You can start viewing and adding work items once you connect to a project.

1. (1) Check that you have selected the right project, then (2) choose **Boards > Work Items**.

The screenshot shows the Azure DevOps interface for the 'fabrikam / Fabrikam Fiber' project. The 'Work Items' tab is active. The sidebar on the left has a red box around the 'Work Items' menu item, with a red circle containing the number '2' to its right. At the top, the project name 'fabrikam / Fabrikam Fiber' is highlighted with a red box, and a red circle with the number '1' is positioned to its right. The main area displays a table of work items with columns for ID, Assigned To, State, and Title. The work items listed are:

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

2. Within the drop-down menu, you can focus on relevant items inside a project using one of the seven pivots, as described next.

Work Items" />

- **Assigned to me:** lists all work items assigned to you in the project in the order they were last updated. To open or update a work item, simply click its title.
- **Following:** lists work items that you've elected to follow.
- **Mentioned:** lists work items in which you've been mentioned in the last 30 days.
- **My activity:** lists work items that you've recently viewed or updated.
- **Recently updated:** lists work items recently updated in the project.
- **Recently completed:** lists work items completed or closed in the project.
- **Recently created:** lists work items created within the last 30 days in the project.

3. To add a work item, choose the work item type from the **New Work Item** drop down menu.

For example, here we choose User Story.

Work Items

The screenshot shows the 'Work Items' list interface. At the top, there's a dropdown menu labeled 'Assigned to me' with a downward arrow. Next to it is a '+ New Work Item' button with a plus sign. To the right of the button are links for 'Open filtered view in Queries' and 'Column Options'. Further right are 'Re' and 'Pin' buttons. Below the menu is a search bar with the placeholder 'Filter by keyword'. To the right of the search bar are three dropdown filters: 'States' (with options 'Resolved', 'New', 'Active'), 'Area' (with options 'Fabrikam Fiber', 'Fabrikam Fiber', 'Fabrikam Fiber', 'Fabrikam Fiber'), and 'Tags' (with options 'Fabrikam Fiber', 'Fabrikam Fiber', 'Fabrikam Fiber', 'Fabrikam Fiber'). A 'Clear' button is also present. On the left, a list of work item types is shown with icons: Bug (red exclamation), Epic (orange crown), Feature (purple trophy), Issue (pink exclamation), Task (yellow checkmark), Test Case (green checkmark), and User Story (blue document). The 'User Story' item is highlighted with a red box. On the right, a table lists several work items with their titles, states, areas, and tags.

State	Area	Tags
Resolved	Fabrikam Fiber	
New	Fabrikam Fiber	
Active	Fabrikam Fiber	
New	Fabrikam Fiber	
Resolved	Fabrikam Fiber	
Closed	Fabrikam Fiber	

4. Enter a title and then save the work item. Before you can change the State from its initial default, you must save it.

The screenshot shows the 'USER STORY 398' edit screen. At the top, the title 'USER STORY 398' and the ID '398 Cancel order form' are displayed. Below the title, the author 'Jamal Hartnett' and the creation date '0' are shown. There are buttons for 'Add Tag' and 'Save & Close' (which is highlighted with a red box). The main area contains fields for 'Description' (with rich text editor), 'Planning' (Story Points: 2, Priority: 2, Risk: 2), 'Development' (with a note: 'Development hasn't started on this item.'), 'Acceptance Criteria' (with rich text editor), 'Classification' (Value area: Business), and 'Discussion' (with a comment placeholder 'Add a comment').

NOTE

A caution icon on a tab indicates values that violate validation rules. You must correct information on that tab in order to save the work item.

1. Choose **Work**, choose a work item, for example User Story, from the New Work Item list of options. Choose the pin icon to have it show up within the **Work** drop down menu.

Fabrikam Fiber ☆

Tracking web, voice, and other app development

Showing README.md in \$/Fabrikam Fiber A

Fabrikam Fiber Voice team

The Voice team supports all voice services, including VOIP, voicemail, instant messaging, and the frameworks, security, authentication, and file services associated with these services.

NEW WORK ITEM

- Epic
- Feature
- Issue
- Task
- Test Case
- User Story

- Enter a title and then save the work item. Before you can change the State from its initial default, you must save it.

USER STORY 398

398 Cancel order form

Jamal Hartnett 0 Add Tag

Save & Close Follow ...

State: New Area: Fabrikam Fiber Updated by Raisa Pokrovskaya 11/3/2015

Reason: New Iteration: Fabrikam Fiber

Description:

Planning:

Development:

Acceptance Criteria:

Discussion:

Classification:

NOTE

A caution icon on a tab indicates values that violate validation rules. You must correct information on that tab in order to save the work item.

Work items you add are automatically scoped to your team's default area and iteration paths. To change the team context, see [Switch project or team focus](#).

- Choose **Work>Queries**, choose a work item from the **New** drop down menu.

The screenshot shows the Azure DevOps 'Queries' interface. On the left, a sidebar lists work item types: Bug, Epic, Feature, Issue, Task, Test Case, and User Story, with 'User Story' highlighted by an orange rectangle. The main area displays a query titled 'Assigned to me'. The 'Results' tab is selected, showing three items in a table:

ID	Work Item...	Title
466	Task	Develop standards guidelines
346	User Story	Add animated emoticons
512	Task	Welcome screen

2. Enter a title and then save the work item. Before you can change the State from its initial default, you must save it.

Work items you add are automatically scoped to your team's default area and iteration paths. To change the team context, see [Switch project or team focus](#).

For descriptions of each field, see [Work item field index](#).

NOTE

Depending on the process chosen when the project was created, the types of work items you can create may differ. For example, backlog items may be called user stories ([Agile](#)), product backlog items ([Scrum](#)), or requirements ([CMMI](#)). All three are similar—they describe the customer value to deliver and the work to be performed. For an overview of all three processes, see [Choose a process](#).

Add tags to a work item

Tags are useful for filtering backlogs, boards, and queries

All users granted Stakeholder access for a private project can only [add existing tags to work items](#), not add new tags. Even if the **Create tag definition** permission for the user is set to Allow, per the Stakeholder access settings.

Azure DevOps Services users granted Stakeholder access for a public project can add new and existing tags to work items.

Check the backlog, add work items to the backlog

Work appears in the backlog in priority order. Work item types may include bugs depending on the settings made for the team.

1. (1) Check that you selected the right project, (2) choose **Boards > Backlogs**, and then (3) select the correct team from the team selector menu.

The screenshot shows the Azure DevOps interface for the project 'fabrikam / Fabrikam Fiber'. The top navigation bar has 'Azure DevOps' and the project name 'fabrikam / Fabrikam Fiber'. A red box labeled '1' highlights the project selector. Below it, a red box labeled '2' highlights the 'Backlogs' option in the left sidebar. Another red box labeled '3' highlights the 'Fabrikam Fiber Team' dropdown in the top right, which is currently selected. The main area displays a backlog of work items with columns for Order, Assigned To, State, and Title. The backlog items are:

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 another team, open the selector and select a different team or choose the [Browse all sprints](#) option. Or, you can enter a keyword in the search box to filter the list of team backlogs for the project.

This is a modal dialog titled 'My Team Backlogs'. At the top is a search bar labeled 'Search team backlogs'. Below it is a list of backlog items: 'Account Management', 'Customer Profile', 'Fabrikam Team' (which is highlighted with a gray background), 'Phone', 'Service Delivery', 'Service Status', and 'Shopping Cart'. At the bottom of the list is a link 'Browse all backlogs'.

TIP

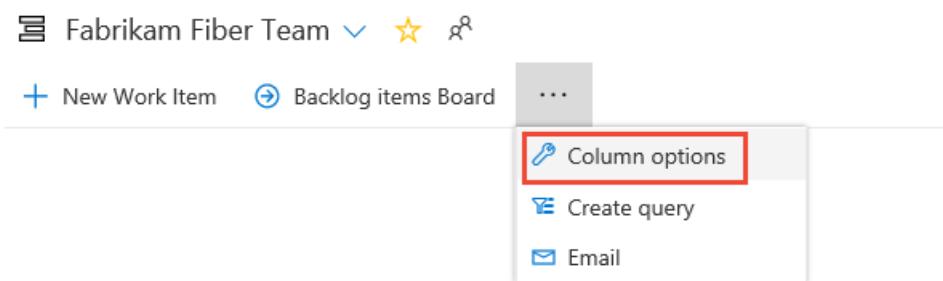
Choose the star icon to favorite a team backlog. Favorited artifacts (favored icon) appear at the top of the team selector list.

- Check that you have selected **Backlog items** (for Scrum), **Stories** (for Agile), or **Requirements** (for CMMI) as the backlog level.

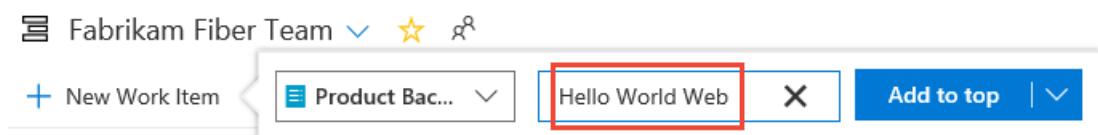
The screenshot shows the ribbon bar at the top of the backlog items page. It includes buttons for 'New Work Item', 'Backlog items Board', '...', and 'Backlog items'. The 'Backlog items' button is highlighted with a red box.

- (Optional) To choose which columns should display and in what order, choose the actions icon and

select **Column options**. To learn more, see [Change column options](#).

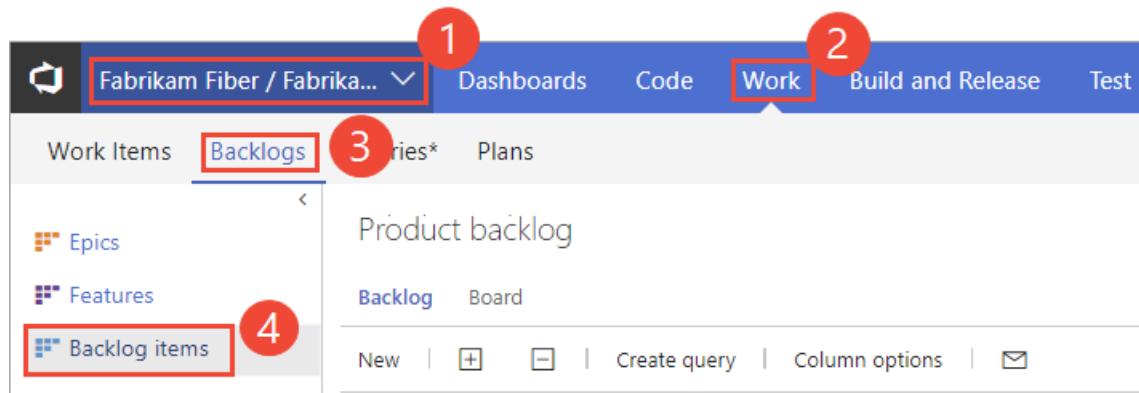


4. To view or edit a work item, select it and choose **Enter**.
5. To add a work item, choose the **+ New Work Item**, enter a title, and then press the Enter key or choose **Add to top**.

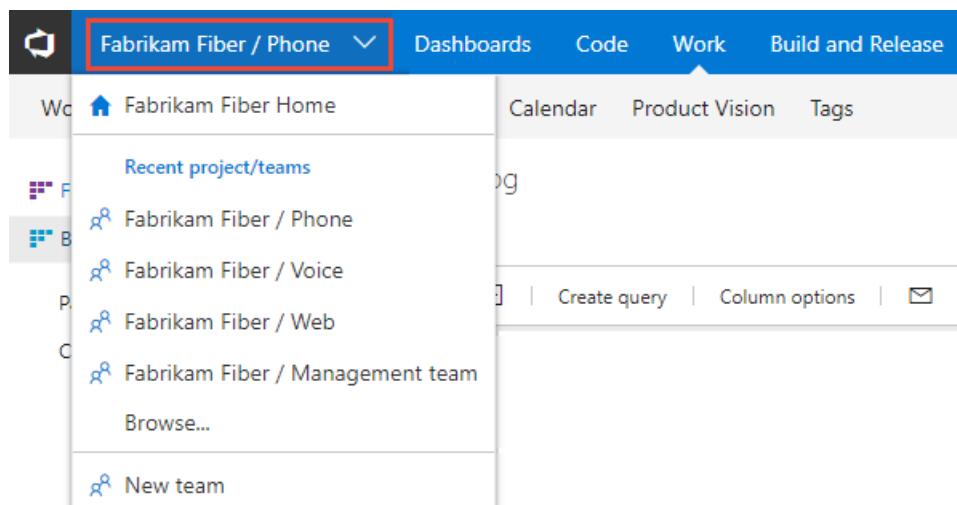


Repeat this step to capture all your ideas as work items.

1. From your web browser, open your team's product backlog. (1) Select the team from the project/team selector, choose (2) **Work**, (3) **Backlogs**, and then (4) the product backlog, which is **Backlog items** (for Scrum), **Stories** (for Agile), or **Requirements** (for CMMI).



To choose another team, open the project/team selector and select a different team or choose the **Browse** option.



2. To view or edit a work item, select it and choose **Enter**.
3. Add a work item to your backlog by entering a title and choosing **Add**. If you don't see the **Add** link, choose **New** to open the quick add panel. Repeat this step until you've captured all your main ideas.

The screenshot shows the 'Backlog items' page. At the top, there are navigation links: Backlog (selected), Board, Parents Show, In progress items Show, Mapping Off, settings icon, and a refresh icon. Below this is a toolbar with New, Create query, Column options, and a mail icon. A quick add panel is open, showing 'Type: Product Backlog Item' and a 'Title' input field. The 'Add' button in this panel is highlighted with a red box. The main area displays a table of backlog items with columns: Order, State, Effort, Title, and Tags. The items listed are:

Order	State	Effort	Title	Tags
1	● Committed	8	> 🚫 Slow response on welcome page	Web
2	● Committed	5	> 🚫 Secure sign-in	Mobile Web
3	● New	5	> 🚫 Change the initial view	Web
4	● New	3	> 🚫 Welcome back page	
5	● New	3	> 🚫 Canadian addresses don't display	RC Review

1. From your web browser, open your team's product backlog. Select **Boards > Backlogs**.

The screenshot shows the 'Backlog items' page. The navigation bar includes HOME, CODE, WORK (selected), BUILD, TEST, and RELEASE. The left sidebar shows 'Backlogs' selected, with 'Features' and 'Backlog items' under it. A tree view shows 'Current Sprint 1' and 'Future Sprint 2, Sprint 3'. The main area has a 'Backlog' tab selected. The quick add panel at the top has 'Type: Product Backlog Item' and a 'Title' input field. The 'Add' button in this panel is highlighted with a yellow box. The table below lists backlog items with columns: Backlog, Board, Forecast Off, Mapping On, Parents Hide, In progress items Show, New, Create query, Column options, and a mail icon.

2. To view or edit a work item, select it and choose **Enter**.
3. To add a work item to your backlog, enter a title and choose **Add**. If you don't see the **Add** link, choose **New** to open the quick add panel. Your items are added to the bottom of the list.

Backlog items

The screenshot shows the 'Backlog' tab in the Azure DevOps interface. At the top, there are buttons for 'New', 'Create query', 'Column options', and a mail icon. Below this is a search bar with 'Type: Product Backlog Item' and an 'Add' button (which is highlighted with a red box). The main area displays a table of backlog items:

Order	State	Effort	Title	Tags
1	● Committed	8	> 🚫 Slow response on welcome page	Web
2	● Committed	5	🚫 Secure sign-in	Mobile Web
3	● New	5	> 🚫 Change the initial view	Web
4	● New	3	🚫 Welcome back page	
5	● New	3	🚫 Canadian addresses don't display	RC Review

Repeat this step until you've captured all your main ideas.

Check work in progress

To view the team's progress, open the Kanban board. To view or edit a work item, choose a title and press **Enter**, or double-click the title.

1. (1) Check that you selected the right project, (2) choose **Boards > Boards**, and then (3) select the correct team from the team selector menu.

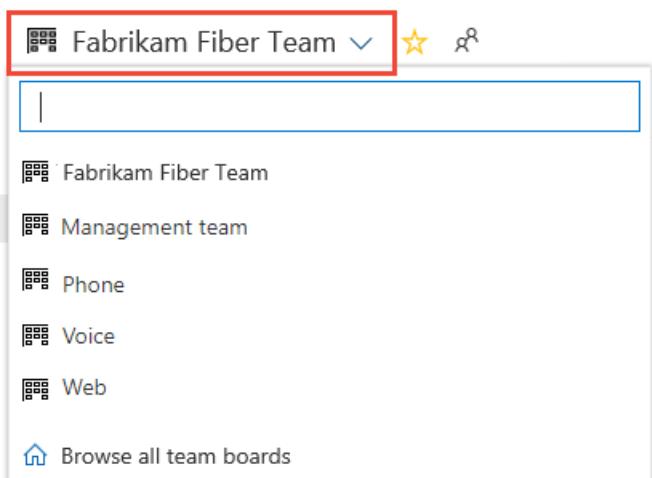
The screenshot shows the 'Boards' screen in Azure DevOps. A red box highlights the 'Boards' tab in the left sidebar (labeled 2). Another red box highlights the team selector dropdown 'Fabrikam / Fabrikam Fiber' at the top (labeled 1). A third red box highlights the 'Fabrikam Fiber Team' dropdown in the center (labeled 3). The main area shows a 'Backlog' board with several items listed:

- + New item
- Add an information form
- Raisa Pokrovskaya
- Iteration ... Sprint 3
- 0/2

On the right, there are 'Analyze' and 'Develop' sections:

- Analyze: Welcome back page, Johnnie McLeod, Iteration ... Sprint 3, 0/4, 1
- Develop: Slow form, Jam, 0/2

To choose another team's board, open the selector and select a different team or choose the [Browse all team boards](#) option. Or, you can enter a keyword in the search box to filter the list of team backlogs for the project.



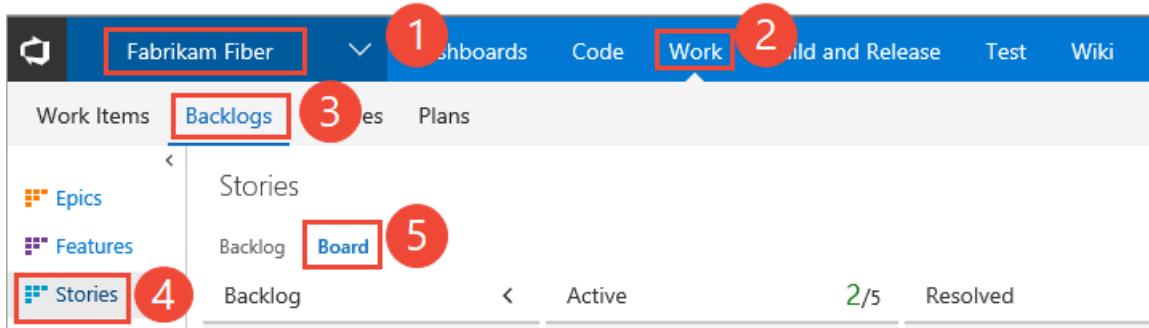
TIP

Choose the star icon to favorite a team board. Favorited artifacts (favored icon) appear at the top of the team selector list.

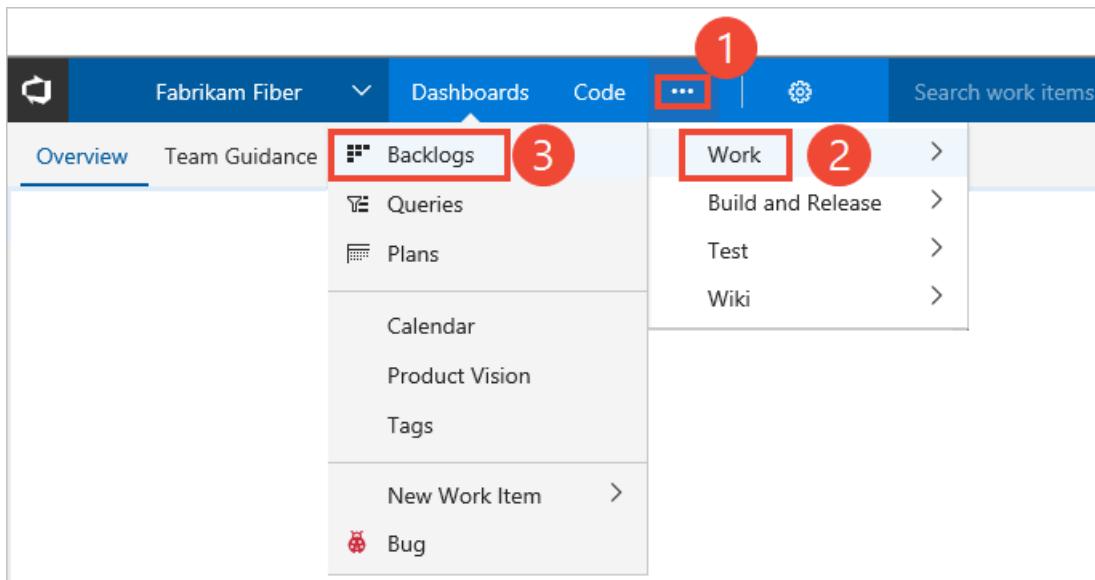
2. Check that you have selected **Backlog items** (for Scrum), **Stories** (for Agile), or **Requirements** (for CMMI) as the backlog level.



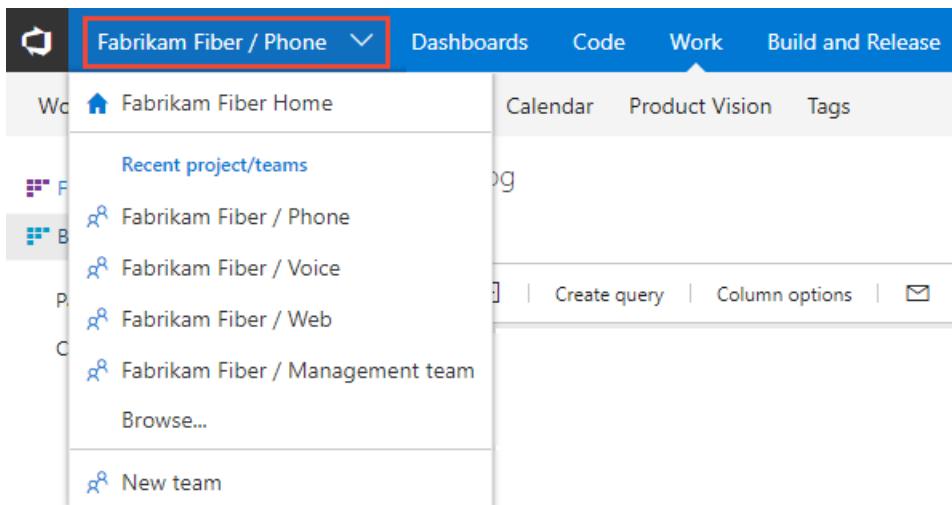
1. To view your Kanban board, open your (1) project from a web browser and choose (2) **Work**, (3) **Backlogs**, (4) **Stories**, and then (5) **Board**.



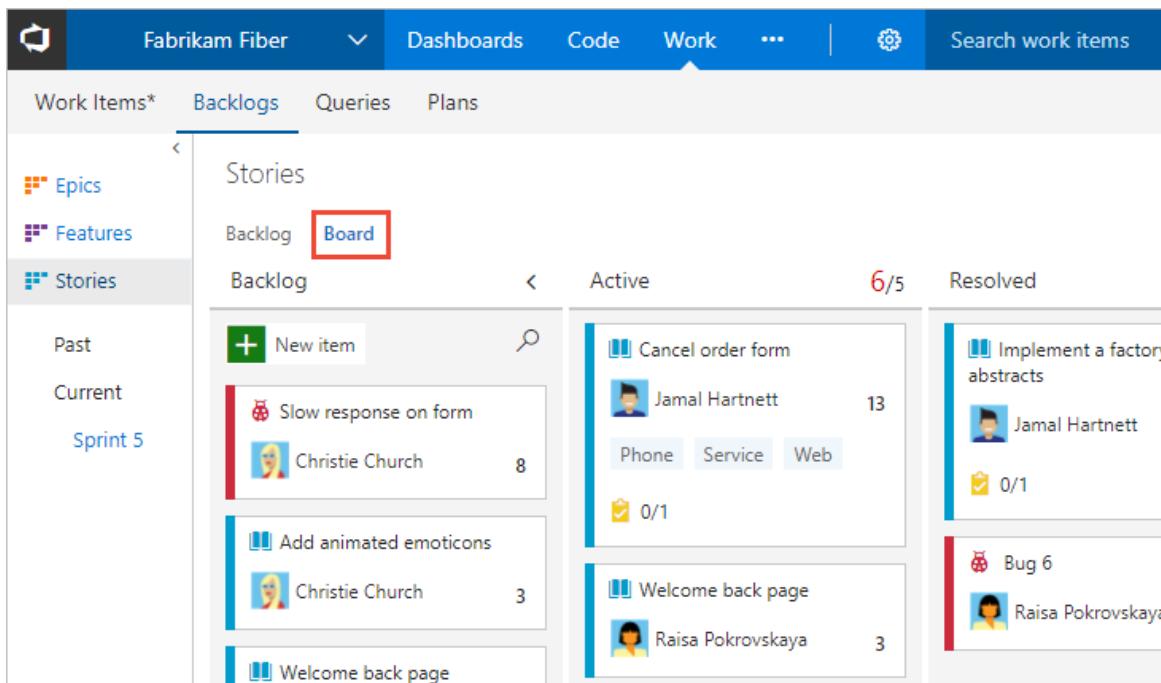
If you don't see **Work**, your screen size may be reduced. Choose the three dots (⋮), then choose **Work**, **Backlogs**, and then **Board**.



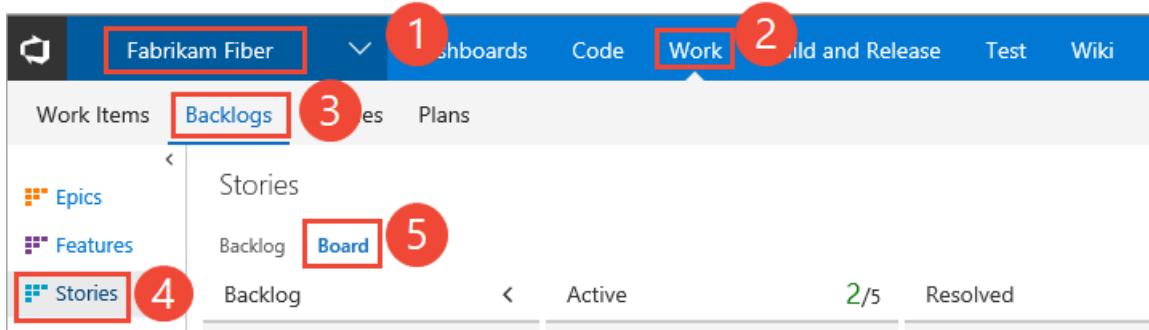
2. To choose another team, open the project/team selector and select a different team or choose the **Browse** option.



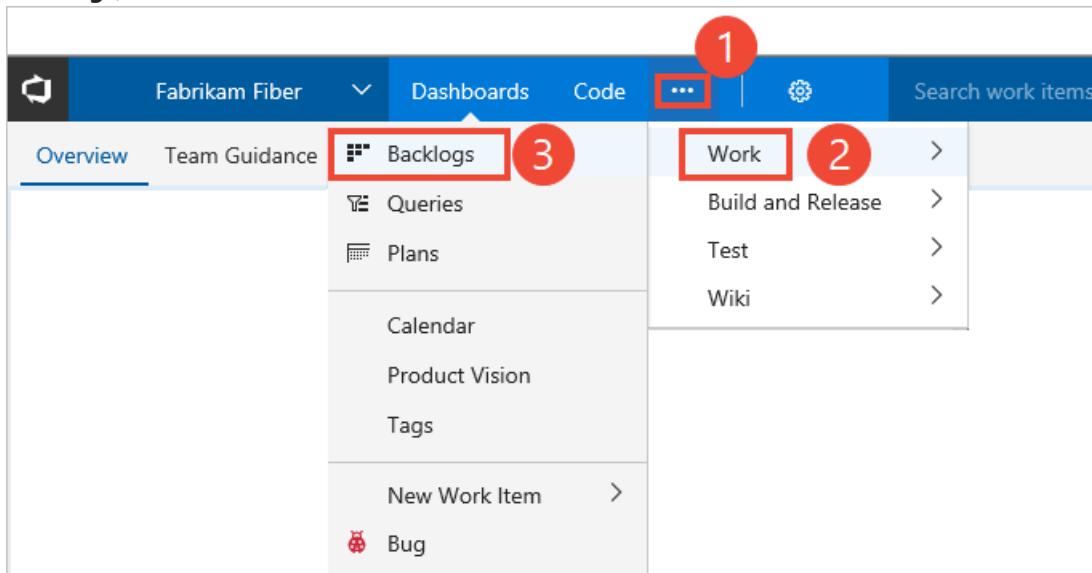
3. Your Kanban board displays.



- To view your Kanban board, open your (1) project from a web browser and choose (2) **Work**, (3) **Backlogs**, (4) **Stories**, and then (5) **Board**.



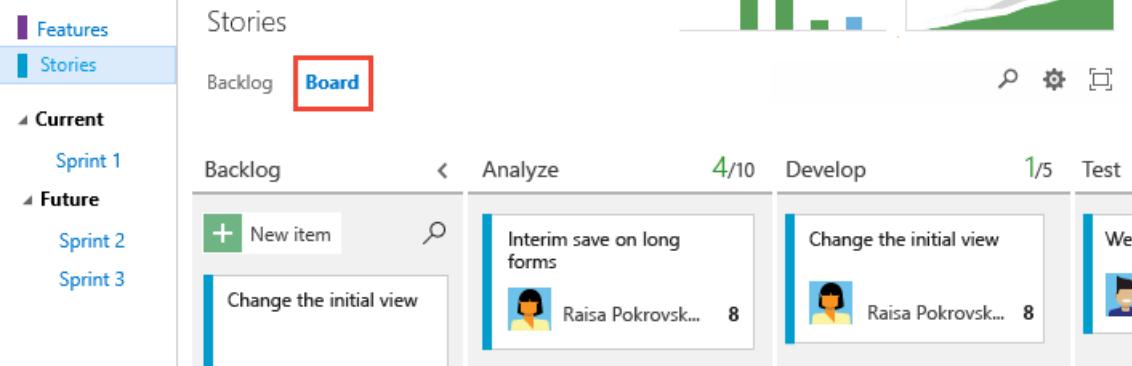
If you don't see **Work**, your screen size may be reduced. Choose the three dots (⋮), then choose **Work**, **Backlogs**, and then **Board**.



- To choose another team, open the project/team selector and select a different team or choose the **Browse** option.



- Your Kanban board displays.

[HOME](#) [CODE](#) [WORK](#) [BUILD](#) [TEST](#) [RELEASE](#)
[Backlogs](#) [Queries](#)


Stories

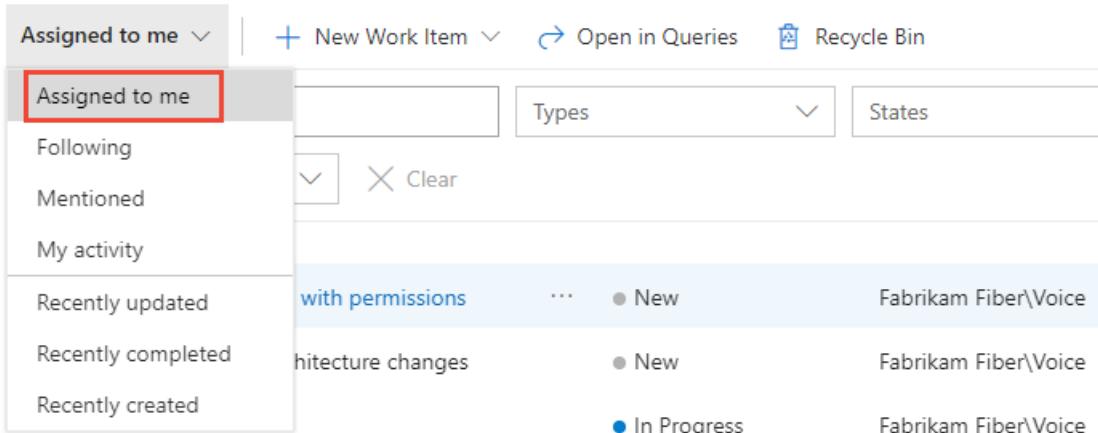
Backlog **Board**

Backlog	Analyze	Develop	Test
New item	Interim save on long forms Raisa Pokrovsk... 8	Change the initial view Raisa Pokrovsk... 8	Wel...
Change the initial view			

Find work assigned to you, or query for other work items

1. Choose **Boards>Work Items**, and then select **Assigned to me**.

Work Items



Assigned to me | [New Work Item](#) | [Open in Queries](#) | [Recycle Bin](#)

Assigned to me

- Following
- Mentioned
- My activity
- Recently updated
- Recently completed
- Recently created

with permissions

	... ● New	Fabrikam Fiber\Voice
hitecture changes	● New	Fabrikam Fiber\Voice
	● In Progress	Fabrikam Fiber\Voice

You can focus on relevant items inside a project using one of the seven pivots as described next. Additionally, you can filter and sort each pivot view. For details, see [View and add work items using the Work Items page](#).

2. To query for work items, see [View, run, or email a work item query](#).

1. Open **Work>Queries** and select **Assigned to me** to see the list of work items assigned to you.

Assigned to me

2 work items (1 sel...)

Results Editor Work item pane Bottom...

ID	Work Item Type	Title	State
190	Bug	Simplify the search experience	New
191	Bug	Log-in button needs to be more prominent	New

Bug 190: Simplify the search experience

Simplify the search experience

2. Or, open any of the queries defined in the Shared Queries folder.

Work in progress

Results Editor Column

ID	Work Item Type	State	Remaining Work
164	Task	In Progress	8
165	Task	In Progress	8
166	Task	In Progress	6
167	Task	In Progress	2
168	Task	In Progress	2
169	Task	In Progress	1
170	Task	In Progress	4
173	Task	In Progress	2
174	Task	In Progress	1.5
181	Task	In Progress	1
186	Task	In Progress	1

3. And, you can [create new queries or edit existing queries](#) and save them under My Queries folder.

New |

Assigned to me
Unsaved work items

My favorites
Drag queries here to add t...

Team favorites
Drag queries here to add t...

My Queries
Shared Queries
Current Sprint
Blocked Tasks

Work in Progress

Results **Editor** Charts

Column options Copy query URL

Type of query Flat list of work items Query across projects

Filters for top level work items

	And/Or	Field	Operator	Value
<input type="checkbox"/>	Iteration Path	Under	Fabrikam\Sprint 1	
<input type="checkbox"/>	Work Item Type	In Group	Microsoft.TaskCategory	
<input type="checkbox"/>	State	=	In Progress	
+ Add new clause				

Related articles

For a comparison chart of Stakeholder vs Basic access, see this [feature matrix](#). See also these quickstart guides:

- [Add work items](#)
- [Create your backlog](#)
- [Kanban quickstart](#)
- [Access levels](#)

If you want to provide a group of users access to provide feedback, then you don't need to give them Stakeholder access. Instead, [give reviewers permissions to provide feedback](#).

About permissions and groups

5/24/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

To access the resources you manage in Azure DevOps—such as your code, builds, and work tracking—you must have permissions for those specific resources. Most permissions are granted through built-in security groups as described in [Permissions and access](#). You can grant or deny permissions to specific users, built-in security groups, or groups defined in Azure Active Directory (Azure AD) if integrated with Azure DevOps, or Active Directory if integrated with TFS.

Permissions may apply to a specific project or objects within the project, such as Git or TFVC repositories, branches, build pipelines, area paths, and more. Or, they can apply to an entire Azure DevOps organization or TFS collection, or to a TFS instance. Each functional area uses groups to simplify management across the deployment.

You manage security groups and permissions from the web portal administration context. Permissions are automatically set based on the group that you add users to, or based on the object, project, collection, or server level to which you add groups.

Permission settings

Here's what you need to know about permission settings:

- **Allow** or **Deny** explicitly grants or restricts users from performing specific tasks, and are usually inherited from group membership.
- **Not set** implicitly denies users the ability to perform tasks that require that permission, but allows membership in a group that does have that permission set to take precedence, also known as **Allow (inherited)** or **Inherited allow** and **Deny (inherited)** or **Inherited deny**.
- For most groups and almost all permissions, **Deny** overrides **Allow**. If a user belongs to two groups, and one of them has a specific permission set to **Deny**, that user is not able to perform tasks that require that permission even if they belong to a group that has that permission set to **Allow**.

For members of the **Project Collection Administrators** or **Team Foundation Administrators** groups, Deny doesn't trump Allow. Permissions assigned to these groups take precedent over any Deny set within any other group to which that member might belong.

- Changing a permission for a group changes that permission for all users who are members of that group. In other words, depending on the size of the group, you might affect the ability of hundreds of users to do their jobs by changing just one permission. So make sure you understand the impact before you make a change.

Inheritance and security groups

Some permissions are managed through a hierarchy. Within this hierarchy, permissions can be inherited from the parent or overridden. Security groups assign a set of permissions to those members of the group. For example, members of the **Contributors** group or **Project Administrators** group are assigned the permissions that are set as **Allowed** to those groups.

If a permission isn't directly allowed or denied for a user, then it may be inherited in two ways.

- Users inherit permissions from the groups to which they belong. When a permission is allowed for a user directly or through membership in a group that has that permission, and it is denied, either directly or through group membership, the permission is denied.

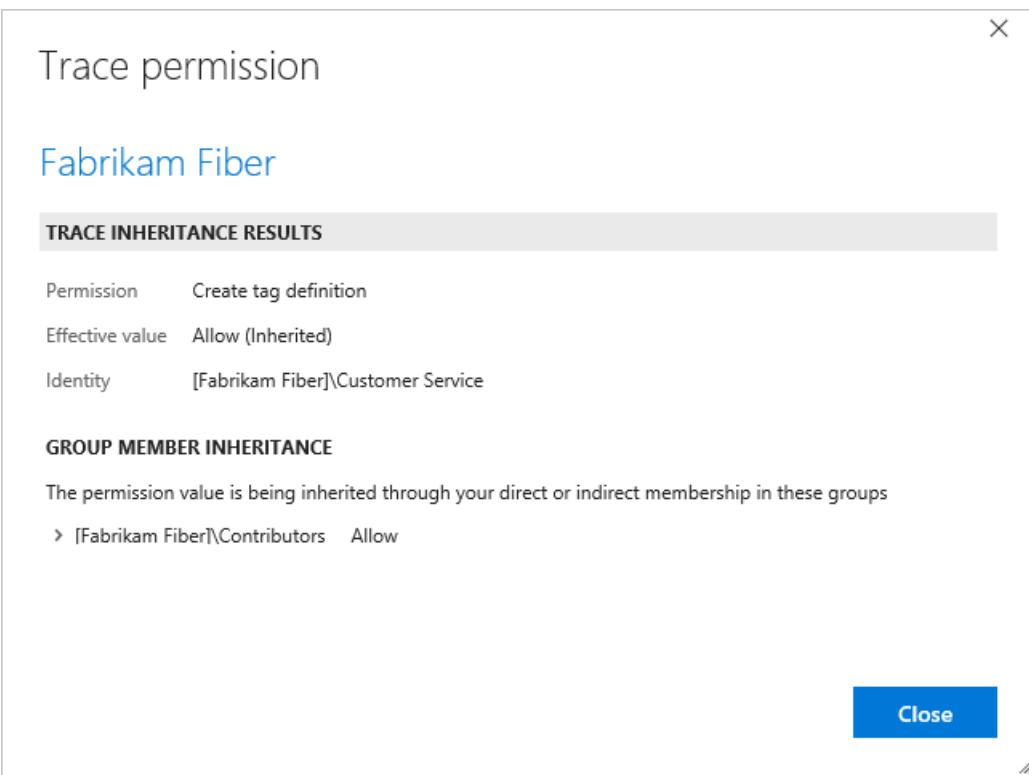
Members of **Project Collection Administrators** or **Team Foundation Administrators** retain any allowed permissions, even if they belong to other groups that deny those permissions.

- Object-level permissions that are assigned for nodes of a hierarchy - areas, iterations, version control folders, work item query folders - are inherited down the hierarchy. That is, a user's permissions that are set at `area-1` are inherited by `area-1/sub-area-1`, if the same permission is not explicitly allowed or denied for `area-1/sub-area-1`. If a permission is set explicitly for an object, like `area-1/sub-area-1`, then the parent node is not inherited, regardless of whether it is denied or allowed. If it's not set, then the permissions for that node are inherited from the closest ancestor that has the permission explicitly set.

To understand why a permission is inherited, you can pause over a permission setting, and then choose **Why?** To open a **Security** page, see [View permissions](#).

	Permissions	Members	Member of
Create tag definition	Allow (inherited)		Why?
Create test runs	Allow (inherited)		
Delete and restore work items	Not set		
Delete team project	Not set		
Delete test runs	Allow (inherited)		
Edit project-level information	Not set		
Manage project properties	Not set		
Manage test configurations	Allow (inherited)		
Manage test environments	Allow (inherited)		
Move work items out of this project	Not set		
Permanently delete work items	Not set		
Rename team project	Not set		
View project-level information	Allow (inherited)		
View test runs	Allow (inherited)		
Clear explicit permissions			

A new window opens that shows the inheritance information for that permission.



Control Panel > CSI > Fabrikam Fiber

Overview Iterations Areas Security Alerts Version Control

Groups Users OneView > Contributors Edit... ▾

Create TFS group

Search...

Members Member of

Members of this group can add, modify, and delete items within the team project.

Permission	Action	Reason
Create tag definition	Inherited allow	I Why?
Create test runs	Allow	
Delete team project	Deny	

VSC Groups

- Build Administrators
- Contributors

Some object level Security dialog boxes provide an Inheritance on/off option. Use this option to disable inheritance for folders, shared queries, and other objects.

PERMISSIONS FOR SHARED QUERIES/FABRIKAMFIBER

Owner Antonia Branch

Add... Inheritance ▾

Search On Off

Project Build Administrators Contributors Project Administrators Readers

ACCESS CONTROL SUMMARY

Shows information about the permissions being granted to this identity

Permission	Inheritance Status
Contribute	Inherited allow
Delete	Inherited allow
Manage Permissions	Inherited allow
Read	Inherited allow

Clear explicit permissions Remove Save changes Undo changes

Close

When assigning permissions

Do:

- Use Windows groups when managing lots of users.

- Consider granting the [work item query folders](#) **Contribute** permission to users or groups that require the ability to create and share work item queries for the project.
- When adding many teams, consider creating a **Team Administrators** custom group where you allocate a subset of the permissions available to **Project Administrators**.
- When adding teams, consider what permissions you want to assign to team leads, scrum masters, and other team members who may need to create and modify area paths, iteration paths, and queries.

Don't:

- Don't add users to the project **Readers** group that you've added to the **Project Administrators** group. Because the Readers group denies several permissions that the Project Administrators group allows, and deny takes precedence.
- Don't change the default assignments made to the valid users groups. If you remove or set the **View instance-level information** permission to Deny for one of the Valid Users groups, no users in the group are able to access the project, collection, or deployment, depending on the group you set.
- Don't assign permissions that are noted as 'Assign only to service accounts' to user accounts.

Permissions versus access levels

Permissions are different from access levels. Access levels control what features are visible to users in the web portal, and are dependent on user licenses; permissions control a user's ability to use web portal features. If you're just trying to give someone access to a team room or to Agile portfolio management and test case management features, you'll want to [change access levels](#), not permissions.

Setting the access level for users or groups doesn't provide them access to a project or the web portal. Only users or groups added to a team or security group can connect to a project and the web portal. Make sure your users have both the permissions and the access level they need. You do this by making sure they're [added to the project or a team](#).

Manage large numbers of users

If you need to set permissions for large numbers of users, create a group in Windows, Active Directory, or Azure Active Directory, add these groups to a default or custom security group, and add the same groups to grant access to additional resources.



Of course, you don't need to grant permissions for reports or the project portal if your project doesn't use SQL Server Reporting Services or a SharePoint site.

Valid user groups

When you add accounts of users directly to a built-in group or through a Windows group, they are automatically added to one of the valid user groups.

- Server\Team Foundation Valid Users*: All members added to server-level groups.
- ProjectCollectionName\Project Collection Valid Users*: All members added to collection-level groups.
- TeamProjectName\Project Valid Users*: All members added to project-level groups.

The default permissions assigned to these groups are primarily limited to read access, such as **View build resources**, **View project-level information**, and **View collection-level information**.

This means that all users that you add to one project can view the objects in other projects within a collection. If

you need to restrict view access, then you can [set restrictions through the area path node](#).

If you remove or deny the **View instance-level information** permission for one of the Valid Users groups, no users in the group are able to access the project, collection, or deployment, depending on the group you set.

Tools used to set permissions

You set most permissions through the web portal. You can use the tools listed in the following table to set permissions. Different tools are used depending on whether you are setting permissions at a server, collection, or project level. You use the [web portal administration context](#) to set most permissions.

PERMISSION LEVEL	WEB PORTAL SECURITY PAGES	TEAM FOUNDATION ADMINISTRATION CONSOLE	TFSSecurity COMMAND-LINE TOOL	TF COMMAND-LINE TOOL	TFSLABCONFIG COMMAND-LINE TOOL
Server-level		✓	✓		
Collection-level	✓	✓	✓		
Project and test level	✓		✓		
Build level	✓		✓		
Git repository	✓			✓	
Team Foundation Version Control	✓			✓	
Area level for work item tracking	✓		✓		
Iteration level for work item tracking	✓		✓		
Work item query	✓		✓		
Work item tags			✓		
Alerts			✓		
Releases	✓				
Lab Management					✓

Setting permissions for SQL Server reports

For information about how to set permissions in Reporting Services, see [Grant permissions to view or create SQL Server reports in TFS](#).

Setting permissions for SharePoint integration

For information about how to set permissions for SharePoint Products integrated with TFS, see [Set SharePoint site permissions](#).

For more information, see [Determine permission levels and groups in SharePoint 2013](#).

About security roles

6/12/2019 • 5 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

While the majority of features and functional tasks are managed by [individual permissions](#), there are several artifacts and features that the system manages through role-based permissions. You can add users or groups to a role. Each role determines the set of operations that the user can perform as described in the following sections.

Many role-based permissions can be set for all artifacts of a specific type in a project, or for the project or collection and then selectively inherited for a specific artifact. Role memberships for individual items automatically inherit those set for the project or collection. If required, you can turn off Inheritance for a specific artifact.

Agent pool security roles, project-level

You [add users to the following security roles](#) from the project-level admin context, **Agent Pools** page. For information on adding and managing agent queues, see [Agent pools](#).

ROLE (PROJECT-LEVEL)	DESCRIPTION
Reader	Can view the queue. You typically add operators to this role that are responsible for monitoring the build and deployment jobs in that queue.
User	Can use the queue when authoring build or release pipelines.
Creator	Can use the queue when authoring build or release pipelines.
Administrator	Can manage membership for all roles of the queue, as well as view and use the queues. The user that created a queue is automatically added to the Administrator role for that queue.

You control the security of all project agent pools from the **Security** tab. Role memberships for individual project agent pools automatically inherit from what those roles. By default, the following groups are added to the Administrator role of 'All agent pools': Build Administrators, Release Administrators, Project Administrators.

To manage role settings for a project agent pool, open **Project settings**, choose **Agent Pools**, choose a pool, and then add a user and select their role.

Agent pool security roles, organization or collection-level

You [add users to the following security roles](#) from the **Organization settings** or collection-level admin settings, **Agent Pools** page. For information on adding and managing agent pools, see [Agent pools and queues](#).

ROLE (ORGANIZATION-LEVEL)	DESCRIPTION
Reader	Can view the pool as well as agents. You typically add operators to this role that are responsible for monitoring the agents and their health.

ROLE (ORGANIZATION-LEVEL)	DESCRIPTION
Service Account	Can use the pool to create an agent queue in a project. If you follow the guidelines for creating new pools and queues , you typically do not have to add any members to this role.
Administrator	Can register or unregister agents from the pool and manage membership for all pools, as well as view and create pools. They can also use the agent pool when creating an agent queue in a project. The system automatically adds the user that created the pool to the Administrator role for that pool.

To manage role settings for organization or collection-level agent pools, open **Organization settings**, choose **Agent Pools**, choose a pool, and then add a user and select their role.

Deployment group security roles

You [add users to the following roles](#) from **Pipelines** or **Build and Release**. For information on adding and managing deployment groups, see [Deployment groups](#).

ROLE	DESCRIPTION
Reader	Can only view deployment groups.
Creator	Can view and create deployment groups.
User	Can view and use but cannot manage or create deployment groups.
Administrator	Can administer roles, manage, view and use deployment groups.

Deployment pool security roles

You [add users to the following roles](#) from the collection-level admin context, **Deployment Pools** page. To create and manage deployment pools, see [Deployment groups](#).

ROLE	DESCRIPTION
Reader	Can only view deployment pools.
Service Account	Can view agents, create sessions, and listen for jobs from the agent pool.
User	Can view and use the deployment pool for creating deployment groups.
Administrator	Can administer, manage, view and use deployment pools.

Library asset security roles: Variable groups and secure files

You [add users to a library role](#) from **Pipelines** or **Build and Release**. To learn more about using these library

assets, see [Variable groups and Secure files](#)

ROLE	DESCRIPTION
Administrator	Can use and manage library items.
Reader	Can only read library items.
User	Can use library items, but not manage them.

Service connection security roles

You [add users to the following roles](#) from the project-level admin context, **Services** page. To create and manage these resources, see [Service connections for build and release](#).

ROLE	DESCRIPTION
User	Can use the endpoint when authoring build or release pipelines.
Administrator	Can manage membership of all other roles for the service connection as well as use the endpoint to author build or release pipelines. The system automatically adds the user that created the service connection to the Administrator role for that pool.

Marketplace extensions

The **Manager** role is the only role used to manage the security of Marketplace extensions. Members of the Manager role can install extensions and respond to requests for extensions to be installed.

To learn more, see [Grant permissions to manage extensions](#).

Team administrator role

For [each team that you add](#), you can assign one or more team members as administrators. The team admin role isn't a group with a set of defined permissions. Instead, the team admin role is tasked with managing team assets.

For details, see [Manage teams and configure team tools](#).

NOTE

Members of the Project Administrators or Project Collection Administrators groups can manage all team admin areas for all teams.

Related articles

- [About permissions and groups](#)
- [Permissions and groups reference](#)
- [Access with Azure Active Directory \(Azure AD\)](#).

About access levels

7/10/2019 • 19 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Access levels grant or restrict access to select web portal features. This is in addition to permissions granted through security groups which provide or restrict specific tasks. Access levels enable administrators to provide their user base access to the features they need and only pay for those features.

IMPORTANT

To view the content available for your platform, make sure that you select the correct version of this article from the version selector which is located above the table of contents.

When you add a user or group to a team or project, they're automatically granted access to those features supported by the default access level and those supported by the security group to which they are added. Most users can access most features by being assigned to the **Basic** access level and **Contributors** security group. For a simplified overview of the permissions assigned to the most common groups—**Readers**, **Contributors**, and **Project Administrators**—as well as the **Stakeholder** access group, see [Permissions and access](#).

To add user accounts or groups to specific access levels, see [Manage users and access](#). Make sure to set each user's access level based on what you've purchased for that user.

To add user accounts or groups to specific access levels, see [Change access levels](#). Make sure to set each user's access level based on what you've purchased for that user.

Supported access levels

Assign users or groups of users to one of the following access levels:

- **Stakeholder:** Provides partial access, can be assigned to unlimited users for free. Assign to users with no license or subscriptions who need access to a limited set of features.
- **Basic:** Provides access to most features. Assign to users with a Visual Studio Professional or MSDN Platforms subscription, and to users for whom you are paying for Basic + Test Plans access in an organization.
- **Basic + Test Plans:** Provides access to all features included in Basic, as well as Azure Test Plans. Assign to users with an Azure DevOps Server CAL or Visual Studio Professional subscription, and to users for whom you're paying for Basic access in an organization.
- **Visual Studio subscription:** 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 that are included in their subscription level. If you assign Basic or Stakeholder, they also receive their Visual Studio subscription benefits upon sign-in.

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 & 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning tools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced home page Includes access to projects , work items , and pull requests defined across projects you work in	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced portfolio management Includes full access to define features and epics from a portfolio backlog or Kanban board	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile boards Includes limited access to Kanban boards . Stakeholders can't add work items, can't drag-and-drop work items to update status, and can't update fields displayed on cards.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile Portfolio Management Includes limited access to portfolio backlogs and Kanban boards . Stakeholders can't change the backlog priority order, and can't assign items to an iteration, use the mapping pane, or exercise forecasting.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analyze test results and manage machine groups Includes tracking test status and testing different configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Artifacts Includes full access to all Azure Artifacts features (previously referred to as package management), up to 2GB free	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Author Release Pipelines and Manage Releases Includes defining release pipelines and multi-stage continuous deployment (CD) pipelines , and using approvals and gates to control deployments ; when the Free access to Pipelines Preview feature is enabled , Stakeholders gain access to all Azure Pipelines features.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Build Includes full access to all features to manage continuous integration and continuous delivery of software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chart Authoring Can create work tracking query charts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Chart Viewing Can only view work tracking query charts. Stakeholders can't view query charts from the Queries page, however can view them when added to a dashboard.		<input type="checkbox"/>	<input type="checkbox"/>
Code Includes full access to all features to manage code using Git repositories or using Team Foundation Version Control (TFVC)		<input type="checkbox"/>	<input type="checkbox"/>
Delivery Plans Includes full access to add and view Delivery plans.		<input type="checkbox"/>	<input type="checkbox"/>
Request and Manage Feedback Includes full access to request and manage feedback on working software.		<input type="checkbox"/>	<input type="checkbox"/>
Standard Features Includes working across projects , View dashboards , View wikis , Manage personal notifications . Stakeholders can't view markdown README files defined for repositories and can only read wiki pages.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Test services in build and release Includes running unit tests with your builds , reviewing and analyzing test results		<input type="checkbox"/>	<input type="checkbox"/>
Test summary access to Stakeholder license Includes performing user acceptance testing and requesting Stakeholder feedback using the Test & Feedback extension	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View Releases and Manage Approvals Includes viewing releases and approving releases ; when the Free access to Pipelines Preview feature is enabled , Stakeholders gain access to all Azure Pipelines features.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web-based Test Case Management Includes adding test plans and test suites , creating manual test cases , and deleting test artifacts			<input type="checkbox"/>
Web-based Test Execution Includes running manual and automated tests		<input type="checkbox"/>	<input type="checkbox"/>

- **Stakeholder:** Provides partial access, can be assigned to unlimited users for free. Assign to users with no license or subscriptions who need access to a limited set of features.
- **Basic:** Provides access to most features. Assign to users with an Azure DevOps Server CAL, with a Visual Studio Professional subscription, and to users for whom you're paying for Basic access in an organization.
- **Basic + Test Plans:** Provides access for users who have a monthly Test Manager subscription, Visual Studio Test Professional, or MSDN Platforms subscription.
- **VS Enterprise:** Provides access to premium features. Assign to users with a subscription to Visual Studio Enterprise.

The following table indicates those features available for each supported access level.

FEATURE	STAKEHOLDER	BASIC	BASIC + TEST PLANS & VS ENTERPRISE
Administer organization Can configure resources when also added to a security group or role: team administrator, Project Administrator, or Project Collection Administrator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning tools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced home page Includes access to projects, work items, and pull requests defined across projects you work in	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced portfolio management Includes full access to defining features and epics from a portfolio backlog or Kanban board	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile boards Includes limited access to Kanban boards . Stakeholders can't add work items, can't drag-and-drop work items to update status, and can't update fields displayed on cards.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile Portfolio Management Includes limited access to portfolio backlogs and Kanban boards . Stakeholders can't change the backlog priority order, and can't assign items to an iteration, use the mapping pane, or exercise forecasting.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analyze test results and manage machine groups Includes tracking test status and testing different configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Artifacts Includes full access to all Azure Artifacts features (also referred to as package management), up to 2GB free	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Author Release Pipelines and Manage Releases Includes defining release pipelines and multi-stage continuous deployment (CD) pipelines , and using approvals and gates to control deployments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Build Includes full access to all features to manage continuous integration and continuous delivery of software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chart Authoring Can create work tracking query charts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Chart Viewing Can only view work tracking query charts; Stakeholders can't view query charts from the Queries page, however can view them when added to a dashboard.		<input type="checkbox"/>	<input type="checkbox"/>
Code Includes full access to all features to manage code using Git repositories or using Team Foundation Version Control (TFVC)		<input type="checkbox"/>	<input type="checkbox"/>
Delivery Plans Includes full access to add and view Delivery plans.		<input type="checkbox"/>	<input type="checkbox"/>
Request and Manage Feedback Includes full access to request and manage feedback on working software.		<input type="checkbox"/>	<input type="checkbox"/>
Standard Features Includes working across projects , View dashboards , View wikis , Manage personal notifications ; Stakeholders can't view markdown README files defined for repositories and can only read wiki pages.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Test services in build and release Includes running unit tests with your builds , reviewing and analyzing test results		<input type="checkbox"/>	<input type="checkbox"/>
Test summary access to Stakeholder license Includes performing user acceptance testing and requesting Stakeholder feedback using the Test & Feedback extension	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View My Work Items Includes limited 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).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View Releases and Manage Approvals Includes viewing releases and approving releases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web-based Test Case Management Includes adding test plans and test suites , creating manual test cases , and deleting test artifacts			<input type="checkbox"/>
Web-based Test Execution Includes running manual and automated tests		<input type="checkbox"/>	<input type="checkbox"/>
Microsoft published Azure DevOps Extensions			<input type="checkbox"/>

- **Stakeholder:** Provides partial access, can be assigned to unlimited users for free. Assign to users with no license or subscriptions who need access to a limited set of features.
- **Basic:** Provides access to most features. Assign to users with a CAL or with a Visual Studio Professional subscription.
- **Advanced** (legacy access level, deprecated in Azure DevOps Server 2019): Provides access to premium features. Only assign to users with a subscription to MSDN Platforms or Visual Studio Test Professional.
- **VS Enterprise:** Provides access to premium features. Assign to users with a subscription to Visual Studio Enterprise.

- **Stakeholder**: Provides partial access, can be assigned to unlimited users for free. Assign to users with no license or subscriptions who need access to a limited set of features.
- **Basic**: Provides access to most features. Assign to users with a CAL or with a Visual Studio subscription.
- **Advanced** (TFS 2017): Provides access to premium features. Only assign to users with a subscription to MSDN Platforms or Visual Studio Test Professional.
- **VS Enterprise** (TFS 2017.1 and later versions): Provides access to premium features. Assign to users with a subscription to Visual Studio Enterprise.

The following table indicates those features available for each supported access level.

FEATURE	STAKEHOLDER	BASIC	ADVANCED & VS ENTERPRISE
Administer organization Can configure resources when also added to a security group or role: team administrator, Project Administrator, or Project Collection Administrator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning tools	<input type="checkbox"/>	<input type="checkbox"/>	
Advanced home page Includes access to projects , work items , and pull requests defined across projects you work in	<input type="checkbox"/>	<input type="checkbox"/>	
Advanced portfolio management Includes full access to defining features and epics from a portfolio backlog or Kanban board	<input type="checkbox"/>	<input type="checkbox"/>	
Agile boards Includes limited access to Kanban boards . Stakeholders can't add work items, can't drag-and-drop work items to update status, and can't update fields displayed on cards.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile Portfolio Management Includes limited access to portfolio backlogs and Kanban boards . Stakeholders can't change the backlog priority order, and can't assign items to an iteration, use the mapping pane, or exercise forecasting.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analyze test results and manage machine groups Includes tracking test status and testing different configurations	<input type="checkbox"/>	<input type="checkbox"/>	
Artifacts Includes full access to all Azure Artifacts features (also referred to as package management), up to 2GB free		<input type="checkbox"/>	
Author Release Pipelines and Manage Releases Includes defining release pipelines and multi-stage continuous deployment (CD) pipelines , and using approvals and gates to control deployments	<input type="checkbox"/>	<input type="checkbox"/>	
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.	<input type="checkbox"/>	<input type="checkbox"/>	
Build Includes full access to all features to manage continuous integration and continuous delivery of software	<input type="checkbox"/>	<input type="checkbox"/>	

Chart Authoring Can create work tracking query charts	<input type="checkbox"/>	<input type="checkbox"/>	
Chart Viewing Can only view work tracking query charts; Stakeholders can't view query charts from the Queries page, however can view them when added to a dashboard.	<input type="checkbox"/>	<input type="checkbox"/>	
Code Includes full access to all features to manage code using Git repositories or using Team Foundation Version Control (TFVC)	<input type="checkbox"/>	<input type="checkbox"/>	
Delivery Plans Includes full access to add and view Delivery plans.	<input type="checkbox"/>	<input type="checkbox"/>	
Request and Manage Feedback Includes full access to request and manage feedback on working software.	<input type="checkbox"/>	<input type="checkbox"/>	
Standard Features Includes working across projects , View dashboards , View wikis , Manage personal notifications . Stakeholders can't view markdown README files defined for repositories and can only read wiki pages.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Team rooms Requires TFS 2017 or earlier versions. Deprecated for TFS 2018 and later versions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Test summary access to Stakeholder license Includes performing user acceptance testing and requesting Stakeholder feedback using the Test & Feedback extension	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View My Work Items Includes limited 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).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View Releases and Manage Approvals Includes viewing releases and approving releases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web-based Test Case Management Includes adding test plans and test suites , creating manual test cases , and deleting test artifacts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web-based Test Execution Includes running manual and automated tests	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- **Stakeholder/Limited:** Provides partial access, can be assigned to unlimited users for free. Assign to users with no license or subscriptions who need access to a limited set of features.
- **Basic/Standard:** Provides access to most features. Assign to users with a CAL or with a Visual Studio subscription.
- **Advanced/Full:** Provides access to premium features. Assign to users with a subscription to Visual Studio Enterprise, Visual Studio Test Professional or MSDN Platforms.

The following table indicates those features available for each supported access level.

FEATURE	STAKEHOLDER (LIMITED)	BASIC (STANDARD)	ADVANCED (FULL)
Administer organization Can configure resources when also added to a security group or role: team administrator, Project Administrator, or Project Collection Administrator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning features.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced home page Includes access to projects, work items, and pull requests defined across projects you work in	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile boards Includes limited access to Kanban boards . Stakeholders can't add work items and can't drag-and-drop work items to update status.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agile Portfolio Management Includes full access to portfolio backlogs and Kanban boards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Build Includes full access to all features to manage continuous integration and continuous delivery of software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chart Authoring Can create work tracking query charts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chart Viewing Can only view work tracking query charts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Code Includes full access to all features to manage code using Git repositories or using Team Foundation Version Control (TFVC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request and Manage Feedback Includes full access to request and manage feedback on working software.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standard Features Includes working across projects , viewing dashboards , and managing personal notifications ; Stakeholders have no access to repositories.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Team rooms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View My Work Items Includes limited 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).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Web-based Test Management

Includes adding and executing [test plans and test suites](#) and [manual test cases](#), and deleting [test artifacts](#)

Stakeholder access

With Stakeholder access, users can create and modify work items and create and save queries. They have limited access to many of the Azure Boards features. They also can view and approve release pipelines and perform administrative tasks when granted administrative permissions or added to an administrative group.

To get started as a Stakeholder, see [Get started as a Stakeholder](#).

Public versus private feature access

Stakeholder access grants access to features differently depending on whether you're working from a private or a public project. To learn more about public projects, see [What is a public project?](#).

SERVICE, APPLICATION, OR SETTING	PRIVATE PROJECT	PUBLIC PROJECT
Dashboards	Partial access	Full access
Wiki	Partial access	Full access
Boards	Partial access	Full access
Repos	No access	Full access
Pipelines	Full access	Full access
Test Plans	No access	No access
Notifications	Full access	Full access
Semantic search	Full access	Full access
Project settings	Partial access	Partial access
Organization settings	Partial access	Partial access

Features not available to users with Stakeholder access

If a Stakeholder needs access to one or more of the following features—which support the daily work of product owners, team leads, developers, testers, and project administrators—you need to grant them **Basic** access.

For Private projects:

- Change the priority of an item within a backlog
- Delete work items or move work items to another project
- Create shared queries, view charts, and modify the home page
- View Delivery Plans (a Marketplace extension)
- Access the full set of features under **Pipelines**, **Repos** or **Test Plans**.

For Public projects:

- View Delivery Plans (a Marketplace extension)
- Access the full set of features under **Repos** or **Test Plans**.

- Change the priority of an item within a backlog
- Delete work items or move work items to another project
- Create shared queries, view charts, and modify the home page
- View Delivery Plans (a Marketplace extension)
- Access the full set of features under **Pipelines, Repos** or **Test Plans**.

- Change the priority of an item within a backlog
- Delete work items
- Create shared queries, view charts, and modify the home page
- View Delivery Plans (a Marketplace extension)
- Access the full set of features under **Code, Build and Release** or **Test**.

- Change the priority of an item within a backlog
- Delete work items
- Create shared queries, view charts, and modify the home page
- View Delivery Plans (a Marketplace extension)
- Access the full set of features provided under **Code, Build and Release** or **Test**
- Participate in team rooms, which capture interactive, detailed conversations about the project.

NOTE

Stakeholders that choose a feature that's not available to them receive an error message indicating that they don't have permissions to complete the task.

Visual Studio subscription access

Visual Studio subscribers are entitled to **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 that are included, based on their subscription level.

VS Enterprise access

Visual Studio Enterprise subscribers are entitled to **VS Enterprise** access as a subscriber benefit. When you add those users, be sure to assign them the **VS Enterprise** access level.

With VS Enterprise access, users have access to any fee-based, Marketplace extension published by Microsoft Marketplace extension published by Microsoft that is included for active Visual Studio Enterprise subscribers.

For TFS 2017.2 and later versions, assign **VS Enterprise** to those users for whom you've purchased Visual Studio Enterprise. These include a TFS CAL plus the rights to access VS Enterprise features. (For users with MSDN Platforms subscriptions or Test Professional, assign the Basic access level and the Test Manager extension for Azure Test Plans.) To learn more, see [Assign paid extension access to users](#). For example, for users with Visual Studio Test Professional or Visual Studio Enterprise, assign them [access to the Test Manager extension for Azure Test Plans](#).

Advanced access

Users assigned Advanced access can manage test cases when you have [purchased the Test Manager extension](#) for Azure Test Plans and assigned to the user accounts to gain full access to [Web-based test case management tools](#).

Users assigned Advanced access have all the Basic features, plus [web-based test case management tools](#). You can [buy monthly access](#) or add users who already have a Visual Studio Test Professional with MSDN or MSDN Platforms subscription.

For TFS 2017 and earlier versions, you should assign the **Advanced** level to those users for whom you've purchased the full Test feature set. Here are the purchasing options:

- Higher-level Visual Studio subscriptions: Visual Studio Test Professional, Visual Studio Enterprise, or MSDN Platforms subscriptions. These include a TFS CAL plus the rights to access the full set of Test features.
- A paid Azure DevOps user (which includes a TFS CAL) plus the [Test Manager extension](#).

For TFS 2017.2, Assign **Advanced** access to those users for whom you've purchased MSDN Platforms or Visual Studio Test Professional subscriptions. These include a TFS CAL plus the rights to access Test Manager. To learn more, see [Get extensions for TFS, Assign paid extension access to users](#).

NOTE

With TFS 2017.1, the Advanced access level was temporarily disabled. Updating to TFS 2017.2 re-enables it. If you are on TFS 2017.1 and have users with Visual Studio Test Professional or MSDN Platforms subscriptions, you should assign them Basic access. In addition, you need to open **Users** for the project collections in which they are a member and [assign them the Test Manager extension for Azure Test Plans](#). To learn more, see [Buy access to TFS or TFS Test](#).

What features are available to users who are added to two different access levels?

If a user belongs to a group that has **Basic** access and another group that has **VS Enterprise** access, the user has access to all features available through **VS Enterprise**, which is a superset of **Basic**.

Service account access

Azure DevOps Server [service accounts](#) are added to the default access level. If you make Stakeholder the default access level, you must add the service accounts to Basic or Advanced/VS Enterprise access.

Service accounts don't require a CAL or other purchase.

Related articles

- [Free access to Pipelines Preview](#)
- [Manage users and access](#)
- [Export a list of users and their access levels](#)
- [Default permissions and access](#)
- [Change access levels](#)
- [Export a list of users and their access levels](#)
- [Default permissions and access](#)
- [Compare features between plans](#)

Access your organization with Azure Active Directory

4/5/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to authenticate users and control access to your organization the same way that you can with Microsoft services like Office 365 and Azure. If your organization was created with a Microsoft account, you can connect your organization to your [Azure Active Directory \(Azure AD\)](#). You can then sign in to Azure DevOps with the same username and password that you use with these Microsoft services. You can also enforce policies for accessing your team's critical resources and key assets.

To use existing on-premises identities with Azure DevOps, you can integrate directories with Azure AD by using [Azure AD Connect](#). To switch your organization to another directory, learn [how to change your directory in Azure AD](#).

How does Azure Active Directory control access to Azure DevOps?

Your organization authenticates users through your organization's directory so that only users who are members or guests in that directory can get access to your organization. When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials. Only specific [Azure AD administrators](#) can manage users in your directory, so they control who can get access to your organization.

Without Azure AD, you're solely responsible for controlling organization access. And all users must sign in with Microsoft accounts.

What do I need to set up an existing Azure DevOps instance with Azure AD?

You need the following:

- [Ownership of the organization](#) that you want to connect to Azure AD.
- A "full" Azure subscription, such as a [Pay-As-You-Go subscription](#), associated with Azure Active Directory and at least co-administrator permissions for your subscription.

You need both to make your directory appear in the Azure portal, so that you can link your subscription and connect Azure AD to your organization. Learn about [Azure subscription co-administrator permissions](#).

[Want to use Office 365 Azure AD with Azure DevOps?](#)

- Global administrator permissions for your directory so you can add current Azure DevOps users to that directory.

Otherwise, work with your directory's global administrator to add users. Learn more about [Azure AD administrators](#).

To check your permissions, [sign in to the Azure portal](#) with your work or school account. Go to your directory.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various options like 'Create a resource', 'All services', 'FAVORITES', 'Resource groups', 'Dashboard', 'All resources', 'App Services', 'Function Apps', 'SQL databases', and 'Azure Cosmos DB'. The 'Azure Active Directory' option is selected and highlighted with a red box. The main content area is titled 'Fabrikam - Overview' under 'Azure Active Directory'. It features a 'Sign-ins' section with a note that only global administrators, security administrators, security readers, and report readers can view sign-ins, followed by a 'More info' link. Below that, it shows 'Your role Global administrator'. To the right, there's a 'Find' section with a dropdown set to 'Users' and a 'Search' input field. A red box also highlights the 'Your role' section in the main content area.

You must add your Microsoft account to Azure AD.

Although directory membership isn't required to connect your organization to Azure AD, it makes sure that you can sign in and access your organization after you connect to Azure AD. Otherwise, your Microsoft account does not have access to your organization.

What happens to current users?

Your work in Azure DevOps is associated with your sign-in address. After your organization is connected to your directory, users continue working seamlessly if their sign-in addresses appear in the connected directory. If their sign-in addresses don't appear, you must [add those users to your directory](#). Your organization might have policies about adding users to the directory, so find out more first.

What if we can't use the same sign-in addresses?

You have to add these users to the directory with new work or school accounts. If they have existing work or school accounts, they can use those instead. Their work won't be lost and stays with their current sign-in addresses. You must add them as new users, reassign access levels, and readd them to any projects. Users can migrate work that they want to keep, except for their work history. Learn [how to manage organization users](#).

What happens to tools that use my credentials, like alternate credentials?

Alternate credentials won't work anymore for tools that run outside a web browser, like the Git command-line tool. You have to [set up your credentials](#) again for the organization that you connected.

What if I accidentally delete a user in Azure AD?

You should [restore the user](#), rather than create a new one. If you create a new user, even with the same email address, this user is not associated with the previous identity.

Manage organization access with Azure AD

- Add Azure DevOps users to Azure AD
- Connect your organization to Azure AD
- Disconnect your organization from Azure AD

- Delete users from Azure DevOps connected to Azure AD

Add users to your organization or project

6/26/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Learn how to add users to your organization, and specify the level of features they can use, such as Basic or Stakeholder. The following types of users can join your organization for free:

- Five users who get [Basic features](#), such as version control, tools for Agile, Java, build, release, and more
- Unlimited users who get [Stakeholder features](#), such as working with your backlog, work items, and queries
- Unlimited [Visual Studio subscribers](#) who also get Basic features. Additional features, such as [Azure Test Plans](#), can be assigned to users by access level, Basic + Test Plans.

[Need more users with Basic features?](#)

How access differs from permissions

Features that are available to users are controlled by access levels - the full set of organization resources that a user is entitled to access. Permissions control which of these organization resources the user can act on. To learn more, see [Default permissions and access for Azure DevOps](#).

Prerequisites

You must have project collection administrator or owner permissions in Azure DevOps. For more information, see [Set permissions at the project level or project collection level](#).

Add users to your organization

Administrators can now add users to an organization, grant access to appropriate tooling extensions and service access level, and add users to groups all in one view. You can add up to 50 users at once. You can add more than 50 users by repeatedly using this Users view. When you add users, each receives a notification email with a link to the organization page.

NOTE

If you have an Azure Active Directory (Azure AD)-backed organization, and you need to add users who are external to Azure AD, first [add external users](#). On the **Tell us about this user page**, under **Type of user**, be sure to choose **User with an existing Microsoft account**. After you complete those steps, use the following steps to add the Azure AD user to Azure DevOps.

- [Portal](#)
- [Azure DevOps CLI](#)

To give other users access to your organization, add their email addresses.

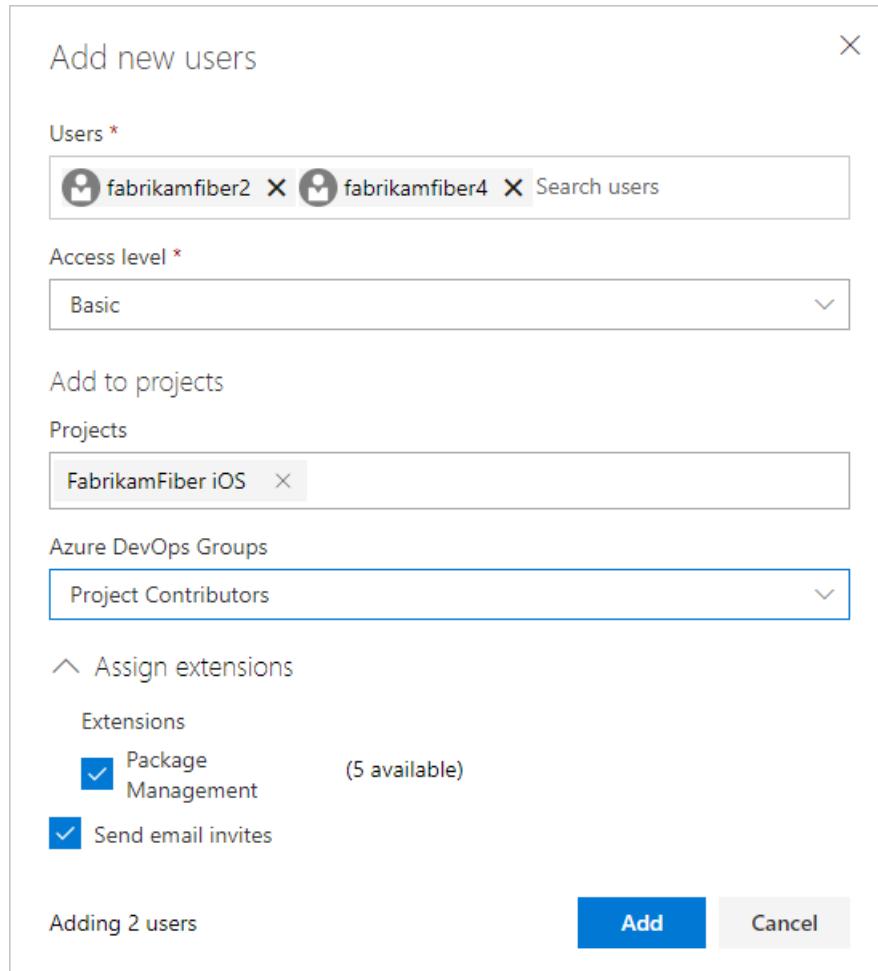
1. Sign in to your organization (<https://dev.azure.com/{yourorganization}>).
2. Select  **Organization settings**.

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled "My organizations" with four items: "FabrikamFiber" (selected), "P [redacted]", "fabrikamfib", and "fabrikamfiber4". Below this is a "New organization" button and an "Organization settings" button, which is highlighted with a red box. The main area is titled "FabrikamFiber" and contains three project cards: "Fabrikam Fiber" (blue card with FF logo), "Fabrikam" (dark green card with F logo), and "FabrikamFiber4.0" (purple card with F logo). At the bottom of the main area, there's a link "All projects".

3. Select **Users**, and then select **Add new users** to open the form.

The screenshot shows the "Manage users" page under the "General" section. The left sidebar has "Users" selected. The main area has tabs "All users" (selected), "Group rules*", "Summary", and "Export users". Below these are filters for "Name" and "Access Level", and buttons for "Clear" and "Extensions". A table lists users, with one row for "Christie Church" (fabrikamfiber1@hotmail.com) shown. To the right of the table is a "...". At the top right of the main area is a "Add new users" button, which is highlighted with a red box.

4. Enter information into the form.



- **Users:** Enter the Microsoft account's email address for the user organization.
- **Access level:** Leave the access level at **Basic** for users who contribute to the code base. To learn more, see [About access levels](#).
- **Add to projects:** Select the project that you named in the previous procedure.
- **Groups:** Leave this entry at Project Contributors, the default security group for people who contribute to your project. To learn more, see [Default permissions and access assignments](#).

5. Select **Add** to complete your invitation.

Related articles

- [Connect to a project](#)
- [Change individual permissions, grant select access to specific functions](#)
- [Grant or restrict access to select features and functions](#)
- [Delete users from Azure DevOps](#)
- [Troubleshoot adding and deleting organization users in Azure DevOps](#)
- [Troubleshoot adding members to projects in Azure DevOps](#)

Change access levels

6/13/2019 • 4 minutes to read • [Edit Online](#)

Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Users must be added to a group with the appropriate permissions, to connect and use the functions and features that Azure DevOps Server provides. To use select web portal features, they must also belong to the access level that enables access to that feature. For an overview of each access level, see [About access levels](#).

This article applies to managing access levels for project collections defined on an on-premises Azure DevOps. To manage access levels for the Azure DevOps cloud service, see [Add users to your organization or project](#). For Azure DevOps feature availability, see the [Azure DevOps Feature Matrix](#).

IMPORTANT

Make sure that you select the correct version of this article for Azure DevOps Services or Azure DevOps Server, renamed from Team Foundation Server (TFS). The version selector is located above the table of contents.

For a simplified overview of the permissions that are assigned to the most common groups—Readers, Contributors, and Project Administrators—and the Stakeholder access group, see [Permissions and access](#).

NOTE

Even if you set a user or group's access level, you must [add them to a project](#) for them to connect to a project and access features available through a supported client or the web portal.

Make sure to set each user's access level based on what you've purchased for that user. Basic access includes all Stakeholder features - Basic + Test Plans, Advanced and Visual Studio Enterprise subscriber access levels include all Basic features. In the images provided below, the circled features indicate the features made available from the previous access level.

Prerequisites

- You must be a member of the Administrators group. If you aren't a member, [get added now](#).
- If you're managing access for a large group of users, it's a best practice to first create either a [Windows group](#), [a group in Active Directory](#), or [Azure DevOps group](#), and then add individuals to those groups.

NOTE

The images you see from your web portal may differ from the images you see in this article. These differences result from updates made to your on-premises Azure DevOps. Make sure you have selected the version of this article using the content version selector. However, the basic functionality available to you remains the same unless explicitly mentioned.

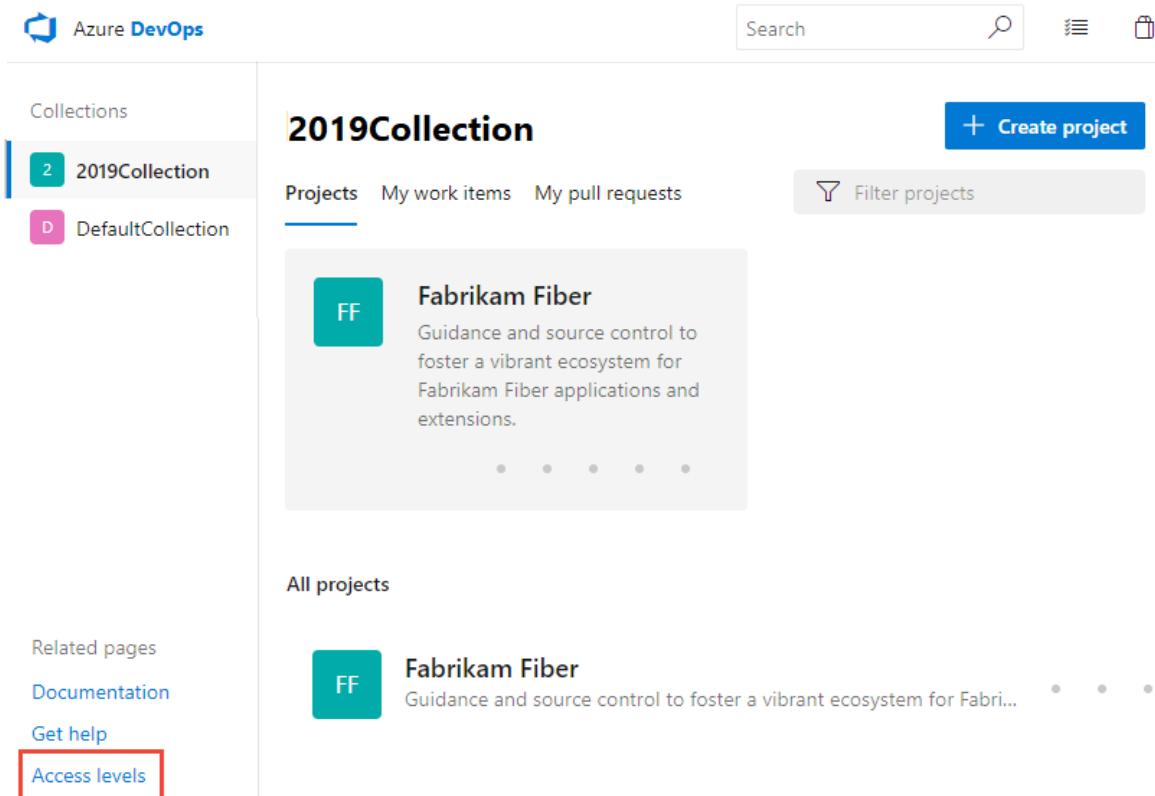
Open access levels

You manage access levels for the collections defined on the application tier. The default access level you set applies to all projects defined for all collections. Users or groups that you add to teams, projects, or collections are granted the access level that you set as the default. To change the access level for a specific group or user,

add them specifically to a non-default access level.

1. From the web portal home page for a project collection (for example,

<http://MyServer:8080/tfs/DefaultCollection/>), open **Access levels**. If you are at a project level, choose the  Azure DevOps logo and then choose **Access levels**.



The screenshot shows the Azure DevOps web interface. At the top, there's a header with the Azure DevOps logo, a search bar, and some navigation icons. On the left, a sidebar titled 'Collections' shows two items: '2019Collection' (selected) and 'DefaultCollection'. The main area is titled '2019Collection' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. A 'Create project' button is visible. Below these tabs is a card for the 'Fabrikam Fiber' project, which has a teal icon with 'FF' and a brief description. Further down, there's a section for 'All projects' with a similar card for 'Fabrikam Fiber'. On the far left of the main content area, there's a vertical list of 'Related pages' with links for 'Documentation', 'Get help', and 'Access levels', where 'Access levels' is highlighted with a red box.

If you don't see **Access levels**, you aren't an administrator and don't have permission. [Here's how to get permissions](#).

2. Select the access level you want to manage.

For example, here we choose **Basic**, and then **Add** to add a group to Basic access.

Export audit log

Stakeholder	Name	Basic
Basic (default)	Features	View My Work Items Standard Features Agile boards Basic backlog and sprint planning tools Request and Manage Feedback Agile Portfolio Management Chart Viewing Code Build Administer organization Advanced home page Advanced backlog and sprint planning tools Web-based Test Execution View Releases and Manage Approvals Author Release Pipelines and Manage Releases Advanced portfolio management Chart Authoring Analyze test results and manage machine groups Test summary access to stakeholder license usage Delivery Plans Test services in build and release
Basic + Test Plans		
VS Enterprise		

Access levels determine the features organization members have.

Set as default access level | + Add... |

Display Name Username Or Scope

No identities found in current scope.

3. Enter the name of the user or group into the text box. You can enter several identities into the text box, separated by commas. The system automatically searches for matches. Choose the matches that meet your choice.

Add users and groups

To add users or groups to this group, just type their sign-in addresses or group aliases

User or group	Chris
Christie Church fabrikamfiber1@hotmail.com	
Showing 1 result	

Save changes Cancel

4. Choose **Save changes**.

From a user context, open **Server Settings** by choosing the gear icon. The tabs and pages available differ depending on which settings level you access.

1. From the web portal home page for a project (for example,

<http://MyServer:8080/tfs/DefaultCollection/MyProject/>), open **Server settings**.

The screenshot shows the Microsoft Team Foundation Server (TFS) web interface. At the top, there's a navigation bar with items like 'Home', 'Code', 'Work', and '...'. Below the navigation bar, there's a secondary navigation menu on the right side with items such as 'Visual Studio', 'Work', 'Security', 'Alerts', 'Version Control', etc. A dropdown menu for 'Work' is open, showing options like 'Backlog', 'Board', 'Task board', and 'Queries'. The main content area on the left is titled 'Welcome' and contains four cards: 'Manage Work' (with 'Add work to your board'), 'Collaborate on code' (with 'Add code to your repository'), 'Continuously integrate' (with 'Automate your builds'), and 'Visualize progress' (with 'Learn how to add charts').

2. From **Access levels**, select the access level you want to manage. For example, here we choose **Stakeholder**, and then **Add** to add a group to Stakeholder access.

The screenshot shows the 'Access levels' page in the TFS web portal. The left sidebar has a 'Control panel' section with links like 'Export audit log', 'Stakeholder' (which is selected and highlighted), 'Basic (default)', 'Advanced', and 'VS Enterprise'. The main content area is titled 'Access levels' and shows a table for the 'Stakeholder' access level. The table has two columns: 'Name' and 'Features'. Under 'Name', it says 'Stakeholder'. Under 'Features', it lists 'View My Work Items', 'Standard Features', 'Agile boards', and 'View Releases and Manage Approvals'. Below the table, there's a note: 'Access levels determine the features account members can use through the web portal. For more information, see Access levels.' At the bottom of the page, there are buttons for 'Set as default access level', '+ Add...', 'Search', and input fields for 'Display Name' and 'Username Or Scope'. A message at the bottom states 'No identities found in current scope.'

If you don't see **Access levels**, you aren't a TFS administrator and don't have permission. [Here's how to get permissions.](#)

3. Enter the name of the user or group into the text box. You can enter several identities into the text box, separated by commas. The system automatically searches for matches. Choose the matches that meet your choice.

4. Choose **Save changes**.

1. From the web portal home page for a project (for example,

<http://MyServer:8080/tfs/DefaultCollection/MyProject/>), open administration settings.

2. From the Access levels page, select the access level you want to manage. For example, here we add a group to Stakeholder access.

If you don't see **Access levels**, you aren't an administrator and don't have permission. Learn more about [how to get permissions](#).

Change the default access level

Change the default access level to match the access you have licenses for. If you change the default access level to Stakeholder, all users not explicitly added to the Basic or an advanced level are limited to the features provided through Stakeholder access.

You set an access level from its page. Choose **Set as default access level** as shown.

Export audit log

Name	Stakeholder
Features	View My Work Items Standard Features Agile boards Basic backlog and sprint planning tools Agile Portfolio Management View Releases and Manage Approvals Test summary access to stakeholder license usage Administer organization

Access levels determine the features organization members can use through the web portal. For more information, see [About access levels](#).

Set as default access level | + Add... | |

Display Name Username Or Scope

No identities found in current scope.

Control panel

Control panel Access levels Legacy Extensions Agent pools

Export audit log

Name	Stakeholder
Features	View My Work Items Standard Features Agile boards View Releases and Manage Approvals

Access levels determine the features account members can use through the web portal. For more information, see [About access levels](#).

Set as default access level | Add... | |

Display Name Username Or Scope

No identities found in current scope.

IMPORTANT

Service accounts are added to the default access level. If you set Stakeholder as the default access level, you must add the Azure DevOps service accounts to the Basic or an advanced access level group.

Guide to features and access levels

For details on the features available to each access level, see [About access levels](#).

Related articles

- [About access levels](#)
- [Export a list of users and their access levels](#)
- [Default permissions and access](#)
- [Web portal navigation](#)

Export a list of users and their access levels

6/18/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You can get a list of users and groups that have access to your organization in Azure DevOps by exporting users. The downloaded list also indicates which access level has been granted.

You can get a list of users and groups that have access to your Azure DevOps Server instance by exporting the audit log. The audit log also indicates which access level has been granted.

You can get a list of users and groups that have access to your Team Foundation Server (TFS) instance by exporting the audit log. The audit log also indicates which access level has been granted.

Prerequisites

- You must be the organization owner or a member of the Project Collection Administrators group. If you aren't a member, get added now. See [Set permissions at the project- or collection-level](#).
- You must be a member of the Team Foundation Administrators group. If you aren't a member, get added now. See [Add administrators to TFS](#).

1. Choose the  Azure DevOps logo to open **Projects**. Then choose **Admin settings**.



2. Choose **Users**, and then **Export users**.

The screenshot shows the 'Organization Settings > Users' page. On the left, there's a sidebar with 'General' expanded, showing 'Overview', 'Projects', 'Policy', and 'Users' (which is selected and highlighted with a blue border). Below the sidebar, there are tabs for 'Security', 'Notifications', 'Extensions', and 'Usage'. The main area has a heading 'Manage users' with a search icon. Below it, there are buttons for 'All users' (which is selected), 'Group rules', 'Summary', 'Add new users', and 'Export users' (which is highlighted with a red box). There are also filters for 'Name', 'Extensions', 'Access Level', and a 'Clear' button. A table below lists two users: 'Christie Church' (fabrikamfiber1@hotmail.com) and 'Chuck Reinhart' (fabrikamfiber3@hotmail.com). Both users are listed as 'Stakeholder' with an 'Access Level' of 'Stakeholder'.

Name	Extensions	Access Level
Christie Church fabrikamfiber1@hotmail.com	...	Stakeholder
Chuck Reinhart fabrikamfiber3@hotmail.com	...	Stakeholder

You can get a list of users and groups that have accessed your Azure DevOps Server instance by exporting the audit log. The audit log also indicates which access level has been granted.

1. From the web portal home page for a project, choose the  Azure DevOps logo, (1) the project collection, and (2) **Access levels**.

The screenshot shows the Azure DevOps web portal. On the left, there's a sidebar with 'Collections' at the top, followed by two items: 'DefaultCollection' (highlighted with a red box and a red circle with the number 1) and 'TestCollection'. Below the collections are links for 'Related pages', 'Documentation', 'Get help', 'Access levels' (highlighted with a red box and a red circle with the number 2), and 'Admin settings'. The main content area is titled 'DefaultCollection' and contains a project named 'MyFirstProject' (with a pink 'M' icon) described as a 'Test project'. At the bottom of the main content area, there's a note: 'If you're not a member of the Team Foundation Server Administrators group, the **Access levels** page won't appear.'

2. Choose **Export audit log**.

The screenshot shows the 'Access levels' page. On the left, there's a sidebar with 'Export audit log' (highlighted with a red box) at the top, followed by 'Stakeholder' (selected), 'Basic (default)', 'Test Plans', and 'VS Enterprise'. The main content area shows the 'Stakeholder' access level details: Name is 'Stakeholder', Features include 'View My Work Items', 'Standard Features', 'Agile boards', 'Basic backlog and sprint planning tools', 'Agile Portfolio Management', 'View Releases and Manage Approvals', 'Test summary access to stakeholder license users', and 'Administer organization'. A note at the bottom states: 'Access levels determine the features organization members can use through the web'.

3. The user log file is saved as a .csv file to your Download folder.

To determine the access level assigned to each user or group, open the file in Excel.

You can get a list of users and groups that have access to your TFS instance by exporting the audit log. The audit log also indicates which access level has been granted.

1. From the web portal home page for a project, choose the gear icon and select **Server settings**.

The screenshot shows the Microsoft Team Foundation Server (TFS) web portal. At the top, there's a navigation bar with links for Home, Code, Work, and ... (with a dropdown arrow). Below the navigation bar is a secondary menu with icons and text: Overview, Plan, Welcome, Visual Studio, Work, Security, Alerts, Version Control, Agent Queues, Service Hooks, Services, Test, Release, Default team settings, Collection settings, and Server settings (which is highlighted with a red box).

2. Choose **Access levels**, and then **Export audit log**.

The screenshot shows the Microsoft Team Foundation Server (TFS) web portal. The URL is [http://myserver:8080/tfs](#). The page title is "Team Foundation Server". The main content area has tabs for Control panel, Access levels (which is selected and highlighted with a red box), and Legacy extensions. Under the Access levels tab, there's a table showing access levels:

	Name	Features
Stakeholder	Stakeholder	View My Work Items Standard Features Agile boards View Releases and Manage Approvals
Basic (default)		
Advanced		
VS Enterprise		

A note at the bottom of the page states: "Access levels determine the features account members can use through the web portal. For more information, see [Access levels](#)".

NOTE

If you're not a member of the Team Foundation Server Administrators group, the link to the **Access levels** page won't appear.

3. The user log file is saved as a .csv file to your Download folder.

To determine the access level assigned to each user or group, open the file in Excel.

You can get a list of users and groups that have access to your TFS instance by exporting the audit log. The audit log also indicates which access level has been granted.

1. From the web portal home page for a project, choose the gear icon. The URL is similar to

<http://myserver:8080/tfs>.

The screenshot shows the Microsoft Team Foundation Server (TFS) web portal for the project "Fabrikam Fiber". The URL is [http://myserver:8080/tfs](#). The page title is "Visual Studio Team Foundation Server 2015 / Fabrikam Fiber". The top navigation bar includes links for HOME, CODE, WORK, BUILD, TEST, and Overview (which is selected and highlighted with a blue box). There's also a search bar for "Search work items" and a gear icon for settings.

2. Choose **Access levels**, and then **Export audit log**.

Control Panel

Control panel Access levels Extensions

Export audit log

Stakeholder
Basic (default)
Advanced

Access levels

Name	Features
Advanced	View My Work Items Standard Features Agile boards Basic backlog and sprint planning tools Request and Manage Feedback Test case management Team rooms

NOTE

If you're not a member of the Team Foundation Server Administrators group, the **Access levels** page won't appear.

3. The user log file is saved as a .csv file to your Download folder.

To determine the access level assigned to each user or group, open the file in Excel.

Related articles

- [About access levels](#)
- [Manage users and access in Azure DevOps](#)
- [Azure DevOps Feature Matrix](#)
- [Default permissions and access.](#)

- [About access levels](#)
- [Change access levels](#)
- [Azure DevOps Feature Matrix](#)
- [Default permissions and access.](#)

Set dashboard permissions

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

As a member of the Project Administrators group, you can set the default dashboard permissions for all teams. As a team or project administrator, you can set individual dashboard permissions for team members. The permissions only affect the team members to which the dashboards belongs.

As a team or project administrator, you can set individual dashboard permissions for team members. The permissions only affect the team members to which the dashboards belongs.

NOTE

The set dashboard permissions feature is available for TFS 2017.1 and later versions. For TFS 2017 and earlier versions, only team and project administrators can add and edit dashboards.

To learn more about adding and viewing dashboards, see [Add, rename, and delete dashboards](#).

TIP

If a user reports that they can't create or edit a team dashboard, and you've set the permissions to allow them to do so, check that they have been added as a member of the team. This includes adding them as a team member to the default project team. For details, see [Add users to a project or specific team](#).

Prerequisites

- If you haven't been added as a team member, [get added now](#).
- Anyone with access to a project, including [stakeholders](#), can view dashboards.
- To add, edit, or manage a team dashboard, you must have **Basic** access or greater and be a [team admin](#), a project admin, or have dashboard permissions. In general, you need to be a team member for the currently selected team to edit dashboards.

Set default dashboard permissions for a project

By default, all team members have permissions to edit dashboards defined for the team. All other valid users of the project have view only permissions, except for members of the Project Administrators group. You can change the default permissions a project from the Project settings.

1. Choose **Project Settings** and then **Dashboards**.

Fabrikam Fiber

Project Settings > Dashboards > Fabrikam Team

General Dashboards

Overview Security

Teams Only team admins can set a team's permissions for all dashboards. The permissions set here affect all dashboards for this team.

Security

Notifications Create dashboards Allows team members to create dashboards.

Service hooks Edit dashboards Allows team members to modify widgets and settings on dashboards.

Artifacts

Dashboard (highlighted with a red box)

Boards Delete dashboards Allows team members to delete dashboards.

Pipelines

Code

Test

Extensions

Project settings

- Check or uncheck those permissions you want to grant or restrict. Your changes are automatically saved by the system.

Set individual dashboard permissions for team members

- Open the [Dashboards directory](#), choose the **...** actions icon for the dashboard, and then select the **Security** menu option.

Dashboards

New Dashboard

Filter by text Team: Fabrikam Team

Name	Team	Description
Analytics	...	g8 Fabrikam Team
Bug status	...	Security (highlighted with a red box)
Overview	...	Active bugs and bug trends
playground	...	
Team Guidance	...	g8 Fabrikam Team

- Change **Allow** or **Deny** to grant or restrict a permission.

Here we lock down the permissions for members of the Fabrikam team to edit the Analytics dashboard.

X

Permissions for Analytics

The screenshot shows a 'Search' bar at the top left. Below it is a sidebar with a user icon and the text 'Fabrikam Team'. The main area is titled 'ACCESS CONTROL SUMMARY' with the sub-instruction 'Shows information about the permissions being granted to this identity'. Underneath, there are two buttons: 'Delete dashboard' and 'Edit dashboard'. The 'Edit dashboard' button has a 'Deny (inherited)' link above it, which is highlighted with a blue border. Below these are three buttons: 'Remove', 'Save changes' (which is also highlighted with a blue border), and 'Undo changes'. At the bottom right of the dialog is a 'Close' button.

NOTE
The dashboard permissions dialog doesn't support granting permissions to other users or groups at this time.

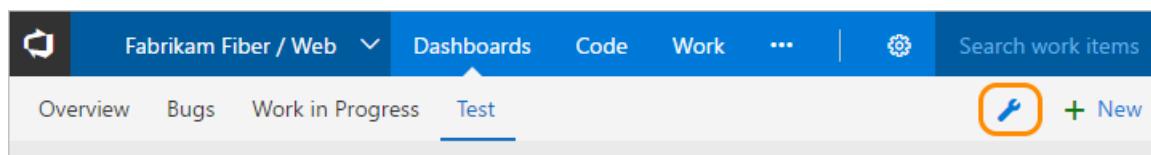
3. Choose **Save changes** and then **Close**.

Set individual dashboard permissions for team members

By default, all team members have permissions to edit dashboards defined for the team. All other valid users of the project have view only permissions, except for administrators. You can change the view, edit, and manage permissions for all team dashboards for members of your team.

1. To change the permissions for a specific dashboard, open the dashboard and then choose the wrench icon for the dashboard.

For example, here we open the Manage Dashboards dialog for the Fabrikam Fiber Web team's Test dashboard.



2. Choose the **Permissions** tab and check those checkboxes to grant or restrict permissions to your team members to edit and manage team dashboards. The default settings, as shown in the illustration, provide all team members permissions to edit and manage dashboards.

NOTE

The dashboard security dialog doesn't support granting permissions to other users or groups.

X

Manage Dashboards

Dashboards Permissions

Select dashboard permissions for members of your team. [Learn more](#)

Create dashboards

Allows team members to create dashboards.

Edit dashboards

Allows team members to modify widgets and settings on dashboards.

Delete dashboards

Allows team members to delete dashboards.

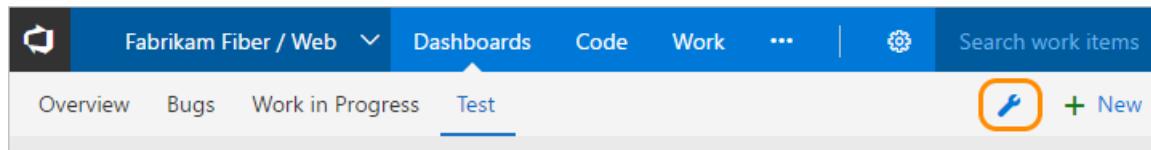
Save

Cancel

3. Choose **Save** to save your changes and dismiss the Settings dialog.

1. To change the permissions for a specific dashboard, open the dashboard and then choose the  wrench icon for the dashboard.

For example, here we open the Manage Dashboards dialog for the Fabrikam Fiber Web team's Test dashboard.



2. Choose the **Permissions** tab and check those checkboxes to grant or restrict permissions to your team members to edit and manage team dashboards. The default settings, as shown in the illustration, provide all team members permissions to edit and manage dashboards.

NOTE

The dashboard security dialog doesn't support granting permissions to other users or groups.

Requires TFS 2017.1 or later version.

X

Manage Dashboards

Dashboards

Permissions

Select dashboard permissions for members of your team. [Learn more](#)

View dashboards

Allows team members to view dashboards.

View and Edit dashboards

Allows team members to view dashboards and modify widgets on dashboards.

View, Edit and Manage dashboards

Allows team members to view dashboards, create dashboards, delete dashboards and modify widgets on dashboards.

Save

Cancel

3. Choose **Save** to save your changes and dismiss the Settings dialog.

Related articles

- [Add users to a project or specific team](#)
- [Add a team administrator](#)

Set branch permissions

5/31/2019 • 3 minutes to read • [Edit Online](#)

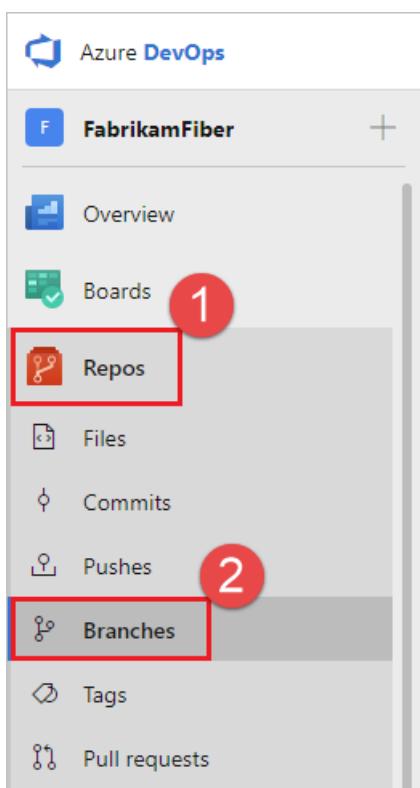
Azure Repos | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 Update 1

Overview

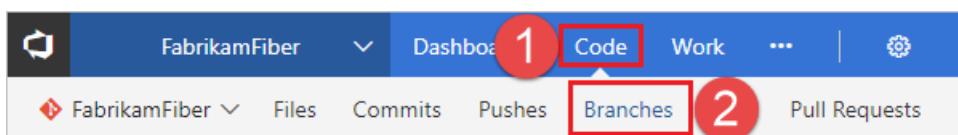
Set up permissions to control who can read and update the code in a branch on your Git repo. You can set permissions for individual users and groups, and inherit and override permissions as needed from your [repo permissions](#).

Use the branches view to configure security

1. Open the **Branches** page by navigating to your project in the web portal and selecting **Repos**, **Branches**.



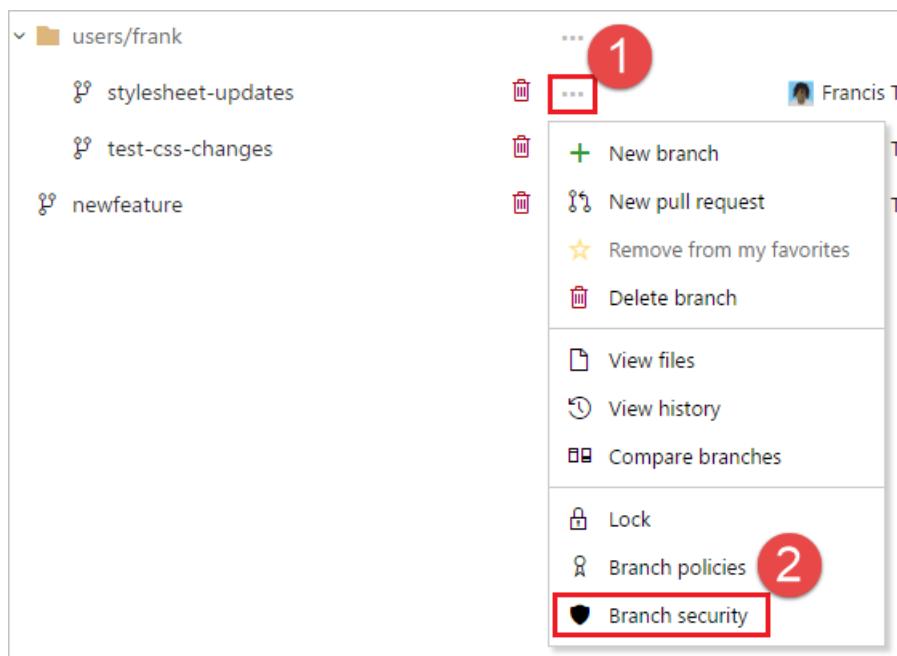
If you're not using the new navigation preview, select **Code**, **Branches**.



2. Locate your branch in the page. You can browse the list or you can search for your branch using the **Search all branches** box in the upper right.

Branches							
Mine	All	Stale			Search all branches	New branch	
Branch	Commit	Author	Authored Date		Behind Ahead	Build	Pull Request
users/jamal	★						
bptest	ce63eda0	Johnnie McLeod	7/3/2018	0 2		8% 21	
branch-from-demo	b9650f9c	Jamal Hartnett	1/8/2018	0 0	✓		
date-fix	b9650f9c	Jamal Hartnett	1/8/2018	0 0	✓		
international-address-support	64515222	Jamal Hartnett	1/11/2018	2 1		8% 8	
reademe-updates	36d09ed8	Jamal Hartnett	1/23/2018	2 2		8% 9	
develop	90bdd18e	Jamal Hartnett	10/27/2017	3 0			
master	Default Compare	★	b9650f9c	Jamal Hartnett	1/8/2018		✓

3. Open the context menu by selecting the ... icon next to the branch name. Select **Branch security** from the menu.



Add users or groups

Avoid trouble: You can only add permissions for users and groups already in your Project. [Add new users and groups to your Project](#) before setting branch permissions.

Add users or groups to your branch permissions by selecting **Add**. Enter the sign-in address or group alias, then select **Save Changes**.

Remove users or groups

Remove permissions for a user or group by selecting the user or Azure DevOps group, then selecting **Remove**. The user or group will still exist in your Project and this change will not affect other permissions for the user or group.

Security for users/frank/fix-rendering branch in FabrikamProject

Security Branch Policies

Add... Inheritance ▾

Search

▼ VSTS Groups

- Project Collection Administrators
- Project Collection Build Service Accounts
- Project Collection Service Accounts
- Build Administrators
- Contributors
- Project Administrators
- Readers

▼ Users

- Francis Totten
- Project Collection Build Service (fabrikops2)

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Permission	Status
Bypass policies when completing pull requests	Not set
Bypass policies when pushing	Not set
Contribute	Allow
Edit policies	Allow
Force push (rewrite history, delete branches and tags)	Deny
Manage permissions	Allow
Remove others' locks	Allow

[Clear explicit permissions](#)

[Remove](#) [Save changes](#) [Undo changes](#)

Set permissions

Control branch permission settings from the branch permission view. Users and groups with permissions set at the repo level will [inherit those permissions](#) by default.

NOTE

These permissions have changed in TFS 2017 Update 1 and Azure DevOps Services. Ensure you are viewing the correct version of this documentation for permissions by choosing your product version in the upper left corner of the window.

Azure DevOps Services ▾

Version

- Azure DevOps Services
- Azure DevOps Server 2019
- TFS 2018
- TFS 2017
- TFS 2015
- TFS 2013

Permissions in TFS 2017 Update 1 through TFS 2018 Update 2

PERMISSION	DESCRIPTION
Contribute	Users with this permission can push new commits to the branch and lock the branch.
Edit Policies	Can edit branch policies .

PERMISSION	DESCRIPTION
Exempt from policy enforcement	Users with this permission are exempt from the branch policy set for the branch when completing pull requests and can override the policies by checking Override branch policies and enable merge when completing a PR. Users with this permission can also push to a branch that has branch policies enabled.
Force Push (Rewrite History and Delete Branches)	Can force push to a branch, which can rewrite history. This permission is also required to delete a branch.
Manage Permissions	Can set permissions for the branch.
Remove Others' Locks	Can remove locks set on branches by other users.

Permissions in TFS 2017 and lower

PERMISSION	DESCRIPTION
Administer	Users with this permission can set branch permissions for other users, delete the branch, and lock the branch.
Contribute	Users with this permission can push new commits to the branch. Users with this permission cannot rewrite the existing commits on the branch. Users with this permission can lock the branch.
Exempt from policy enforcement	Users with this permission are exempt from the branch policy set for the branch.
Rewrite and destroy history (force push)	Can force push to a branch. This permission is also required to delete a branch. Users with this permission can modify the commit history of a branch.

Permissions in Azure DevOps Services

NOTE

In Azure DevOps Services, the **Exempt from policy enforcement** permission (which is still available in TFS 2015 through TFS 2018 Update 2) was removed and its functionality divided into the following two new permissions:

- **Bypass policies when completing pull requests**
- **Bypass policies when pushing**

Users that previously had **Exempt from policy enforcement** enabled now have the two new permissions enabled instead. See the following table for more details on these two new permissions.

PERMISSION	DESCRIPTION
Contribute	Users with this permission can push new commits to the branch and lock the branch.
Edit Policies	Can edit branch policies .

PERMISSION	DESCRIPTION
Bypass policies when completing pull requests	Users with this permission are exempt from the branch policy set for the branch when completing pull requests and can opt-in to override the policies by checking Override branch policies and enable merge when completing a PR.
Bypass policies when pushing	Users with this permission can push to a branch that has branch policies enabled. Note that when a user with this permission makes a push that would override branch policy, the push automatically bypasses branch policy with no opt-in step or warning.
Force Push (Rewrite History and Delete Branches)	Can force push to a branch, which can rewrite history. This permission is also required to delete a branch.
Manage Permissions	Can set permissions for the branch.
Remove Others' Locks	Can remove locks set on branches by other users.

Add users to Azure Pipelines

5/6/2019 • 5 minutes to read • [Edit Online](#)

Azure Pipelines | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

NOTE

In Microsoft Team Foundation Server (TFS) 2018 and previous versions, build and release *pipelines* are called *definitions*, *service connections* are called *service endpoints*, *stages* are called *environments*, and *jobs* are called *phases*.

If your teammates want to edit pipelines, then have an administrator add them to your project:

1. Make sure you are a member of the Project Administrators group ([learn more](#)).
2. Go to your project summary: <https://dev.azure.com/{your-organization}/{your-project}>
3. Invite the teammates to join the project.

The screenshot shows the 'Add Users to OurProject' dialog box. At the top, there's a breadcrumb navigation: 'OurOrg / OurProject / Overview / Summary'. To the right are search, filter, and user icons. Below the breadcrumb, the project name 'OurProject' is displayed with a blue 'O' icon. To the right of the project name are 'Private' and 'Invite' buttons, with 'Invite' being highlighted with a red box. The main area of the dialog has two input fields: 'Add users or groups *' containing 'myteammate@fabrikam.com' and 'Add to team(s) *' containing 'OurProject Team'. A note below the second field says: 'myteammate@fabrikam.com has not been assigned an access level, and will be assigned the best available.' At the bottom are 'Add' and 'Cancel' buttons, with 'Add' also highlighted with a red box.

4. After the teammates accept the invitation, ask them to verify that they can [create and edit pipelines](#).

Confirm that contributors have pipeline permissions

If you created your project after about October 2018, then the above procedure is probably sufficient. However, in some cases your team members might see errors or grayed-out controls when they try to work with pipelines. In these cases, make sure that your project contributors have the necessary permissions:

1. Make sure you are a member of the Build Administrators group or the Project Administrators group ([learn more](#)).

2. Open the build security dialog box.

The screenshot shows the Azure DevOps interface for a project named 'OurProject'. In the left sidebar, the 'Builds' option is selected (marked with a red box and number 1). In the main pane, a search bar at the top has a red box and number 2 around its icon. Below it, a list of build pipelines includes 'All build pipelines' (highlighted with a yellow background) and 'OurProject-Cl'. To the right, a context menu for 'All builds' is open, with 'Security' highlighted by a red box and number 3. Other options in the menu include 'Rename' (number 4), 'Delete', and 'Copy link'.

3. On the permissions dialog box, make sure the following permissions are set to Allow.

The screenshot shows the 'Permissions for OurProject' dialog. On the left, a tree view lists 'DevOps Groups' (selected), 'Contributors' (highlighted with a red box and number 1), 'Project Administrators', 'Readers', and 'Users'. Under 'Users' is 'Project Collection Build Service (OurAccount)'. On the right, the 'ACCESS CONTROL SUMMARY' section displays various build-related permissions. Several permissions are highlighted with red boxes and numbers: 'Delete build definition' (number 2), 'Delete builds', 'Destroy builds', and 'Edit build definition' are grouped together; 'Stop builds' (number 3) and 'Update build information' are also highlighted. At the bottom, buttons for 'Remove', 'Save changes' (highlighted with a red box and number 4), 'Undo changes', and 'Close' (highlighted with a red box and number 5) are shown.

Permissions for build and release functions are primarily set at the object-level for a specific build or release, or for select tasks, at the collection level. For a simplified view of permissions assigned to built-in groups, see [Permissions and access](#).

In addition to permission assignments, you manage security for several resources—such as variable groups, secure files, and deployment groups—by adding users or groups to a role. You grant or restrict permissions by setting the [permission state to Allow or Deny](#), either for a security group or an individual user. For definitions of each build and release permission and role, see [Build and release permissions](#).

Set permissions for build pipelines

1. To set the permissions for all build pipelines, click the Security From the web portal **Build-Release**

hub, **Builds** page

The screenshot shows the Microsoft DevOps hub's Builds page. At the top, there's a navigation bar with 'Fabrikam Fiber' and 'Build and Release'. Below the navigation is a toolbar with 'Builds', 'Releases', 'Library', 'Task Groups', 'Deployment Groups*', 'Build Tags', 'Build ID or build number' search, '+ New', '+ Import', and a 'Security' button which is highlighted with a red box. Underneath is a filter bar with 'Mine', 'Definitions', 'Queued', and 'XAML'. A table follows, showing 'Recently built' items. One item, 'fabrikam build', is selected and has a person icon next to it. To the right of the table, it says 'Status' and 'Triggered by' followed by 'No builds have r...'. The entire interface has a light blue background.

To set the permissions for a specific build pipeline, open the context menu for the build and click Security.

This screenshot shows the same DevOps hub Builds page as above, but with a context menu open over the 'fabrikam build' item. The menu includes options like 'Queue new build...', 'Edit...', 'View definition summary', 'Add to my favorites', 'Add to team favorites', 'Clone...', 'Export', 'Rename...', 'Save as a template...', 'Delete definition', and 'Security...'. The 'Security...' option is highlighted with a red box. The rest of the page remains visible in the background.

2. Choose the group you want to set permissions for, and then change the permission setting to Allow or Deny.

For example, here we change the permission for Edit build pipeline for the Contributors group to Allow.

Permissions for fabrikam build

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Administer build permissions	Not set
Delete build definition	Not set
Delete builds	Not set
Destroy builds	Not set
Edit build definition	Allow
Edit build quality	Allow (inherited)
Manage build qualities	Not set
Manage build queue	Not set
Override check-in validation by build	Not set
Queue builds	Allow (inherited)
Retain indefinitely	Not set
Stop builds	Not set
Update build information	Not set
View build definition	Allow (inherited)
View builds	Allow (inherited)

[Clear explicit permissions](#)

[Remove](#) [Save changes](#) [Undo changes](#)

[Close](#)

- Save your changes.

Set permissions for release pipelines

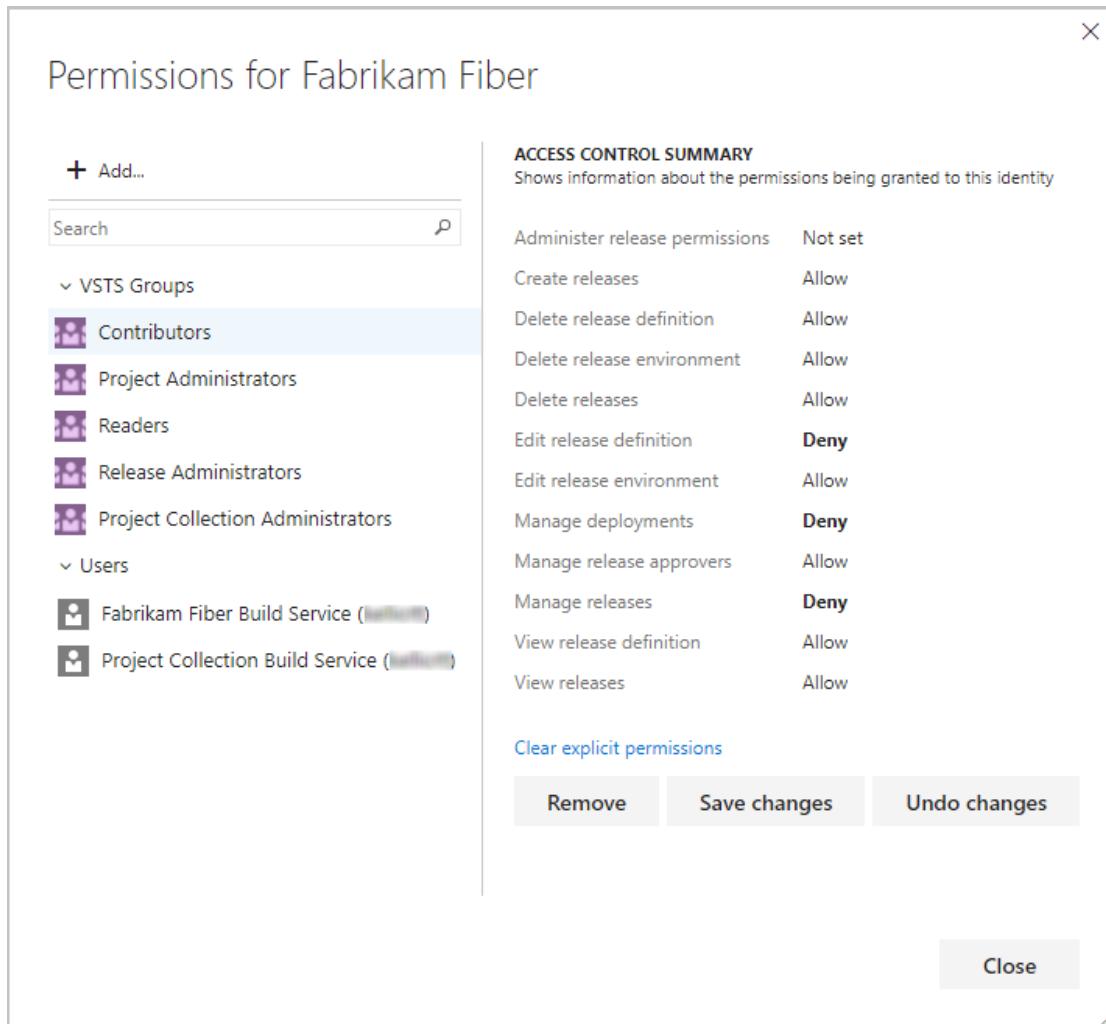
- From the web portal **Build-Release** hub, **Releases** page, open the Security dialog for all release pipelines.

The screenshot shows the 'Releases' tab selected in the top navigation bar. Below it, a list of release definitions is shown. A context menu is open over one of the definitions, with the 'Security...' option highlighted.

If you want to manage the permissions for a specific release, then open the Security dialog for that release.

- Choose the group you want to set permissions for, and then change the permission setting to Allow or Deny.

For example, here we deny access to several permissions for the Contributors group.



3. Save your changes.

Manage Library roles for variable groups, secure files, and deployment groups

Permissions for [variable groups](#), [secure files](#), and [deployment groups](#) are managed by roles. For a description of the roles, see [About security roles](#).

NOTE

Feature availability: These features are available on Azure Pipelines and TFS 2017 and later versions.

You can set the security for all artifacts for a project, as well as set the security for individual artifacts. The method is similar for all three artifact types. You set the security for variable groups and secure files from **Azure Pipelines, Library** page, and for deployment groups, from the **Deployment groups** page.

For example, here we show how to set the security for variable groups.

1. **Build-Release hub, Library** page, open the Security dialog for all variable groups.

The screenshot shows the Azure DevOps interface with the 'Library' tab selected. At the top right, there is a blue button labeled '+ Variable group' and a red-outlined button labeled 'Security'. Below these buttons, there are two links: 'Variable groups' (underlined) and 'Secure files'.

If you want to manage the permissions for a specific variable group, then open the Security dialog for that group.

This screenshot shows the 'Variable groups' list. A context menu is open over the row for 'FF group', with options 'Edit', 'Delete', and 'Security'. The 'Security' option is highlighted with a red box.

2. Add the user or group and choose the role you want them to have.

For example, here we deny access to several permissions for the Contributors group.

This screenshot shows the 'Assign security roles for Library' dialog. A red box highlights the '+ Add' button in the header. A sub-dialog titled 'Add user' is open, showing a list of users and a selection for 'Raisa Pokrovskaya' with a 'User' role assigned. A note at the bottom states: 'User can use, but cannot manage the library items.' There are 'Add' and 'Close' buttons at the bottom of the sub-dialog.

3. Click **Add**.

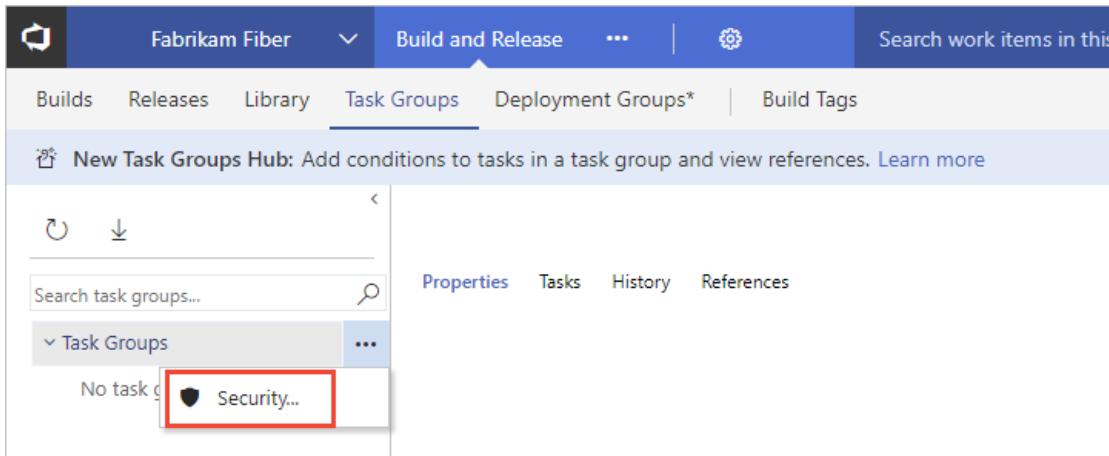
Manage task group permissions

Permissions for task groups are subject to a hierarchical model. You use task groups to encapsulate a sequence of tasks already defined in a build or a release pipeline into a single reusable task. You [define and manage task groups](#) in the **Task groups** tab of **Azure Pipelines**.

NOTE

Feature availability: These features are available on Azure Pipelines and TFS 2017 and later versions.

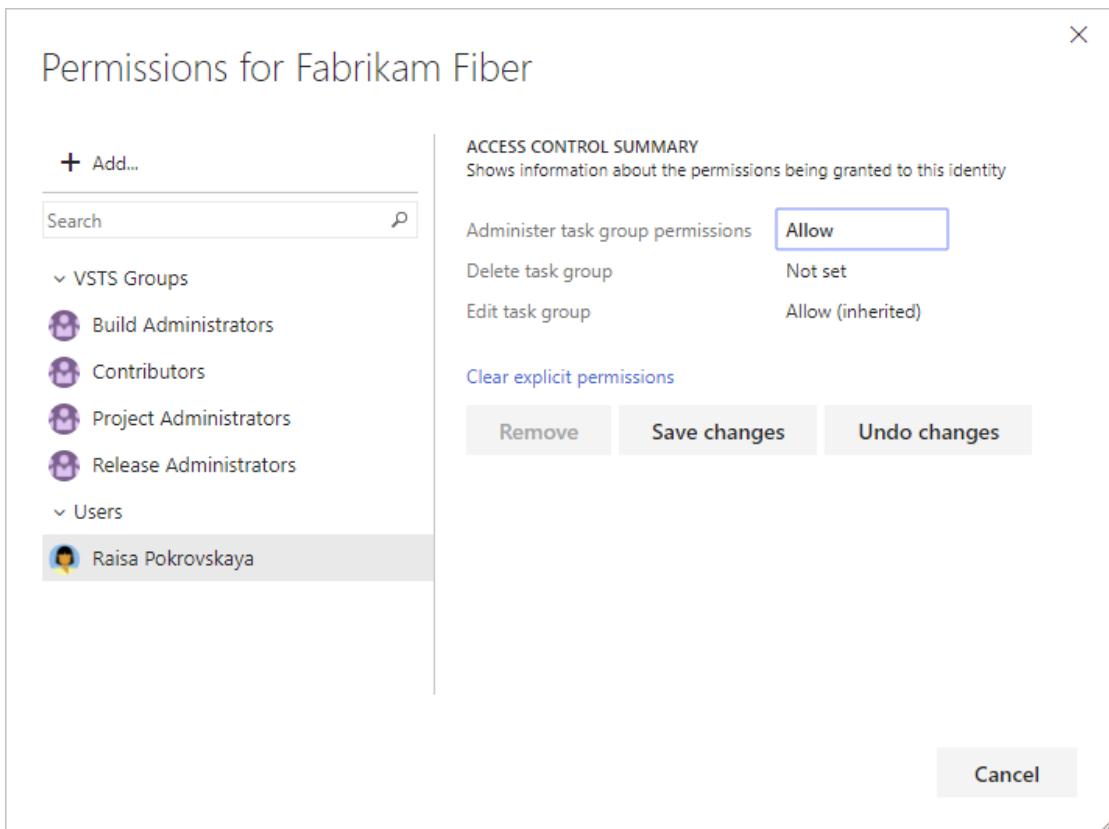
1. From the web portal **Build-Release hub**, **Task groups** page, open the Security dialog for all task groups.



If you want to manage the permissions for a specific task group, then open the Security dialog for that group.

2. Add the user or group and then set the permissions you want them to have.

For example, here we add Raisa and set her permissions to Administer all task groups.



3. Click **Add**.

Set collection-level permissions to administer build resources

1. From the web portal user context, open the admin context by clicking the gear Settings icon and choosing **Organization settings** or **Collection settings**.
2. Click **Security**, and then choose the group whose permissions you want to modify.

Here we choose the Build Administrators group and change the **Use build resources** permission. For a description of each permissions, see [Permissions and groups reference](#), [Collection-level permissions](#).

The screenshot shows the 'Security' tab selected in the 'fabrikam' project collection settings. Under 'VSTS Groups', the 'Project Collection Build Administrators' group is selected. On the right, a table lists build-related permissions with their current status:

Permission	Status
Administer build resource permissions	Allow
Administer process permissions	Not set
Administer shelved changes	Not set
Administer workspaces	Not set
Alter trace settings	Not set
Create a workspace	Allow (inherited)
Create new projects	Not set
Create process	Not set
Delete field from account	Not set
Delete process	Not set
Delete team project	Not set
Edit instance-level information	Not set
Edit process	Not set
Make requests on behalf of others	Not set
Manage build resources	Allow
Manage test controllers	Not set
Trigger events	Not set
Use build resources	Allow
View build resources	Allow
View instance-level information	Allow
View system synchronization information	Not set

At the bottom, there are 'Save changes' and 'Undo changes' buttons.

3. Save your changes.

Manage permissions for agent pools and service connections

You manage the security for [agent pools](#) and [service connections](#) by adding users or groups to a role. The method is similar for both agent pools and service connections. You will need to be a member of the Project Administrator group to manage the security for these resources.

NOTE

Feature availability: These features are available on Azure Pipelines and TFS 2015 and later versions.

For example, here we show how to add a user to the Administrator role for a service connection.

1. From the web portal, click the gear Settings icon to open the project settings admin context.
2. Click **Services**, click the service connection that you want to manage, and then click **Roles**.

User	Role	Access
[Fabrikam Fiber]\Endpoint Administrators	Administrator	Inherited

3. Add the user or group and choose the role you want them to have. For a description of each role, see [About security roles](#).

For example, here we add Raisa to the Administrator role.

Add user

User or group: Raisa Pokrovskaya

Role: Administrator

4. Click **Add**.

Manage permissions for agent pools and deployment pools

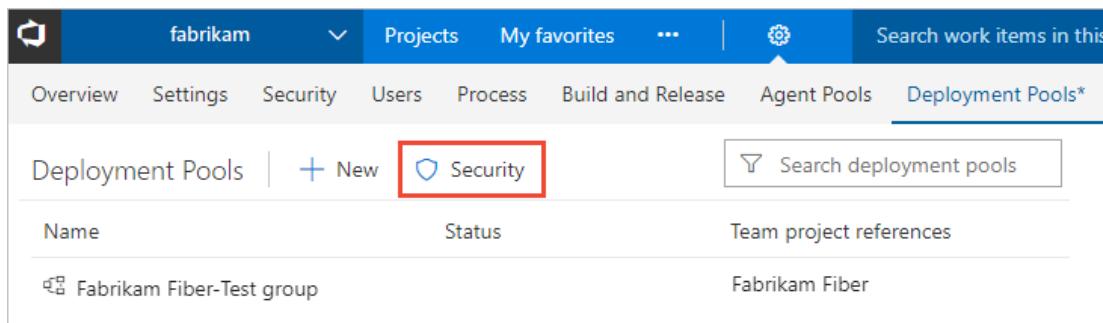
You manage the security for [agent pools](#) and [deployment pools](#) by adding users or groups to a role. The method is similar for both types of pools.

NOTE

Feature availability: These features are available on Azure Pipelines and TFS 2018 and later versions.

You will need to be a member of the Project Collection Administrator group to manage the security for a pool. Once you've been added to the Administrator role, you can then manage the pool. For a description of each role, see [About security roles](#).

1. From the web portal, click the gear Settings icon and choose Organization settings or Collection settings to open the collection-level settings admin context.
2. Click **Deployment Pools**, and then open the **Security** dialog for all deployment pools.

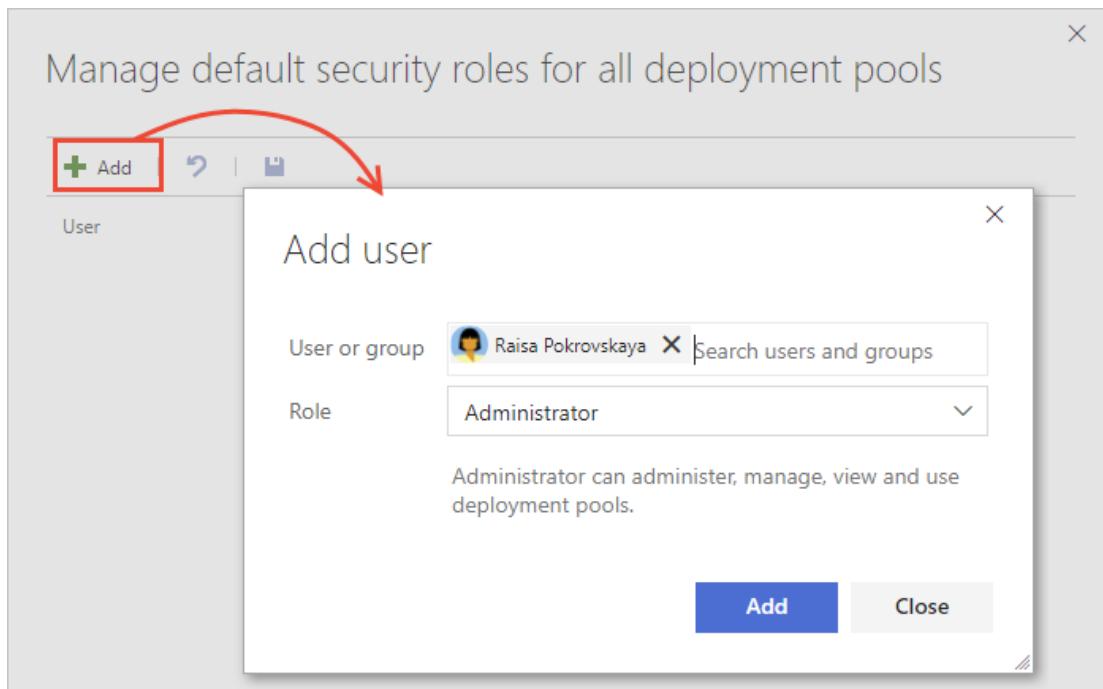


The screenshot shows the Azure DevOps web interface. At the top, there's a navigation bar with 'fabrikam' and dropdown menus for 'Projects', 'My favorites', 'Settings', and 'Search work items in this'. Below the navigation bar, there's a horizontal menu with tabs: 'Overview', 'Settings', 'Security', 'Users', 'Process', 'Build and Release', 'Agent Pools', and 'Deployment Pools*'. The 'Deployment Pools*' tab is currently selected. Underneath this, there's a section titled 'Deployment Pools' with a 'New' button and a 'Security' button, which is also highlighted with a red box. To the right of these buttons is a search bar labeled 'Search deployment pools'. Below this, there are two columns: 'Name' and 'Status' (with a 'Team project references' link), and 'Fabrikam Fiber-Test group' under 'Fabrikam Fiber'.

If you want to manage the permissions for a specific deployment group, then open the Security dialog for that group.

3. Add the user or group and choose the role you want them to have.

For example, here we add Raisa to the Administrator role.



The screenshot shows a modal dialog titled 'Manage default security roles for all deployment pools'. In the top left corner of the main window, there's a '+ Add' button, which is highlighted with a red box and has a red arrow pointing to it from the left. The main window lists 'User' and shows a placeholder for adding users. A smaller 'Add user' dialog is open in the foreground. It has fields for 'User or group' (containing 'Raisa Pokrovskaya') and 'Role' (set to 'Administrator'). Below these fields is a descriptive note: 'Administrator can administer, manage, view and use deployment pools.' At the bottom of the dialog are 'Add' and 'Close' buttons.

4. Click **Add**.

Related notes

[Default build and release permissions](#)

- [Default permissions and access](#)
- [Permissions and groups reference](#)

Provide Stakeholders access to edit build and release pipelines

6/14/2019 • 4 minutes to read • [Edit Online](#)

Azure DevOps Services

To provide Stakeholders permissions to create, edit, and manage build and release pipelines, you can enable the **Free access to Pipelines for Stakeholders** account-level preview feature. This feature essentially enables an unlimited number of free users to manage and configure pipelines in your projects.

IMPORTANT

The **Free access to Pipelines for Stakeholders** preview feature is turned on by default for all organizations created after July, 7th 2018. It is only available from Azure DevOps Services.

Without this feature enabled, stakeholders can only [view and approve releases](#).

Turn on Free access to Pipelines for Stakeholders

To enable the **Free access to Pipelines for Stakeholders** feature, see [Enable preview features](#). You can only enable it at the account level.

Preview features

The following preview features are available for your evaluation. Help us make them better!

for this account [fabrikam] ▾

Build with multiple queues

On

Allows selection of specific queues in build phases. There are some known limitations with this feature. [Learn more](#)

Build YAML definitions

On

Enables YAML build definitions. [Learn more](#)

Free access to Build and Release for Stakeholders

On

Gives users with the Stakeholder license full access to the Build and Release hub. You can limit what they can do via security groups or permissions. This doesn't affect public projects, where they always have full access. [Learn more](#)

When the feature is turned on, all Stakeholders in your account have full access to **Pipelines** or **Build and Release** and its associated features. This includes the ability to view, create, and delete automated test runs. For a complete list of associated features and tasks, see [Build and release permissions and roles](#).

Stakeholders are still subject to the permissions set for their security group. For example, if they are in the Project Readers security group they have Read-only access to **Build and Release**. If you need more fine grained control over what features Stakeholders can access, you can create a custom security group and set more fine grained permissions to certain groups of users as described in the next section.

Limit access to select Stakeholders to CI/CD features

After turning on the **Free access to Pipelines for Stakeholders** preview feature, you can limit access to select features or tasks by setting permissions. The general steps are:

1. Create a custom, project-level, security group in Azure DevOps
2. Add users to this group
3. Set permissions to **Deny** or **Not set** for those CI/CD features you want to limit access to. You can set permissions for these CI/CD artifacts:
 - All build pipelines or select build pipelines
 - All release pipelines or select release pipelines
 - Task groups
4. Add the security group to a Library security role for these artifacts:
 - Variable groups
 - Secure files
 - Deployment groups

Create a custom security group

Create a custom security group at the project-level or the collection-level. The method for creating a custom security group is the same, no matter at what level you add it.

TIP

You only need to create a project-level security group if you are going to limit CI/CD tasks at the project level.

To create a project-level security group, open the web portal and choose the project where you want to add users or groups.

1. Choose **Project Settings** in the sidebar.

The screenshot shows the Azure DevOps Project Summary page for the 'FabrikamFiber' project. The left sidebar contains links for Overview, Summary (which is selected), Dashboards, Wiki, Boards, Repos, Pipelines, Test Plans, Artifacts, and Project settings. The main area features a cartoon illustration of a person working at a desk with a dog. The text 'Welcome to the project!' is displayed, followed by 'What service would you like to start with?' and a row of buttons for Boards, Repos, Pipelines, Test Plans, and Artifacts. A link 'or manage your services' is also present. The 'Project settings' link in the sidebar is highlighted with a red box.

2. Open the **Security** page and choose **Create group** to open the dialog for adding a group.

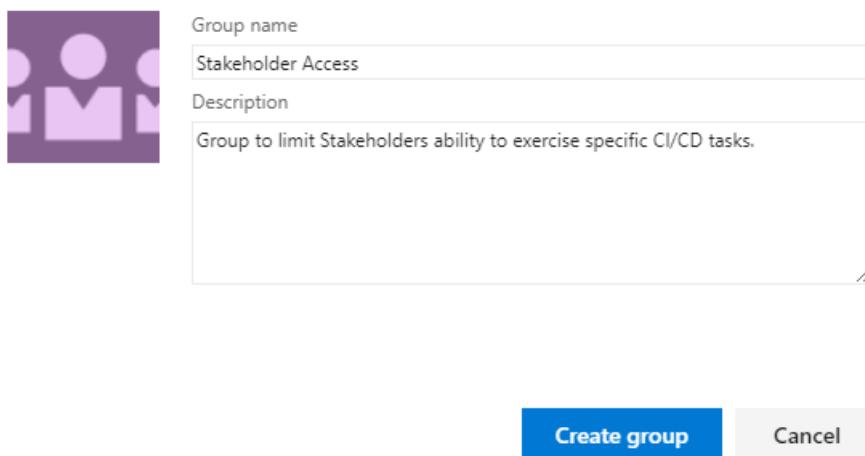
The screenshot shows the 'Project Settings > Security' page. The left sidebar lists General, Security (which is selected), Notifications, Service hooks, and Dashboards. The main area shows a 'Create group' button highlighted with a red box, a 'Filter users and groups' input field, and a list of Teams: Customer Service, Fabrikam Fiber Team, Management team, Phone, Voice, and Web. At the bottom, there is a link to 'Azure DevOps Groups'.

3. Enter a name for the group, and optionally a description.

For example, here we define a *Stakeholder Access* group.

Create new Azure DevOps Services group

PROFILE



Group name
Stakeholder Access

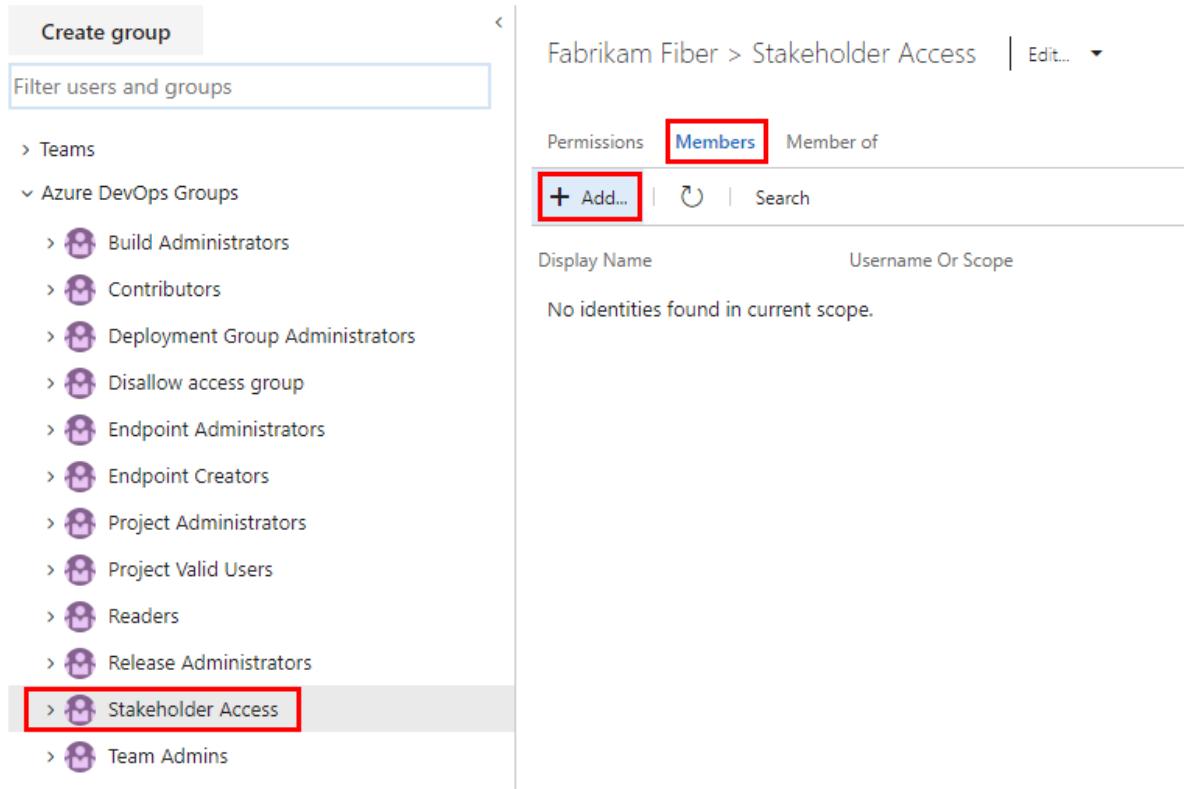
Description
Group to limit Stakeholders ability to exercise specific CI/CD tasks.

Create group Cancel

4. Choose **Create group**.

Add members to the custom security group

1. To add members to the group, choose the security group, choose **Members**, and then choose **Add**.



Filter users and groups

Permissions Members Member of

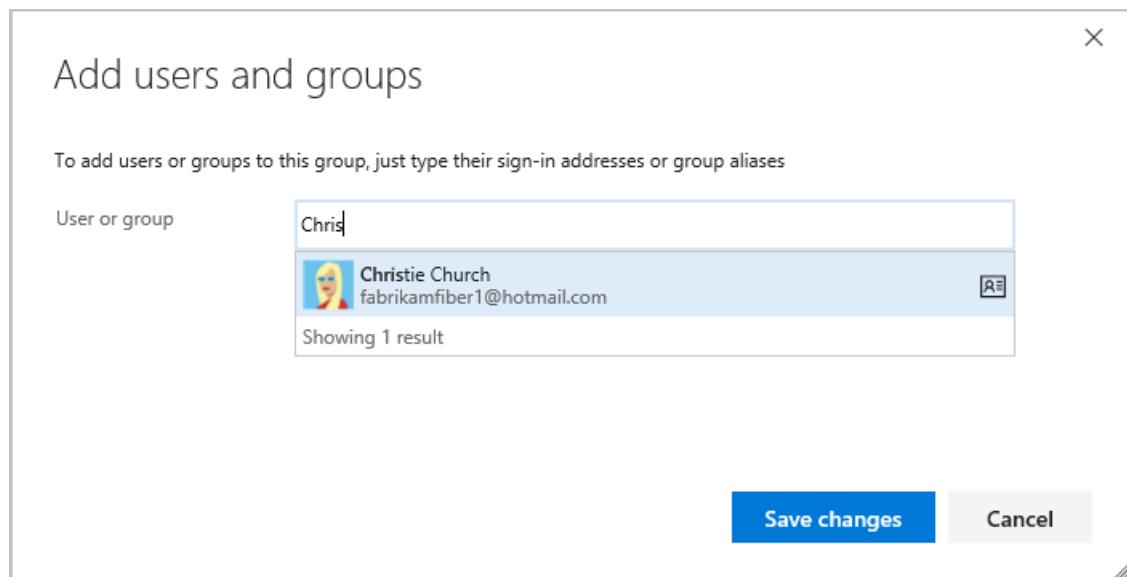
+ Add... | Search

No identities found in current scope.

Display Name Username Or Scope

Stakeholder Access

2. Type the name of the user account into the text box. You can enter several identities into the text box, separated by commas. Specify individual emails, groups defined in an existing Azure Active Directory or existing Azure DevOps groups. The system automatically searches for matches. Choose the match(es) that meets your choice.

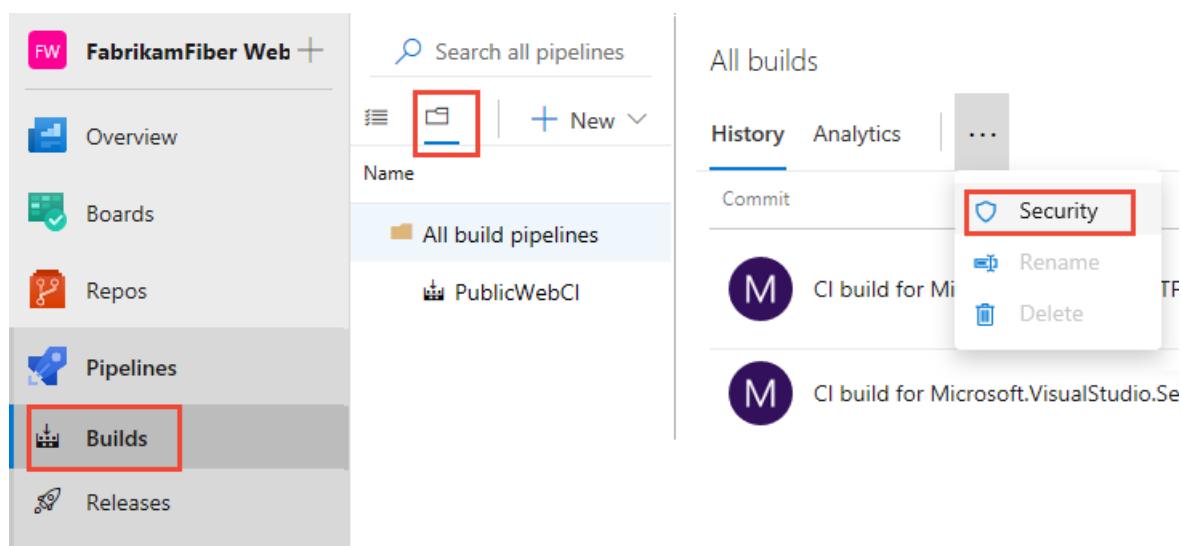


3. Choose **Save changes**.

Set permissions for build pipelines

Open the Security dialog for all or a select build pipeline.

1. To set the permissions for all build pipelines, choose **Pipelines>Builds**, choose the folder icon, and then, with **All build pipelines** selected, choose the actions icon and select **Security**.



2. To set the permissions for a specific build pipeline, open the actions icon for the specific build and choose **Security**.

The screenshot shows the Azure DevOps Pipelines interface. On the left, there's a sidebar with options like Overview, Boards, Repos, Pipelines, Builds (which is selected and highlighted with a red box), Releases, Library, Task groups, Deployment groups, and Test Plans. The main area shows a pipeline named 'PublicWebCI' with three builds listed, each represented by a purple circle with a white letter 'M'. To the right of the pipeline name is a context menu with various options: Commit, Security (which is highlighted with a red box), Rename/move, Pause builds, Add to my favorites, Add to team favorites, Clone, Save as template, Export, Status badge, and Delete.

Add and set permissions for the custom security group

1. Choose **Add** to add the *Stakeholder Access* group to the Permissions dialog.

Permissions for Fabrikam Fiber

This screenshot shows the 'Permissions for Fabrikam Fiber' dialog. It has a search bar at the top with a placeholder 'Search' and a magnifying glass icon. Below the search bar is a button labeled '+ Add...' with a red box around it. The main area is currently empty, showing a message: 'To add explicit permissions for a user or a group, just type their sign-in address or group alias'.

2. In the dialog that opens, enter the group name of the custom security group that you previously added.

Add a user or a group for permissions

To add explicit permissions for a user or a group, just type their sign-in address or group alias

This screenshot shows the 'Add a user or a group for permissions' dialog. It features a search bar with a placeholder 'User or group' and a magnifying glass icon. Below the search bar is a text input field containing the group name '[Fabrikam Fiber]\Stakeholder Access'. There's also a note below the input field: 'Use semicolons to separate multiple entries'. At the bottom of the dialog are two buttons: 'Save changes' (in blue) and 'Cancel'.

And then choose **Save changes**.

3. With the *Stakeholder Access* group selected, change the permission settings to **Deny** for those permissions you want to limit access to.

For example, here we change the permission for **Edit build definition** for the *Stakeholders Access* group to **Deny**.

Permissions for Fabrikam Fiber

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Administer build permissions	Deny
Delete build definition	Not set
Delete builds	Not set
Destroy builds	Not set
Edit build definition	Deny
Edit build quality	Not set
Manage build qualities	Not set
Manage build queue	Not set
Override check-in validation by build	Not set
Queue builds	Not set
Retain indefinitely	Not set
Stop builds	Not set
Update build information	Not set
View build definition	Not set
View builds	Not set

4. Save your changes and choose **Close**.

Set permissions for release definitions

You can follow the steps provided in the previous two procedures to set permissions for release definitions.

Open the Security dialog for all or a select release pipeline.

1. To set the permissions for all release pipelines, open **Build and Release>Releases**, and then choose **Security**.

The screenshot shows the Azure DevOps Pipelines interface. On the left, there's a sidebar with various project management and pipeline-related items: Overview, Boards, Repos, Pipelines, Builds, Releases, and Library. The 'Releases*' item is highlighted with a red box. On the right, the main area is titled 'Release definitions'. It has tabs for Active, All definitions (which is underlined), and Security. The Security tab is also highlighted with a red box. Below the tabs, it says 'Folders / Definitions' and shows a single item: 'All definitions' with a sub-item 'New Empty Definition 12-Jan'.

2. To set the permissions for a specific release pipeline, open the actions icon menu for the build and choose **Security**.
3. Add the custom security group, such as *Stakeholder Access*, to the permissions dialog.
4. With the *Stakeholder Access* group selected, change the permission settings to **Deny** for those permissions you want to limit access to.

For example, here we change the permission for **Edit build definition** for the *Stakeholders Access* group to **Deny**.

The screenshot shows the 'Permissions for All definitions' dialog. On the left, there's a sidebar with a search bar and a list of groups: 'Azure DevOps Groups' (expanded, showing 'Stakeholder Access' selected and highlighted with a red box), 'Contributors', 'Project Administrators', 'Readers', 'Release Administrators', 'Project Collection Administrators', 'Users' (expanded, showing 'Fabrikam Fiber Build Service' and 'Project Collection Build Service'), and 'Service connections' (partially visible). On the right, the 'ACCESS CONTROL SUMMARY' section is titled 'Shows information about the permissions being granted to this identity'. It lists various permissions with their current status: 'Administer release permissions' (Not set), 'Create releases' (Not set), 'Delete release definition' (Deny), 'Delete release environment' (Not set), 'Delete releases' (Deny), 'Edit release definition' (Deny), 'Edit release environment' (Not set), 'Manage deployments' (Not set), 'Manage release approvers' (Not set), 'Manage releases' (Not set), 'View release definition' (Not set), and 'View releases' (Not set). At the bottom, there are buttons for 'Remove', 'Save changes' (highlighted with a red box), and 'Undo changes'. A 'Cancel' button is at the bottom right.

5. Save your changes and the choose **Cancel**.

Limit access to Library resources

To prevent Stakeholders from editing Library resources, add your custom security group to the Library reader role.

To learn how, see [Manage Library roles for variable groups, secure files, and deployment groups](#).

Limit access to task group

To prevent Stakeholders from editing task groups, add your custom security group to the task group permissions and set all permissions to **Deny**. To learn how, see [Manage Library roles for variable groups, secure files, and deployment groups](#).

Related articles

- [Set build and release permissions](#)
- [Build and release permissions and roles \(Security\)](#)
- [Get started as a stakeholder](#)

Secure and share packages using feed permissions

7/1/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | TFS 2017

Packages you host in Azure Artifacts are stored in a **feed**. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires.

Feed permissions overview

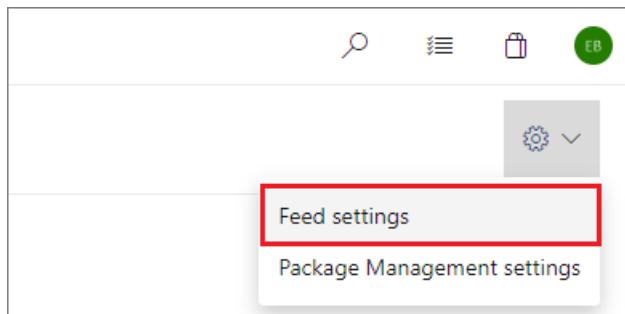
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.

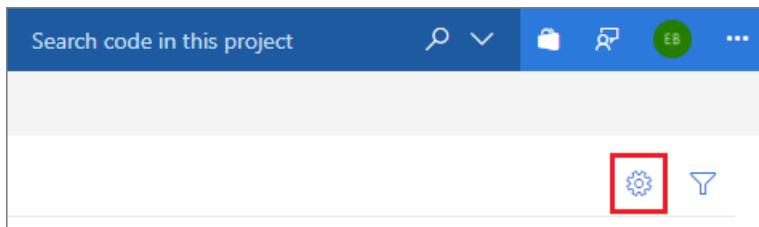
PERMISSION	READER	COLLABORATOR	CONTRIBUTOR	OWNER
List and restore/install packages	✓	✓	✓	✓
Save packages from upstream sources		✓	✓	✓
Push packages			✓	✓
Unlist/deprecate packages			✓	✓
Delete/unpublish package				✓
Edit feed permissions				✓
Rename and delete feed				✓

By default, the Project Collection Build Service is a Contributor and your project team is a Reader.

Editing permissions for a feed

With your feed selected, select **Edit feed** (the gear icon).





Select Permissions.

User/Group	Role
Elijah Batkoski	Owner
[regius]\Project Collection Administrators	Owner
[FabrikamFiber Web]\Project Administrators	Owner
Project Collection Build Service (regius)	Contributor
[FabrikamFiber Web]\Contributors	Contributor

User/Group	Role
[FabrikamFiber]\FabrikamFiber Team	Owner
[codesharing-demo]\Project Collection Administrators	Owner
Project Collection Build Service (codesharing-demo)	Contributor
[codesharing-demo]\Project Collection Valid Users	Reader

User/Group	Role
[FabrikamFiber]\FabrikamFiber Team	Owner
[codesharing-demo]\Project Collection Administrators	Owner
Project Collection Build Service (codesharing-demo)	Contributor
[codesharing-demo]\Project Collection Valid Users	Reader

In the edit feed dialog:

- Choose to make each person or team an Owner, Contributor, Collaborator, or Reader.
- When you're done, select **Save**.

Package permissions in Azure Pipelines

To use packages from a feed in Azure Pipelines, the appropriate build identity must have permission to your feed. By default, the **Project Collection Build Service** is a Contributor. If you've changed your builds to run at [project scope](#), you'll need to add the project-level build identity as a Reader or Contributor, as desired. The project-level build identity is named as follows:

```
[Project name] Build Service ([Organization name]) (e.g. FabrikamFiber Build Service (codesharing-demo))
```

Sharing packages with everyone in your organization

If you want to make the packages in a feed available to all users in your organization, create or select a [view](#) that contains the packages you want to share and ensure its visibility is set to **People in my organization**.

Manage Wiki permissions

7/9/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

By default, all members of the Contributors group can edit Wiki pages.

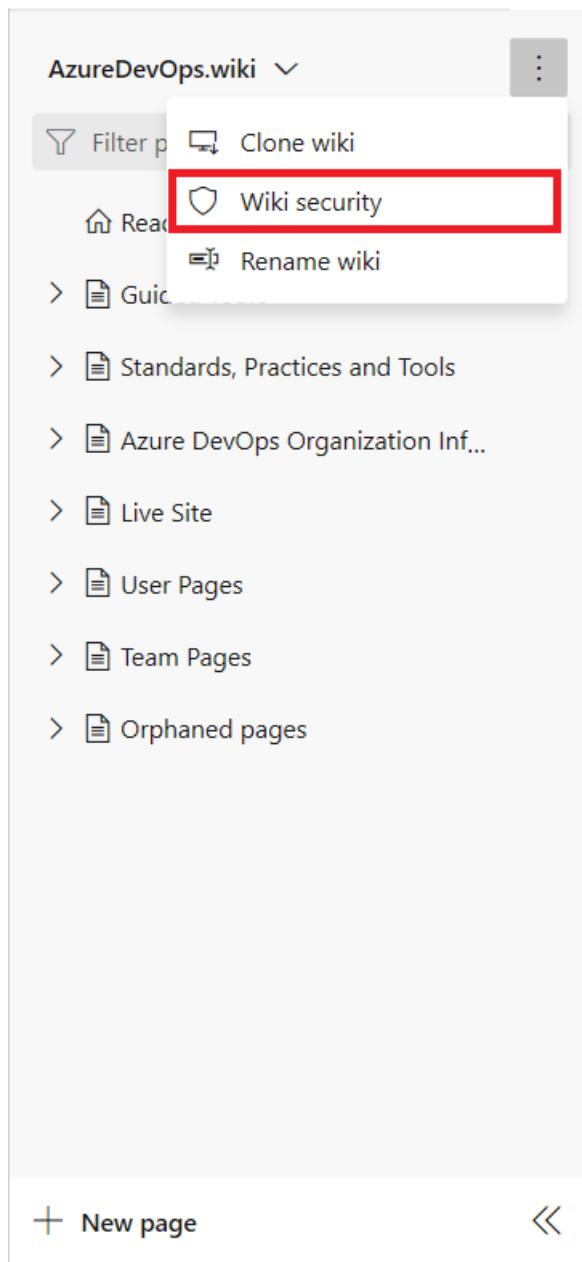
Manage wiki permissions

By default, all project contributors have read and edit access of the wiki repository. You can grant or restrict access to who can read and edit wiki pages by managing the wiki repository permissions.

NOTE

Feature availability: The built-in wiki is available with TFS 2018 and later versions.

To open the Security dialog, choose **More > Wiki Security**.



For definitions of each repository permission, see [Git repository permissions](#).

The screenshot shows the 'Security for Wiki' dialog box. On the left, there's a sidebar with a search bar and a list of roles: Build Administrators, Contributors, Project Administrators, Readers, Project Collection Administrators, Project Collection Build Service Accounts, and Project Collection Service Accounts. The 'Build Administrators' role is selected. On the right, the 'ACCESS CONTROL SUMMARY' section displays a table of permissions and their settings:

Permission	Setting
Bypass policies when completing pull requests	Not set
Bypass policies when pushing	Not set
Contribute	Allow (inherited)
Contribute to pull requests	Allow (inherited)
Create branch	Allow (inherited)
Create tag	Allow (inherited)
Delete repository	Not set
Edit policies	Not set
Force push (rewrite history, delete branches and tags)	Not set
Manage notes	Allow (inherited)
Manage permissions	Not set
Read	Allow (inherited)
Remove others' locks	Not set
Rename repository	Not set

Below the table are buttons for 'Clear explicit permissions', 'Remove', 'Save changes', and 'Undo changes'. At the bottom right is a 'Close' button.

Don't have access to create a page?

If you don't have access to create a wiki page, you need to contact an administrator to grant you adequate permission on the underlying Git repository of the wiki.

Stakeholder wiki access

Users with [Stakeholder access](#) in a private project can read wiki pages and view revisions, however they can't perform any edit operations. For example, stakeholders can't create, edit, reorder, or revert changes to pages. These permissions can't be changed. They have full access to Wikis in public projects.

The screenshot shows a card for a stakeholder named 'SU'. The card has a 'Read this first' header, a timestamp of 'Wednesday', and two action buttons: 'Edit' and '⋮'.

Q & A

Q: Is it possible to grant permissions on a per-page basis?

A: No, permissions to access the wiki are made for all pages and not individual pages.

Related articles

- [Default Git repository and branch permissions](#)
- [Get Started with Git](#)

Set permissions and access for work tracking

6/13/2019 • 8 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You grant or restrict access to various work tracking features by granting users or groups specific permissions for an object, project, or collection. Or, when you assign a user as a team administrator, they have permissions to manage all assets for the specific team. Add users to the Contributors group to provide access to most features as listed in [Permissions and access for work tracking](#).

NOTE

For public projects, Stakeholder access gives users greater access to work tracking features and full access to Azure Pipelines. To learn more, see [About access levels, Stakeholder access](#).

ROLE OR PERMISSION LEVEL	FUNCTIONAL AREAS SET
Team administrator role	<ul style="list-style-type: none">• Manage teams and configure team tools• Define and edit team dashboards• Add and manage team-level work item templates• Add team administrators <p>To add a user to the team administrator role, see Add a team administrator.</p>
Object-level permissions	<ul style="list-style-type: none">• Modify work items under an area path• Create and edit nodes under an area path or iteration path• Define and edit queries or query folders• Define and edit Delivery Plans
Project-level permissions	<ul style="list-style-type: none">• Create work item tags• Delete and restore work items• Move work items out of a project• Permanently delete work items• Delete test artifacts• Edit shared work item queries• Add teams and team administrators• Create and manage area and iteration paths• Edit project-level permissions• Customize a project (On-premises XML or Hosted process models)
Project collection-level permissions	<ul style="list-style-type: none">• Create, delete, or edit a process (Inheritance process model)• Delete field from account (Inheritance process model)• Manage process permissions (Inheritance process model)• Edit collection level permissions <p>Project collection-level permissions include all permissions you can set at the project-level.</p>

[Edit project-level or collection-level/instance-level information](#)

The **Edit project-level information** and **Edit instance-level information** (also referred to as Edit collection-level information) provide permissions to several work tracking features as summarized below. To add users or set permissions at these levels, see [Add administrators, set permissions at the project-level or project collection-level](#).

EDIT PROJECT-LEVEL INFORMATION	EDIT INSTANCE-LEVEL INFORMATION
<ul style="list-style-type: none"> • Add and administer teams and all team-related features • Create and modify areas and iterations • Edit shared work item queries • Edit project level permission ACLs • Manage process templates • Customize a project • Create and modify global lists • Edit event subscriptions (email or SOAP) on project level events. 	<ul style="list-style-type: none"> • Add and administer teams and all team-related features • Create and modify areas and iterations • Edit check-in policies • Edit shared work item queries • Edit project level and collection level permission ACLs • Manage process templates • Customize a project or process • Create and modify global lists • Edit event subscriptions (email or SOAP) on project or collection level events.

Create child nodes, modify work items under an area path

Area path permissions let you grant or restrict access to edit or modify work items, test cases, or test plans assigned to those areas. You can restrict access to users or groups. You can also set permissions for who can add or modify areas or iterations for the project.

You define both areas and iterations for a project from the **Project Settings>Work>Project configuration**.

1. Choose (1) **Project Settings**, expand **Work** if needed, and choose (2) **Project configuration** and then (3) **Areas**.

The screenshot shows the Azure DevOps interface for a project named "Fabrikam Fiber". The left sidebar has a red box around the "Project settings" button, with a red circle containing the number "1" above it. The main content area shows the "Project Settings > Project configuration" screen. A red box highlights the "Areas" tab in the "Work" section, with a red circle containing the number "3" above it. Below the tabs, there is descriptive text about managing areas and a table listing areas and their associated teams. A red box highlights the "Project configuration" button in the "Boards" section, with a red circle containing the number "2" above it.

Areas	Teams
Fabrikam Fiber	Fabrikam Fiber Team, Management team
Customer Service	Customer Service, Fabrikam Fiber Team
Email	Email, Fabrikam Fiber Team
Phone	Fabrikam Fiber Team, Phone
Voice	Fabrikam Fiber Team, Voice
Web	Fabrikam Fiber Team, Web

2. Choose the ... context menu for the node you want to manage and select **Security**.

Work

Iterations [Areas](#)

Create and manage the areas for this project. These areas will be used by teams to determine what shows up on the backlog and Kanban boards. [Learn more about customizing areas and iterations](#)

To select areas for the team, go to [the default team's settings](#).

New New child | +/-

Areas	Teams
✓ Fabrikam Fiber	Fabrikam Fiber Team, Management team
Customer Service	... Customer Service, Fabrikam Fiber Team
Phone	New 1, Phone
Voice	New child 1, Voice
Web	Edit 1, Web
	Delete
	Security

3. Select the group or team member, and then change the permission settings. If you don't see the group you want, try adding it first.

For example, here we've added the Disallow Access Group, and disallowed members of this group the ability to view, modify, or edit work items in the Customer Service area path.

Permissions for Customer Service

+ Add... Inheritance ▾

Search

Azure DevOps Groups

- Disallow access group
- Build Administrators
- Contributors
- Readers
- Team Admins
- Project Collection Build Service Accounts
- Project Collection Test Service Accounts

Users

- Fabrikam Fiber Build Service (kelliott)
- Project Collection Build Service (kelliott)

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Create child nodes	Deny
Delete this node	Deny
Edit this node	Deny
Edit work items in this node	Deny
Manage test plans	Deny
Manage test suites	Deny
View permissions for this node	Deny
View work items in this node	Deny

Clear explicit permissions

Remove Save changes Undo changes

Close

You can specify two explicit authorization states for permissions: **Deny** and **Allow**. In addition, permissions can exist in one of three additional states. To learn more, see [About permissions and groups](#).

1. From the web portal for the project, choose the gear icon.

The screenshot shows the Azure DevOps web portal's top navigation bar. The 'Work' tab is highlighted in blue, indicating the current context. Other tabs include 'Dashboards', 'Code', 'Build and Release', 'Test', and 'Wiki'. A gear icon in the top right corner is highlighted with a red box.

If you're currently working from a team context, then hover over the and choose **Project settings**.

The screenshot shows the 'Files' view for the 'Fabrikam Fiber' project. The left sidebar lists files like 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md'. The right pane shows a table of contents with items like 'page-1.md', 'page-2.md', 'page-3.md', and 'README.md'. A context menu is open over the 'Customer Service' item in the 'Areas' section, listing options: 'New', 'New child', 'Edit', 'Delete', and 'Security'. The 'Project settings' option is highlighted with a red box and has a red arrow pointing to it from the gear icon in the top right corner of the page.

2. Choose **Work** and then **Areas**.

3. Choose the ... context menu for the node you want to manage and select **Security**.

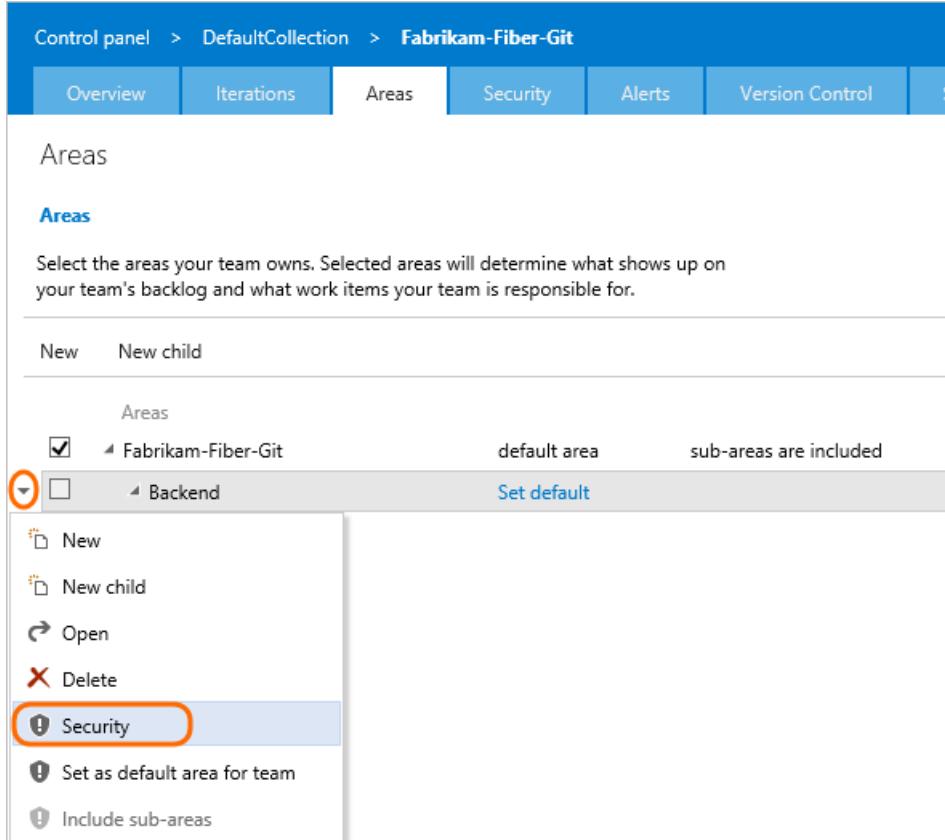
The screenshot shows the 'Areas' management screen. It displays a tree structure of areas under 'Fabrikam Fiber', including 'Customer Service', 'Phone', 'Voice', and 'Web'. A context menu is open over the 'Customer Service' node, listing 'New', 'New child', 'Edit', 'Delete', and 'Security'. The 'Security' option is highlighted with a red box.

1. From the web portal, choose the gear icon to open project administration pages. Then choose

Areas.



2. Choose the context menu for the node you want to manage.



The screenshot shows the 'Areas' configuration screen. At the top, it displays the path: Control panel > DefaultCollection > Fabrikam-Fiber-Git. Below this is a navigation bar with tabs: Overview, Iterations, Areas, Security, Alerts, Version Control, and Settings. The 'Areas' tab is selected. The main content area is titled 'Areas' and contains the following text: 'Select the areas your team owns. Selected areas will determine what shows up on your team's backlog and what work items your team is responsible for.' Below this, there are buttons for 'New' and 'New child'. The 'Backend' area is listed under 'Areas', with a checked checkbox next to it. To the right of the checkbox, it says 'default area' and 'sub-areas are included'. A context menu is open over the 'Backend' area, listing options: New, New child, Open, Delete, Security (which is highlighted with an orange circle), Set as default area for team, and Include sub-areas.

3. Select the group or team member, and then change the permission settings. If you don't see the group you want, try adding it first.

For example, here we've added the Disallow Access Group, and disallowed members of this group the ability to view, modify, or edit work items in the Customer Service area path.

Permissions for Customer Service

Permission	Value
Create child nodes	Deny
Delete this node	Deny
Edit this node	Deny
Edit work items in this node	Deny
Manage test plans	Deny
Manage test suites	Deny
View permissions for this node	Deny
View work items in this node	Deny

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Remove Save changes Undo changes

Close

You can specify two explicit authorization states for permissions: **Deny** and **Allow**. In addition, permissions can exist in one of three additional states. To learn more, see [About permissions and groups](#).

Define and edit queries or query folders

You can specify who can add or edit query folders or queries at the object-level. To manage permissions for a query or query folder, you must be the creator of the query or folder, a member of the Project Administrators or Project Collection Administrators group, or granted explicit access through the object's Security dialog.

Query folder Permissions dialog

Permissions for Shared Queries/Service Delivery team

The screenshot shows the 'Permissions' dialog for a shared query. On the left, a tree view lists 'DevOps Groups' (Service Delivery, Build Administrators, Contributors, Project Administrators) and 'Users' (Project Collection Build Service (fabrikam)). On the right, the 'ACCESS CONTROL SUMMARY' section displays permissions for the 'Service Delivery' group:

Action	Permission
Contribute	Allow
Delete	Allow
Manage Permissions	Not set
Read	Allow (inherited)

Buttons at the bottom include 'Clear explicit permissions', 'Remove', 'Save changes', 'Undo changes', and 'Close'.

For details, see [Set permissions on a shared query or query folder](#). To learn more about queries, see [Create managed queries to list, update, or chart work items](#).

Edit or manage permissions for Delivery Plans

Delivery Plans are an object within a project. You manage plan permissions for each plan similar to the way you manage permissions for shared queries or query folders. The creator of a Delivery Plan as well as all members of the Project Collection Administrators and Project Administrators groups have permissions to edit, manage, and delete plans.

Delivery Plan Permissions dialog

The screenshot shows the 'Permissions' dialog for a specific delivery plan. On the left, a tree view lists 'Azure DevOps Groups' (Project Administrators, Project Collection Administrators, Project Collection Valid Users) and 'Users' (Raisa Pokrovskaya, Jamal Hartnett). On the right, the 'ACCESS CONTROL SUMMARY' section displays permissions for the 'Raisa Pokrovskaya' user:

Action	Permission
Delete	Allow
Edit	Allow
Manage	Allow
View	Allow (inherited)

A red box highlights the 'Allow' permission for the 'Edit' action. Buttons at the bottom include 'Clear explicit permissions', 'Remove', 'Save changes', 'Undo changes', and 'Close'.

To learn more, see [Edit or manage Delivery Plan permissions](#). To learn more about Delivery Plans, see [Review team plans](#).

Move or permanently delete work items

By default, Project Administrators and Contributors can change the work item type and delete work items by moving them to the Recycle bin. Only Project Administrators can permanently delete work items and test artifacts. Project admins can grant permissions to other team members as needed.

For example, as a project admin you can grant a user, team group, or other group you've created to have these permissions. Open the Security page for the project and choose the user or group you want to grant permissions. (To learn how to access project-level **Security**, see [Set permissions at the project-level or project collection-level](#).)

In this example, we grant members assigned to the team administrator role, who belong to the Team Admin groups, permissions to move work items to another project and to permanently delete work items.

The screenshot shows the 'Create group' interface in Azure DevOps. On the left, there's a sidebar with 'Teams' and 'Azure DevOps Groups' sections. On the right, the 'Fabrikam Fiber > Team Admins' group details are shown, including a permissions table and 'Save changes' and 'Undo changes' buttons.

Permissions	Members	Member of
Create tag definition	Allow	
Create test runs	Allow	
Delete and restore work items	Not set	
Delete team project	Allow	
Delete test runs	Not set	
Edit project-level information	Not set	
Manage project properties	Not set	
Manage test configurations	Not set	
Manage test environments	Not set	
Move work items out of this project	Allow	
Permanently delete work items	Allow	
Rename team project	Not set	
View project-level information	Not set	
View test runs	Not set	

[Clear explicit permissions](#)

[Save changes](#) [Undo changes](#)

Manage test artifacts

In addition to the project-level permissions set in the previous section, team members need permissions to manage test artifacts which are set for an area path.

Open the **Security** page for area paths and choose the user or group you want to grant permissions.

Iterations **Areas**

Create and manage the areas for this project. These areas will be used by teams to determine what shows up on the backlog.

To access the default team's area settings, [click here](#).

New New child | + -

Areas	Teams
▼ Fabrikam Fiber	... Fabrikam Fiber Team
Customer Service	New Fabrikam Fiber Team
Phone	New child Phone
Voice	Edit
Web	Delete Web
	Security

Set the permissions for **Manage test plans** and **Manage test suites** to **Allow**.

Permissions for Fabrikam Fiber

Add... ▾

Search

▼ VSTS Groups

- Team Admins
- Build Administrators
- Contributors
- Readers
- Project Collection Build Service Accounts
- Project Collection Test Service Accounts

› Users

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Create child nodes	Not set
Delete this node	Not set
Edit this node	Not set
Edit work items in this node	Allow
Manage test plans	Allow
Manage test suites	Allow
View permissions for this node	Allow
View work items in this node	Allow

[Clear explicit permissions](#)

Remove Save changes Undo changes

Close

To have full access to the Test feature set, your [access level must be set to Basic + Test Plans](#). Users with Basic access and with permissions to permanently delete work items and manage test artifacts can only delete orphaned test cases.

Customize an inherited process

By default, only Project Collection Administrators can create and edit processes. However, these admins can grant permissions to other team members by explicitly setting the **Create process**, **Delete process**, or **Edit process** permissions at the collection level for a specific user.

To customize a process, you need to grant **Edit process** permissions to a user account for the specific process.

1. Open the ... context menu for the inherited process and choose **Security**. To open this page, see [Customize a project using an inherited process](#).

The screenshot shows a list of processes under a collection. The 'MyAgile (default)' process is selected. A context menu is open over it, with the 'Security' option highlighted by a red box.

Name	Description
Agile	This template is flexible and will work great for most tea...
Agile111	Test description
MyAgile (default)	...
MyAgile 2	+ New team project Edit → Change team projects to use MyAgile Disable process Delete Security
Scrum	apps development
Custom scrum	
CMMI	
CMMI 1	

2. Add the account name of the person you want to grant permissions to, set the permissions to **Allow** that you want them to have, and then choose **Save changes**.

Here we add Christie Church and allow her to edit the process.

The dialog box shows the 'Permissions for MyAgile' settings. Under 'ACCESS CONTROL SUMMARY', 'Edit process' is set to 'Allow'. The 'Christie Church' user is selected, and the 'Edit process' permission is also set to 'Allow'. Buttons for 'Remove', 'Save changes', and 'Undo changes' are visible.

Access Control Summary
Shows information about the permissions being granted to this identity
Administer process permissions Deny
Delete process Deny
Edit process Allow
Clear explicit permissions
Remove Save changes Undo changes

NOTE

Each process is a securable unit and has individual access control lists (ACLs) that govern creating, editing, and deleting inherited processes. At the collection level, project collection administrators can choose which processes can be inherited from and by whom. When you create a new inherited process, the process creator as well as project collection administrators have full control of the process and can also set individual ACLs for other users and groups to edit and delete the process.

Additional options for restricting access to work items

NOTE

You can use one or more of the following options with the On-premises XML process models. To learn more about process models, see [Customize work tracking experience](#).

You can restrict access to work tracking objects in one of two ways:

- By [adding WITs to the Hidden Categories group](#), you can prevent the majority of project contributors from creating them. You [can create a hyperlink to a template](#) that opens the work item form and share that link with those team members who you do want to create them.
- [Set a condition field rule](#), [a condition-based field rule](#) or a combination of the two that applies to a group. You can restrict changes from being made to a field by specifying a qualifying rule and making it apply for a specific group. Conditional rules can include **CANNOTLOSEVALUE**, **EMPTY**, **FROZEN**, **NOTSAMEAS**, **READONLY**, and **REQUIRED** elements.

For more information about how to customize WITs, see [Modify or add a custom work item type \(WIT\)](#).

Related articles

- [Set permissions on queries and query folders](#)
- [Permissions and access for work tracking](#)
- [Permissions and groups reference](#)

Give reviewers permissions to provide feedback

1/25/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You provide feedback to users that you plan to [request feedback](#) from. Reviewers who aren't members of your team require special permissions to provide feedback using the Microsoft Feedback Client.

Add reviewers to your team project

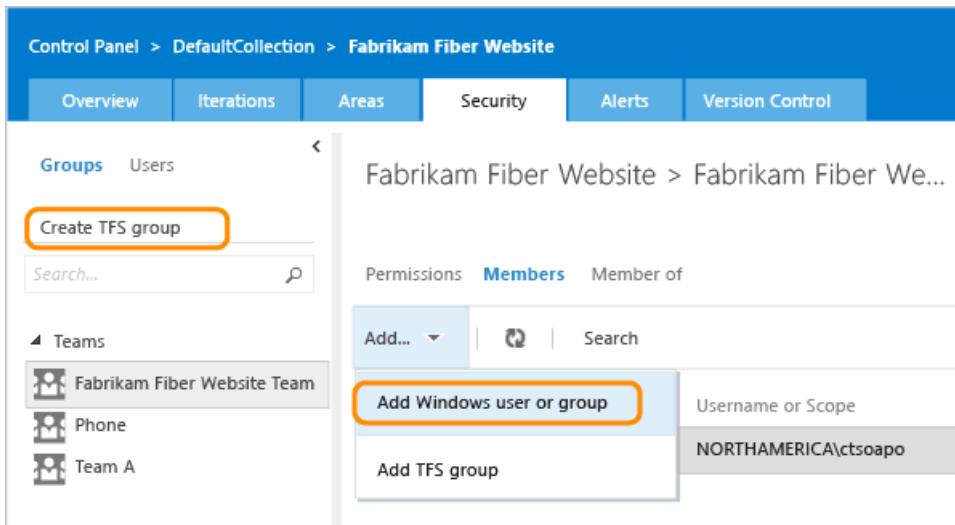
1. From the web portal of your team project home page, open the administration context.



The screenshot shows the top navigation bar of the TFS 2015 web interface. It includes the 'Visual Studio Team Foundation Server 2015' logo, the current project name 'Fabrikam Fiber', the user 'Helena Peterson', and a gear icon which is highlighted with a yellow box. Below the navigation bar is a horizontal menu with links: HOME, CODE, WORK, BUILD, TEST. To the right of the menu is a search bar labeled 'Search work items' with a magnifying glass icon. Underneath the menu, there's a link 'Overview' which is underlined, indicating it's the active page.

If you aren't a member of the **Project Administrators** or **Team Foundation Administrators** group, get added. See [Add an administrator](#). You'll need to be a member in order to add users and groups to a team project, change permissions, and grant them access to the web portal.

2. Create a group for your reviewers.



The screenshot shows the 'Control Panel > DefaultCollection > Fabrikam Fiber Website' interface. The 'Security' tab is selected. On the left, there are tabs for 'Groups' and 'Users'. A button 'Create TFS group' is highlighted with a yellow box. In the main area, there are tabs for 'Permissions', 'Members', and 'Member of'. Under 'Members', there is a search bar and a dropdown menu with options: 'Add...', 'Add Windows user or group', and 'Add TFS group'. The 'Add Windows user or group' option is highlighted with a yellow box. On the right, a list shows a single entry: 'Username or Scope' followed by 'NORTHAMERICA\ctsoapo'.

Tip: If you have a lot of reviewers, creating a Windows, VSO, or TFS group helps you manage permissions more efficiently.

3. Name your group.

CREATE NEW TEAM FOUNDATION SERVER GROUP

PROFILE



Group Name
Reviewers

Description
Group for managing feedback reviewers with limited access to team project.

Create Group **Cancel**

4. Add accounts to your group.

Control Panel > DefaultCollection > Fabrikam Fiber Website

Overview Iterations Areas Security Alerts Version Control

Groups Users

Create TFS group

Search... 

- Teams
 - Fabrikam Fiber Website Team
- TFS groups
 - Build Administrator
 - Contributors
 - Project Administrators
 - Project Valid Users
 - Readers
 - Reviewers**

Fabrikam Fiber Website > Reviewers | Edit... ▾

Permissions Members Member of

Add...  Search

Add Windows user or group 

Username or Scope

Add TFS group

ADD A WINDOWS USER OR GROUP

To add a Windows user or group that is not currently known to Team Foundation Server, type the domain/user... the identity is known, just type the display name.

Identities Annie Herriman (Fabrikam)  Ming-Yang Xie (Fabrikam)  Roberto Tamburello (Fabrikam) 

Display Name or Domain\Username  

Save Changes

Set permissions so reviewers can provide feedback

Allow reviewers to **Create test runs**, **View project-level information**, and **View test runs**.

Control Panel > DefaultCollection > Fabrikam Fiber Website

Overview Iterations Areas Team field Security Alerts Version Control

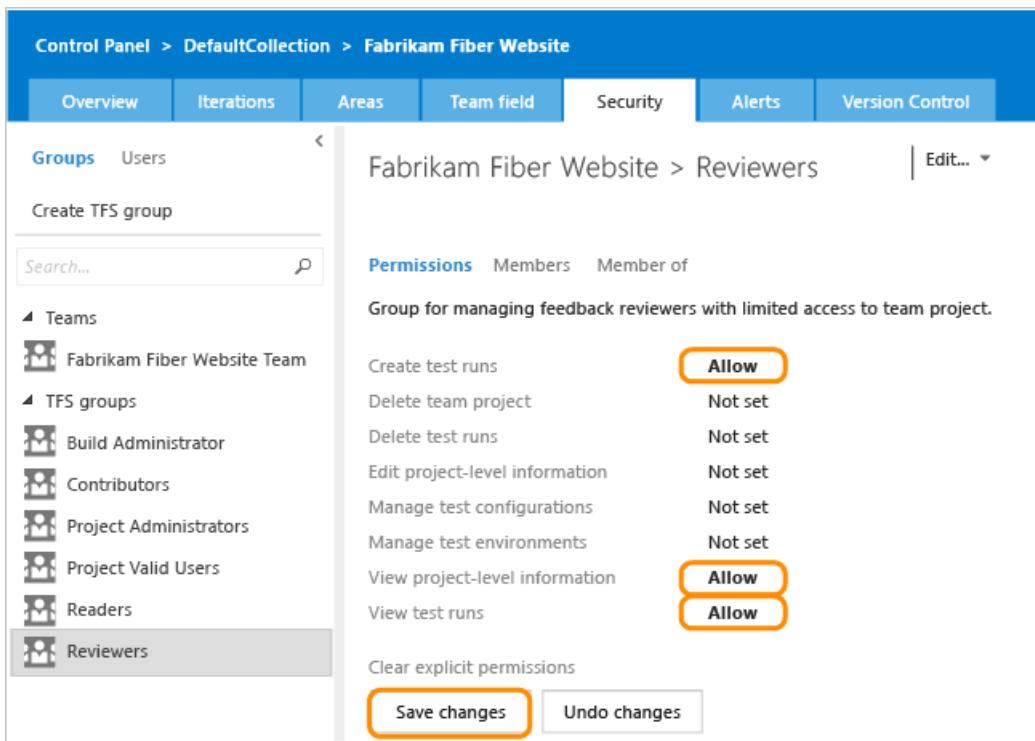
Groups Users Create TFS group Search... ▾ Teams Fabrikam Fiber Website Team ▾ TFS groups Build Administrator Contributors Project Administrators Project Valid Users Readers Reviewers

Fabrikam Fiber Website > Reviewers Edit... ▾

Permissions Members Member of Group for managing feedback reviewers with limited access to team project.

Action	Allow
Create test runs	Allow
Delete team project	Not set
Delete test runs	Not set
Edit project-level information	Not set
Manage test configurations	Not set
Manage test environments	Not set
View project-level information	Allow
View test runs	Allow

Clear explicit permissions Save changes Undo changes



Set permissions so reviewers can modify work items

Since feedback is captured in a feedback response work item, reviewers need to be able to modify work items in the product areas they will review.

1. Open security for the team project.

Control Panel > DefaultCollection > Fabrikam Fiber Website

Overview Iterations Areas Security Alerts Version Control

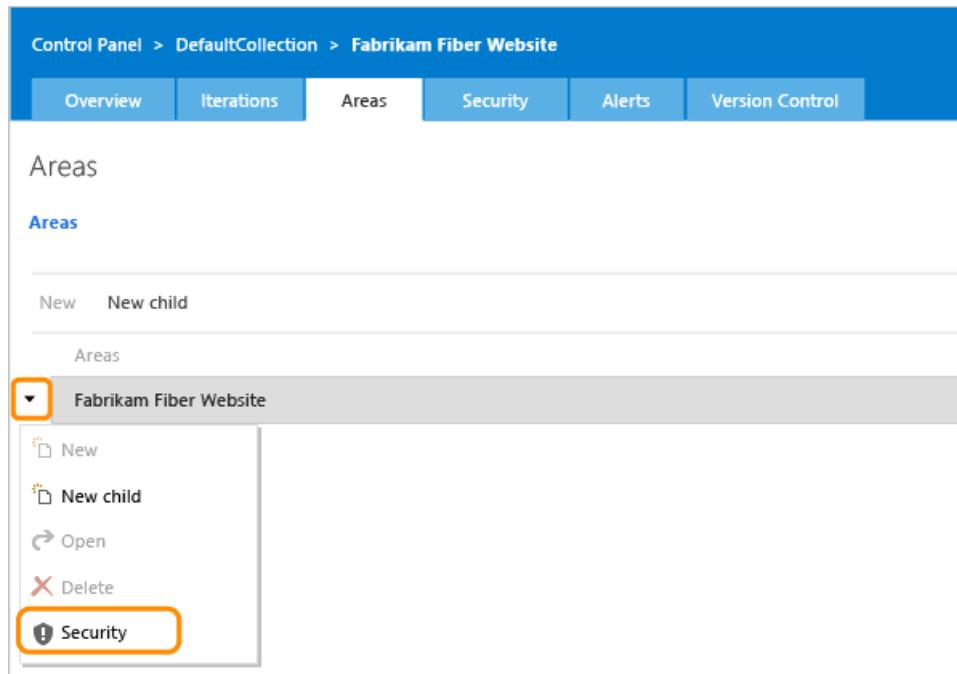
Areas

Areas New New child

Areas

Fabrikam Fiber Website

- New
- New child
- Open
- Delete
- Security



2. Add the reviews group to the **VSO Groups** or **TFS Groups**.

PERMISSIONS FOR FABRIKAM FIBER WEBSITE

Add... ▾

Add Windows identity

Add TFS group

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted...

Create child nodes	not set
Delete this node	not set
Edit this node	not set

ADD A WINDOWS USER OR GROUP

Fabrikam Fiber Website

To add explicit permissions for a Windows user or group, type their display name or Domain\U...

Identity R browse

- [Fabrikam Fiber Website]\Fabrikam Fiber Website Team
- [Fabrikam Fiber Website]\Project Administrators
- [Fabrikam Fiber Website]\Project Valid Users
- [Fabrikam Fiber Website]\Readers
- [Fabrikam Fiber Website]\Reviewers**
- [TEAM FOUNDATION]\Project Server Integr...

- Allow reviewers to Edit work items in this node and View work items in this node.

PERMISSIONS FOR FABRIKAM FIBER WEBSITE

Add... ▾

Search...

▲ TFS groups

- Reviewers**
- Project Collection Build Service Acc...
- Project Collection Test Service Acc...
- Build Administrators
- Contributors
- Readers

▼ Users

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted...

Create child nodes	Not set
Delete this node	Not set
Edit this node	Not set
Edit work items in this node	Allow
Manage test plans	Not set
View permissions for this node	Not set
View work items in this node	Allow

Clear explicit permissions

Remove Save changes Undo changes

If you want, allow reviewers the ability to modify their feedback submissions

Sometimes additional ideas occur after reviewers submit their feedback. By providing access to the web portal, reviewers can revisit and further annotate their feedback submissions.

- Azure DevOps Services:** Assign the **Stakeholder** license to accounts that you add to your Reviewer group
- On-premises TFS:** Add your Reviewer group to the **Stakeholder** group on the [access levels page](#). If you don't see this tab, get administrative permissions.

Control panel

Control panel Access levels Extensions

Export audit log

Limited Standard (default) Full

Access levels

Name Limited
Features View My Work Items

Access levels only apply to features in Team Web Access. For more information, [see...](#)

Set as default access levels Add... Search

Display Name Add Windows user or group
No identities found in cur... Add TFS group

The screenshot shows the 'Access levels' section of the Control panel. It lists three options: 'Limited' (selected and highlighted), 'Standard (default)', and 'Full'. Under 'Limited', it shows 'Name: Limited' and 'Features: View My Work Items'. A note says 'Access levels only apply to features in Team Web Access. For more information, see...'. Below are buttons for 'Set as default access levels', 'Add...', 'Search', 'Display Name', 'Add Windows user or group', and 'Add TFS group'. The 'Add...' button and the 'Add TFS group' button are specifically highlighted with orange boxes.

Your reviewers will be able to view and modify only those work items that they create, which includes feedback responses. The [Stakeholder group provides limited access](#) to features and data for those members of your organization who do not have a TFS client access license (CAL).

Related articles

- [Initiate a feedback request](#)
- [Respond to a feedback request](#)
- [Work as a stakeholder](#)

Grant permissions to manage extensions

7/3/2019 • 2 minutes to read • [Edit Online](#)

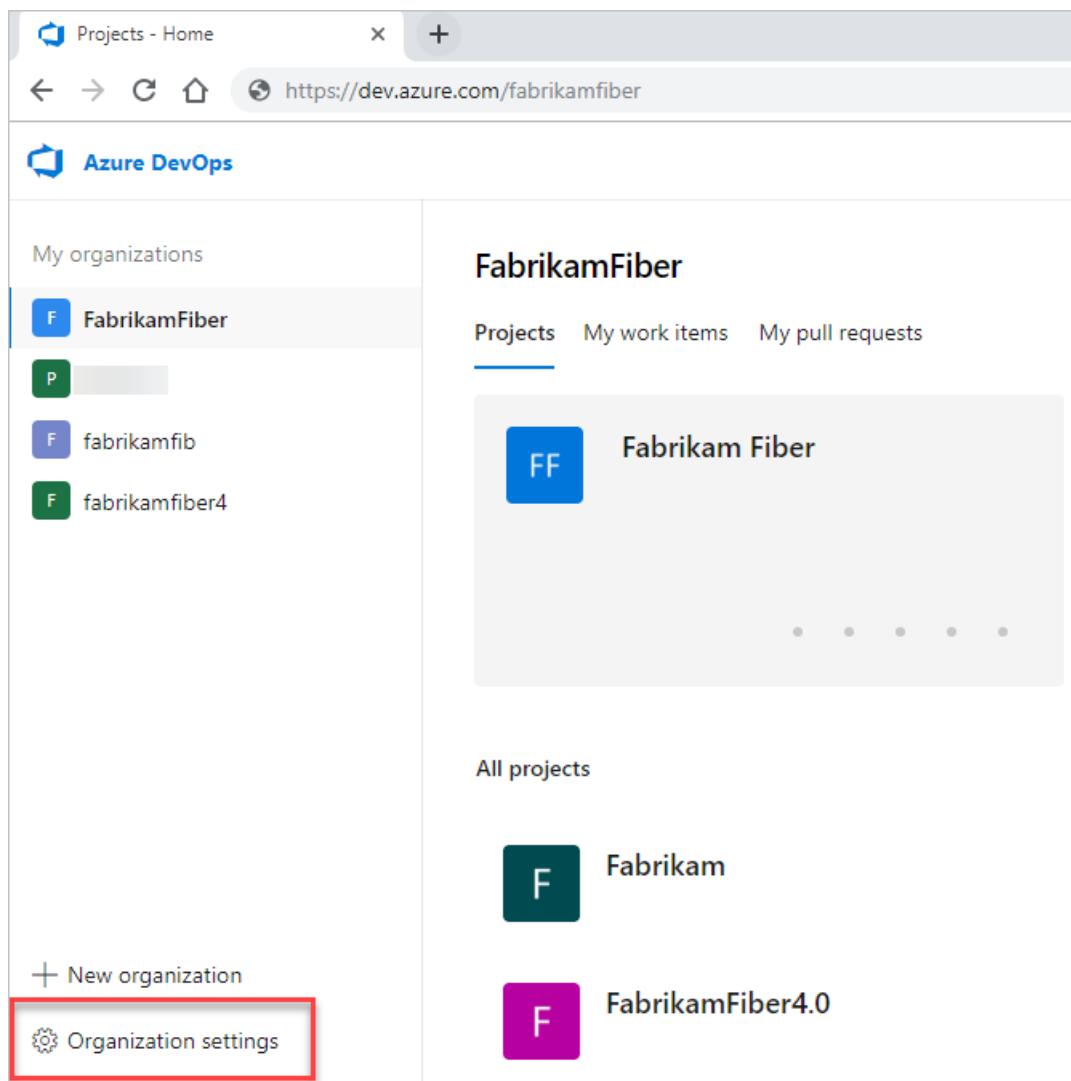
Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

In this article, learn how to grant permissions for managing extensions, like install, disable, enable, review, and approve an extension.

In this article, learn how to grant permissions for publishing or updating extensions for users or groups.

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

2. Select **Organization settings**.



3. Select **Extensions**.

 Azure DevOps

FabrikamFiber / Organization Settings / Extensions / Installed

Organization Settings	Extensions
General	Installed Requested Shared
Overview	Analytics by Microsoft Gain insights into the health and status of your Azure DevOps Server projects Not Supported: Team Foundation Server 2018 and prior versions.
Users	
Billing	
Auditing	
Global notifications	
Usage	
Extensions	
Azure Active Directory	

4. Select **Security** in the upper right of the Extension Security page:

FabrikamFiber / Organization Settings / Extensions / Installed

Search JH

Extensions **Security** Browse marketplace

Installed Requested Shared

 Analytics by Microsoft
Gain insights into the health and status of your Azure DevOps Server projects.
Not Supported: Team Foundation Server 2018 and prior versions.

5. Add users or update permission settings:

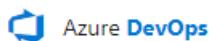
Security

Add Inheritance

User	Role	Access
[FabrikamFiber]\Project Collection Administrat	Manager Assigned	

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

2. Select  **Admin settings**.



Collections

D DefaultCollection

Related pages

Documentation

Get help

Access levels

Admin settings

Collection Settings

- General
- Projects
- Security
- Notifications
- Extensions
- Boards
- Process
- Pipelines
- Agent pools
- Deployment pools
- Retention
- OAuth configurations

3. Select **Extensions**, and then select **Security**.

The screenshot shows the 'Extensions' page in the Azure DevOps interface. On the left, there's a sidebar with 'Collection Settings' and a list of categories: General, Projects, Global notifications, Extensions (which is highlighted with a red box), Security, Boards, and Process. The main area is titled 'Extensions' and shows a single item: 'Test Manager (Azure Test Plans)'. At the top right, there are buttons for Refresh, Security (which is highlighted with a red box), Browse Marketplace, and Browse local extensions. The 'Security' button has a small lock icon next to it.

4. Add users or update permission settings:

The screenshot shows the 'Security' settings page. At the top, there's a header with 'Security' and buttons for '+ Add' (highlighted with a red box), 'Inheritance', and a dropdown for 'Role'. Below this, there's a table with columns: User, Role, and Access. A single row is shown: '[FabrikamFiber]\Project Collection Administrat' (the user name is cut off) with 'Manager' selected in the Role dropdown (highlighted with a red box) and 'Assigned' in the Access column.

To grant permissions for publishing or updating to users or groups, use [TFS Security](#) command-line tool.

1. At the server level, create a group, for example, "TFS Extension Publishers":

```
tfssecurity /gca "TFS Extension Publishers" "publishers who can manage extensions for the server"  
/server:ServerURL
```

2. Grant access to the "TFS Extension Publishers" group to manage extensions:

```
tfssecurity /a+ Publisher //" CreatePublisher n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL  
tfssecurity /a+ Publisher //" PublishExtension n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL  
tfssecurity /a+ Publisher //" UpdateExtension n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL  
tfssecurity /a+ Publisher //" DeleteExtension n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL
```

For Team Foundation Server "15" RC2 or earlier, use this syntax:

```
tfssecurity /a+ Publisher //" Create n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL  
tfssecurity /a+ Publisher //" Publish n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL  
tfssecurity /a+ Publisher //" Write n:"[TEAM FOUNDATION]\TFS Extension Publishers" allow  
/server:ServerURL
```

3. Add existing users and groups to the "TFS Extension Publishers" group.

```
tfssecurity /g+ "[TEAM FOUNDATION]\TFS Extension Publishers" n:User /server:ServerURL
```

You can add users later to "TFS Extension Publishers". This is a server-level permission, so updating and deleting an extension will affect all the project collections that use the extension.

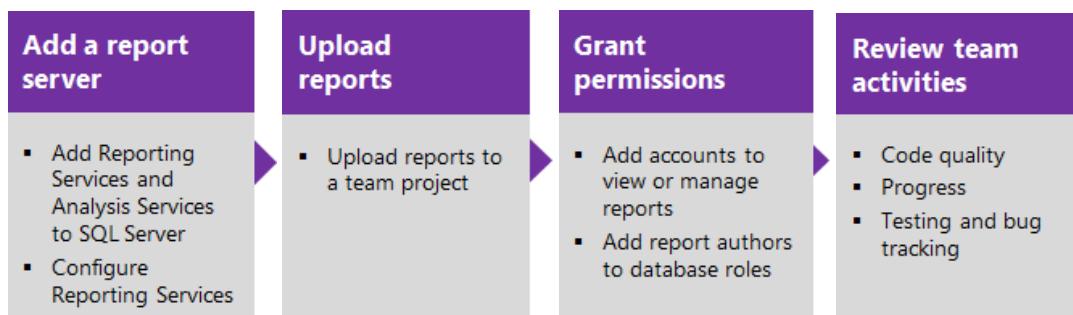
Grant permissions to view or create SQL Server reports in TFS

5/24/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Note: Azure DevOps Server was previously named Visual Studio Team Foundation Server.

This is the third task in the four-task sequence to add reports to your team project. You can use the procedures in this article to set permissions to view or author reports.



IMPORTANT

Feature availability: You can only add a report server to an on-premises TFS. If you're using Azure DevOps, adding a report server isn't a supported option, instead, you can use the [Analytics Service](#).

Now that you've uploaded reports, you'll want to enable members of your team to view or manage them. Also, to create or modify reports, you'll need to grant them access to read databases.

Add accounts to predefined roles to view or manage reports

Add report viewers to the **Browser** role. Add TFS report authors to the **Team Foundation Content Manager** role.

TIP

Permissions to access Report Manager are managed separately from TFS permissions. Even if you have added team members to a TFS group, you will still have to add them to a Report Manager role.

1. If you haven't been added to the **Content Manager** role for Reporting Services, get added by someone who has been added to this role.
2. From the Report Manager home page, open **Folder Settings**.

The screenshot shows the 'SQL Server Reporting Services Home' page. At the top, there are buttons for 'New Folder', 'New Data Source', 'Report Builder', and 'Folder Settings'. The 'Folder Settings' button is highlighted with an orange box. Below the toolbar, there are two items in the folder list: 'TfsReports' and 'Tfs2010ReportDS'. The URL in the address bar is <http://ReportServer/Reports/Pages/Folder.aspx>.

The URL is <http://ReportServer/Reports/Pages/Folder.aspx>, or if using a named instance, http://ReportServer/Reports_InstanceId/Pages/Folder.aspx.

3. Open New Role Assignment.

The screenshot shows the 'SQL Server Reporting Services Home' page with the 'Security' section selected. A 'New Role Assignment' button is highlighted with an orange box. The table below lists role assignments:

	Group or User	Role(s)
<input type="checkbox"/>	BUILTIN\Administrators	Content Manager
<input type="checkbox"/>	NORTHAMERICA\ctsdev1	Content Manager
<input type="checkbox"/>	NORTHAMERICA\ctsdev2	Content Manager
<input type="checkbox"/>	NT AUTHORITY\NETWORK SERVICE	Team Foundation Content Manager

TIP

To limit access to reports defined for a team project or team project collection, first navigate to the corresponding folder and then open New Role Assignment.

4. Add the account name and select their role.

The screenshot shows the 'New Role Assignment' dialog box. The 'Group or user name' field contains 'NORTHAMERICA\cts...' and is highlighted with an orange box. The 'Role' table lists several roles, with 'Team Foundation Content Manager' checked and highlighted with an orange box.

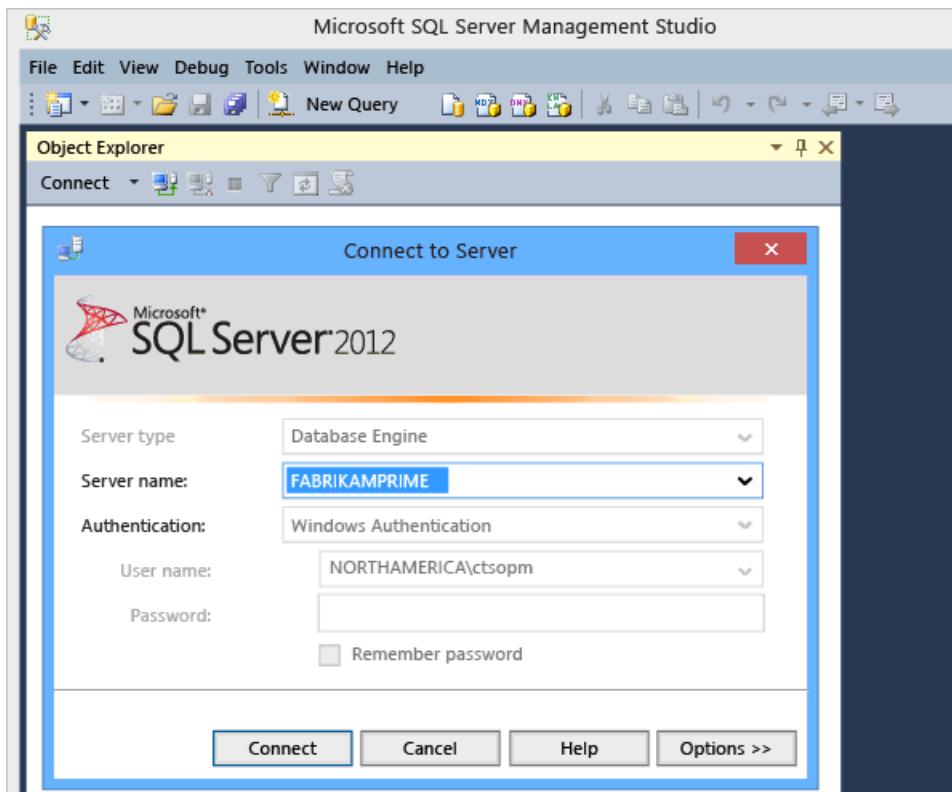
Role	Description
<input type="checkbox"/> Browser	May view folders, reports and subscribe to reports.
<input type="checkbox"/> Content Manager	May manage content in the Report Server. This includes... reports and resources
<input type="checkbox"/> My Reports	May publish reports and linked reports; manage folders, r... resources in a users My Reports folder.
<input type="checkbox"/> Publisher	May publish reports and linked reports to the Report Serv...
<input type="checkbox"/> Report Builder	May view report definitions.
<input checked="" type="checkbox"/> Team Foundation Content Manager	May manage Team Foundation Server related content in th... Server. This includes folders, reports and resources.

Buttons at the bottom are 'OK' and 'Cancel'.

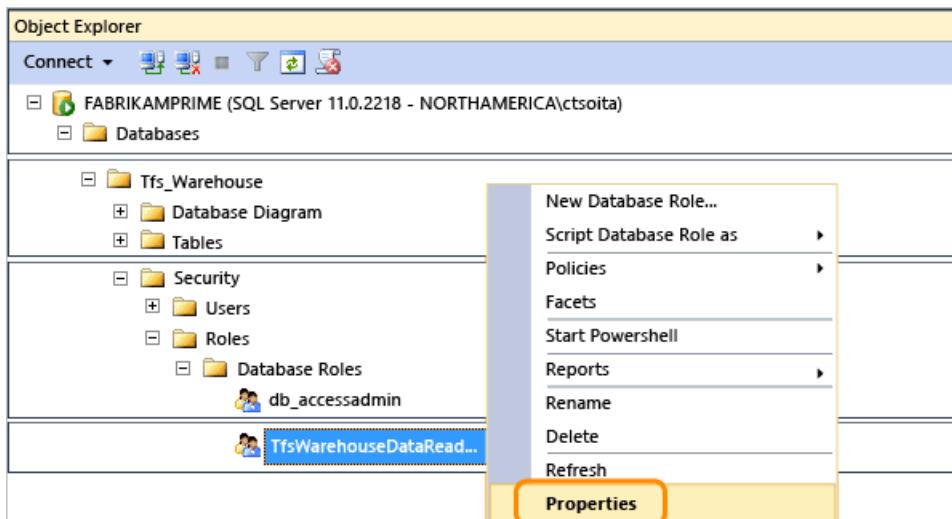
Add report authors to database roles

If members need to create or customize reports, add their accounts to the **TfsWarehouseDataReader** role. Report authors need read access to both the relational data warehouse and Analysis Services cube. Team members who create Excel reports from work item queries or by connecting to the cube need only read access to the cube.

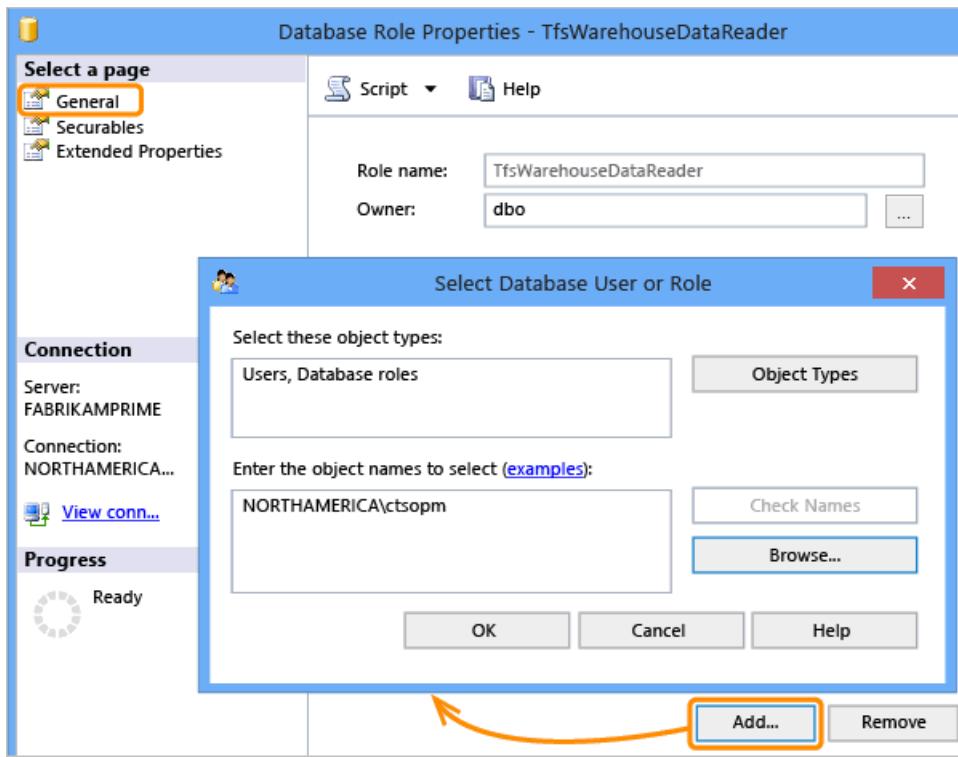
1. If you aren't an administrator for the TFS database, [get added as one](#).
2. Connect to the **Database Engine** for TFS using **SQL Server Management Studio**.



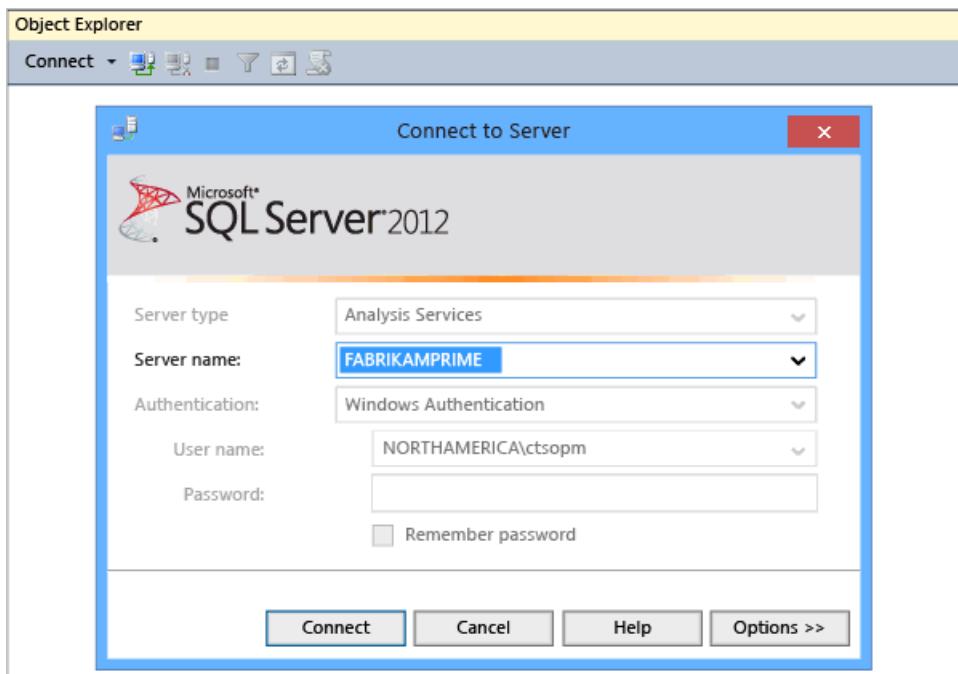
3. Open the properties page for the **TfsWarehouseDataReader** role under the **Databases/Tfs_Warehouse/organizations/security/Roles/Database Roles** folder.



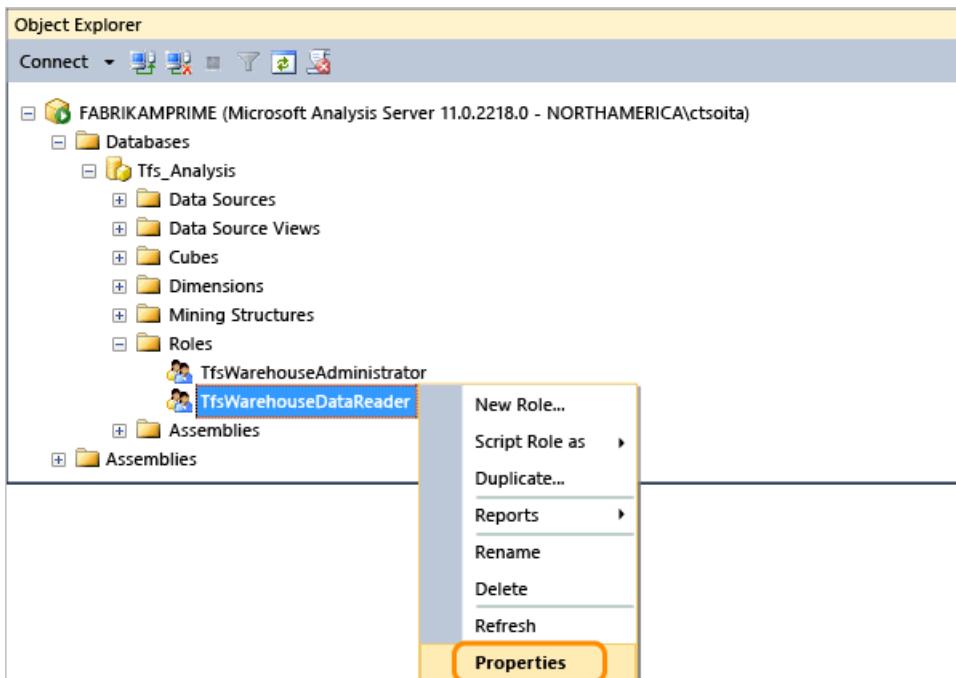
4. Add the account.



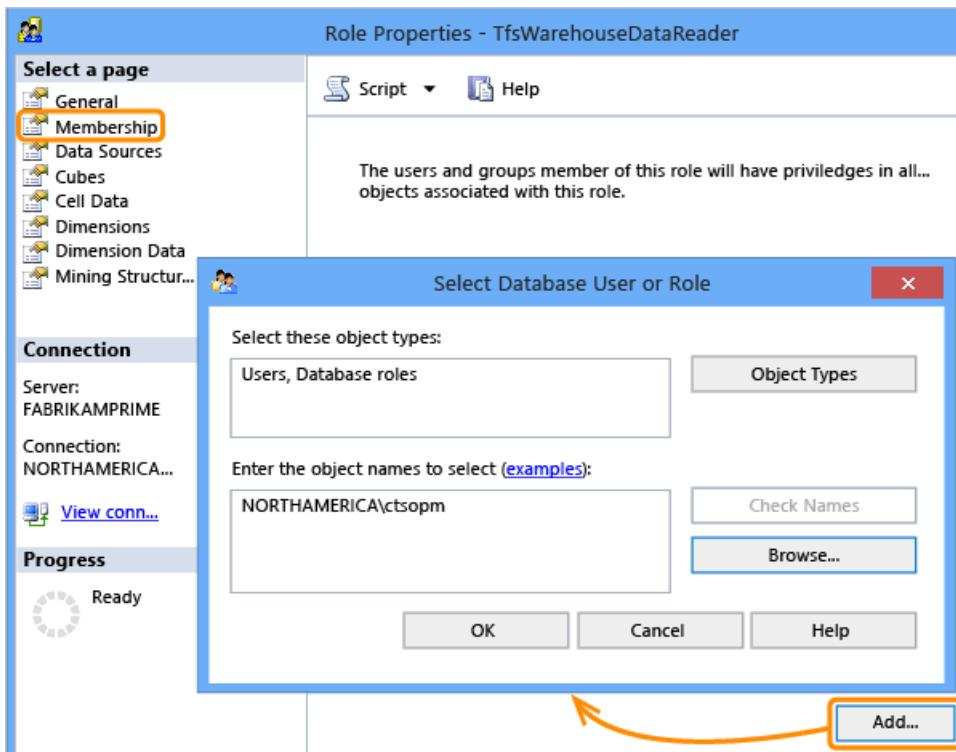
5. Next, connect to the **Analysis Services** database.



6. Open the properties page for the **TfsWarehouseDataReader** role under the **Databases/Tfs_Analysis/Roles** folder.



7. Add the account.



IMPORTANT

Accounts that you add to the **TfsWarehouseDataReader** roles can view data for all team projects that are hosted in all team project collections in the TFS deployment. There is no way to limit access to a team project or collection.

Try this next

- Review team activities to support useful reports.

Related notes

- Create Excel reports from a work item query

Set SharePoint site permissions

3/5/2019 • 2 minutes to read • [Edit Online](#)

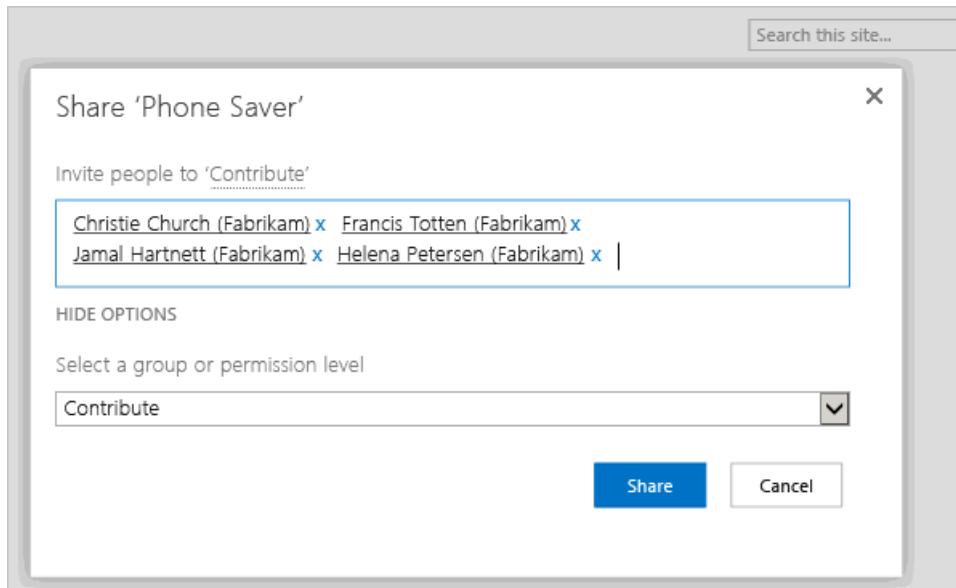
[TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

IMPORTANT

Integration with a SharePoint site is only supported for on-premises TFS. For information on what is supported for Azure DevOps, see [Dashboards and reports overview](#). If you don't have a site and want to add it, see [Configure or add a project portal](#).

Add users to SharePoint site

1. Open your project portal.
2. Choose **Share**, and add users or user groups to the appropriate SharePoint groups.



- To add users who require minimal access to the project, choose **Readers**.
- To add users who contribute fully to this project, choose **Contributors**.
- To add users who act as project leads, choose **Full Control**.

For more information about users and groups in SharePoint Products, [go here](#).

If your TFS deployment is integrated with SQL Server Reporting Services, you'll need to manage users in the appropriate SQL Server Reporting Services groups, or they won't be able to view or edit those reports.

Add a user account as an administrator of the SharePoint site

1. On the server that's running SharePoint Products, open SharePoint Central Administration.
2. Grant permissions that are appropriate for this user at the farm or the Web application level, depending on your security needs.

For optimum interoperability, consider adding users of the **Team Foundation Administrators** group to the following groups in SharePoint Products:

- **Farm Administrators**
- **Site Collection Administrators** group for all site collections that the deployment of Team Foundation Server uses



Quickstart: Connect to a project in Azure DevOps

6/21/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In this quickstart, you learn how to connect to a project in order to share code, build apps, track work, and collaborate with team members, from one of the following clients:

- [Web portal](#)
- [Visual Studio or Team Explorer](#)
- [Eclipse/Team Explorer Everywhere](#)
- [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. Within that collection, one or more projects may be defined. At a minimum, at least one project must be created in order to use the system. For more information, see [About projects and scaling your organization](#).

Prerequisites

- If you don't have a project yet, [create one](#). If you need to add a team, see [Add teams](#). If you don't have access to the project, [get invited to the team](#).
- From each of these clients, you can quickly switch context to a different project and connect under a different sign-in user name. If you work remotely, configure your client to [connect to a TFS Proxy server](#).
- To get started with a code base, [set up Git](#) or [set up TFVC](#).

Connect from the web portal

1. If you're not a member of a security group, ask your project administrator to add you.
2. Open a browser window and enter a URL that uses the following form:

```
https://dev.azure.com/OrganizationName/ProjectName
```

```
http://ServerName:8080/tfs/DefaultCollection/ProjectName
```

For example, to connect to the server named **FabrikamPrime**, type:

<http://FabrikamPrime:8080/tfs/>.

The default Port is 8080. Specify the port number and directory for your server if defaults aren't used.

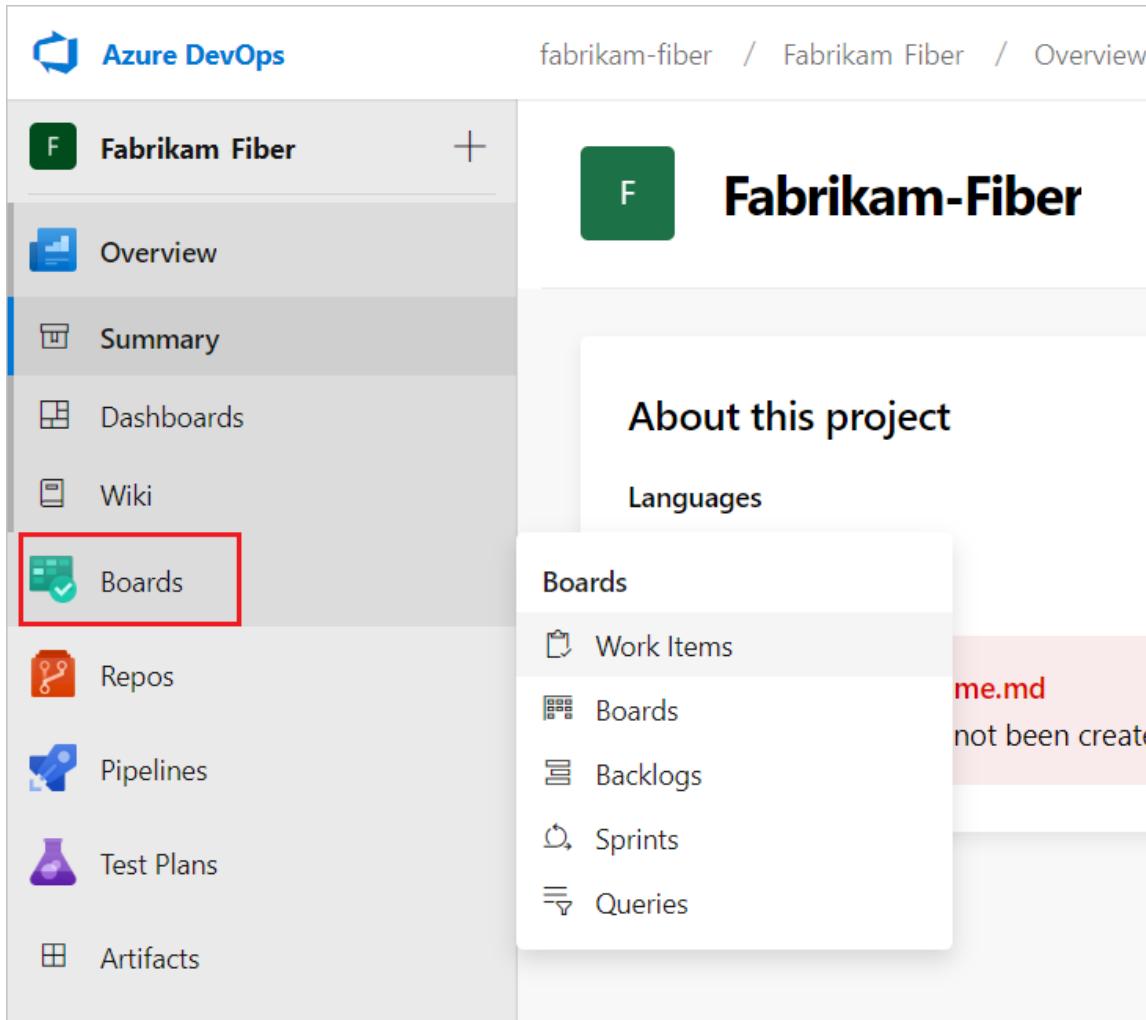
3. When you access the server for the first time, a Windows Identity dialog box appears. Fill in your credentials and choose the **OK** button.

TIP

If you select the **Remember me** check box you won't have to enter your credentials the next time you connect.

4. Choose your project, team, or page of interest.

From the project summary page, hover over a service and then choose the desired page. To choose another project, choose the  Azure DevOps logo.



The screenshot shows the Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, a sidebar lists various project services: Overview, Summary (selected), Dashboards, Wiki, Boards (highlighted with a red box), Repos, Pipelines, Test Plans, and Artifacts. On the right, the main content area displays the 'Fabrikam-Fiber' project summary. A tooltip for the 'Boards' service in the sidebar is open, showing five options: Work Items, Boards, Backlogs, Sprints, and Queries. The 'Boards' option is highlighted in the tooltip. The main content area also includes sections for 'About this project' and 'Languages'.

From the project summary page, hover over a service and then choose the desired page. To choose another project, choose the  Azure DevOps logo.

The screenshot shows the Microsoft Team Foundation Server 2015 interface. At the top, there is a navigation bar with links for 'Fabrikam Fiber', 'Dashboards', 'Code', 'Work' (which is highlighted with a red box), 'Build and release', 'Test', and 'Wiki'. Below the navigation bar, the project 'Fabrikam Fiber' is displayed with a star icon. A sidebar on the right contains links for 'Work Items', 'Backlogs', 'Queries', 'Plans', and a 'New work item' button. The main content area shows a file named 'Fabrikam Fiber / README.md' with the following text:

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 can do.
[Learn more](#) ↗ about Markdown.

[page 1](#)
[page 2](#)
[page 3 - verifying this works as advertised](#)

Choose your project or team from the set of available links, or choose [Browse](#) to access all projects and teams.

The screenshot shows the Microsoft Team Foundation Server 2015 Overview page. At the top, it says 'Visual Studio Team Foundation Server 2015'. Below that, there are tabs for 'Overview' (which is selected) and 'Rooms'. The main content area has a heading 'About Team Foundation Server' with four purple buttons:

- Features**
What does Team Foundation Server have to offer?
- Learn**
Access online help for Team Foundation Server
- Get Visual Studio**
View all the download options
- Administer**
Manage projects, users, groups and permissions

Below these buttons, there are sections for 'Recent projects & teams' and 'Recent team rooms'.

Recent projects & teams

[Browse](#)

- [Fabrikam Fiber / Web Service](#)
2 minutes ago
- [Fabrikam Fiber](#)
21 hours ago
- [Fabrikam Fiber / Migrate](#)
5/27/2016
- [Fabrikam Fiber / Fiber Suite](#)
2/3/2016

Recent team rooms

[Fabrikam Fiber Team Room](#)
0 users in room

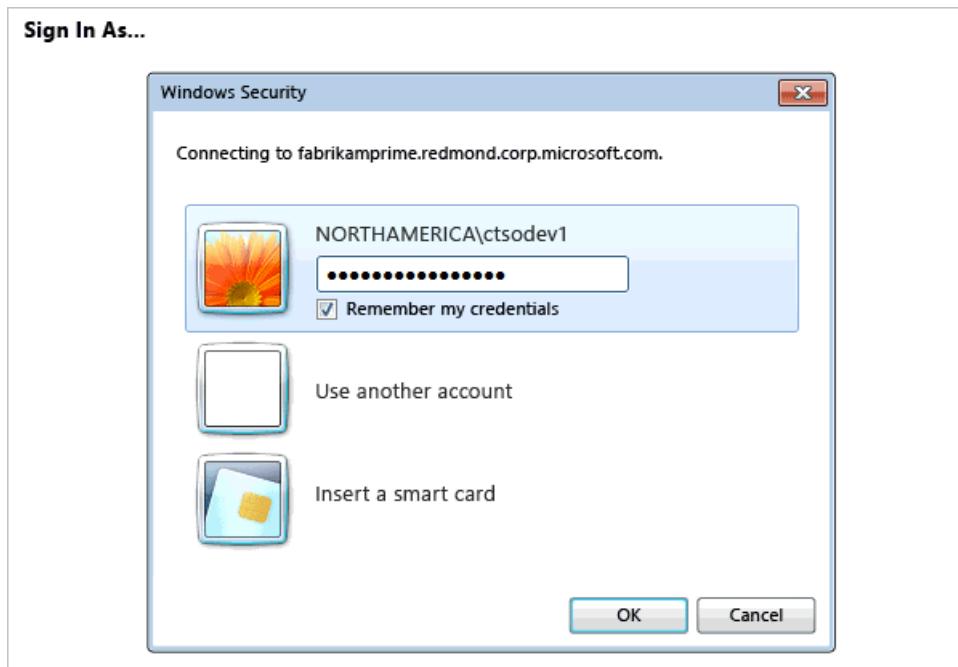
To learn more about each page and the tasks you can perform, see [Web portal navigation](#).

Sign in with different credentials

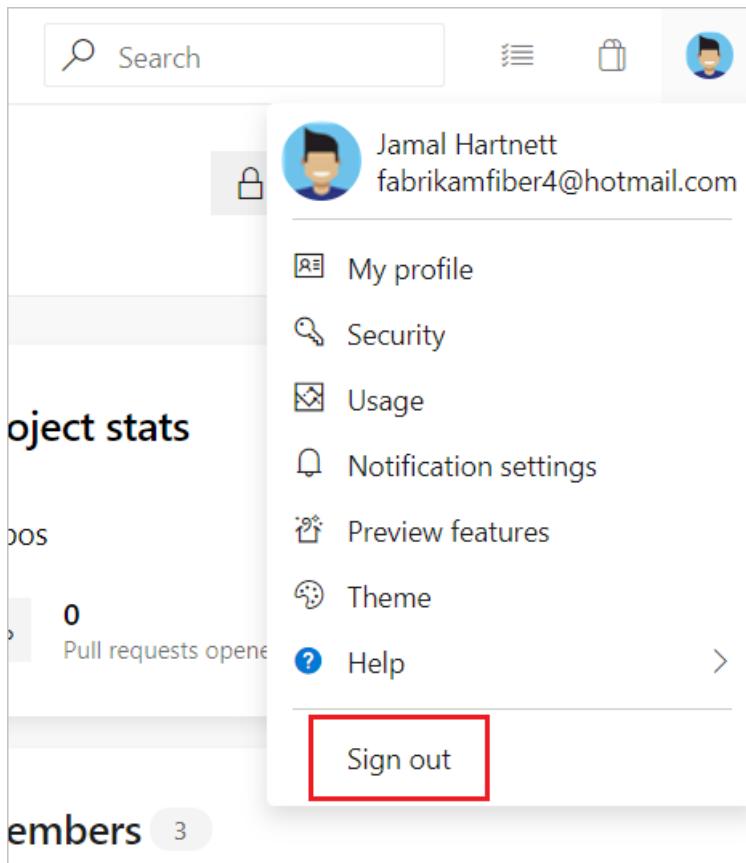
1. Open Windows Security from the context menu associated with your name.

The screenshot shows the Visual Studio Team Foundation Server 2015 interface. At the top, the title bar reads "Visual Studio Team Foundation Server 2015 / Fabrikam Fiber". The navigation bar includes links for HOME, CODE, WORK, BUILD, TEST, and RELEASE. Below the navigation bar, there are two sections: "Visual Studio" and "Get Visual Studio". The "Visual Studio" section contains a "Open in Visual Studio" button (requires VS 2013+) and a "Get Visual Studio" button (see downloads). On the right side, there is a user profile menu for "Raisa Pokrovskaya" (ms). The menu items are "My profile", "My alerts", "Sign in as...", "Sign out", and "NORTHAMERICA\ctsodev1". The "Sign in as..." option is highlighted with an orange circle. A search bar at the top right contains the text "ms".

2. Enter your credentials.



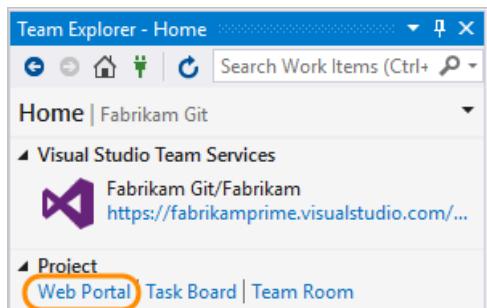
1. Open your profile menu and choose **Sign out**.



2. Choose Sign in and enter the new credentials.

Open the web portal from Team Explorer

- Open the web portal from the home page.

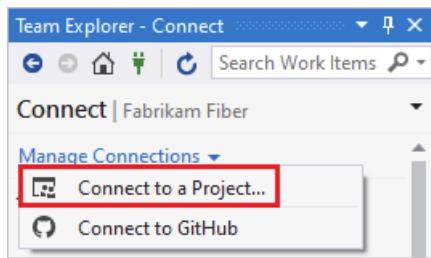


Connect from Visual Studio or Team Explorer

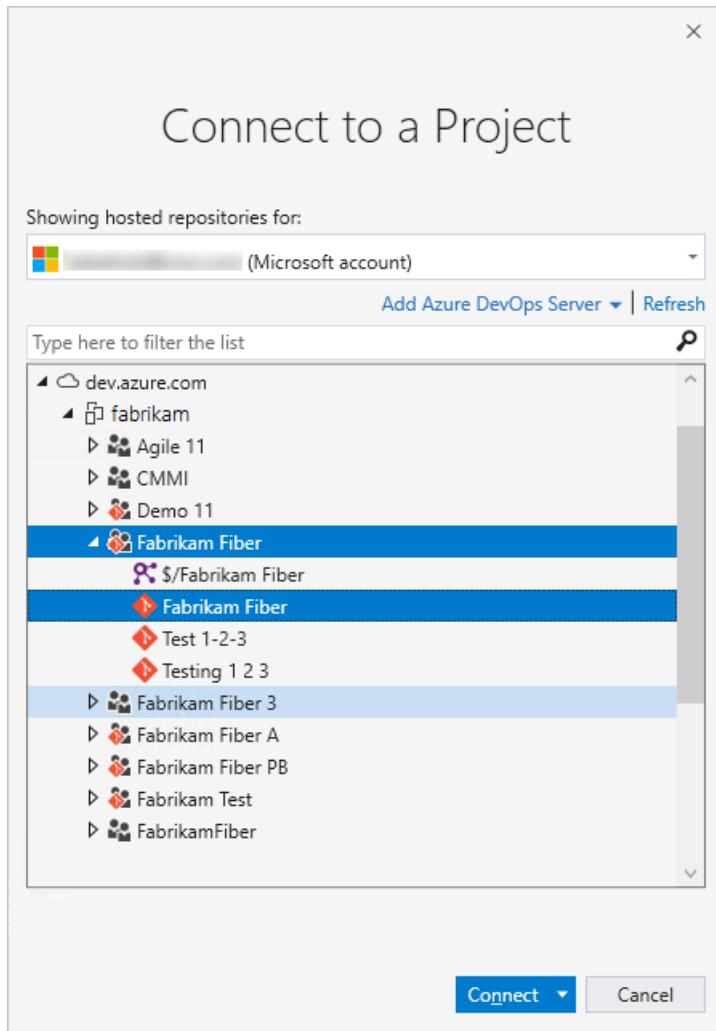
1. If you haven't already, [download and install a version of Visual Studio](#).
2. If you're not a member of an Azure DevOps security group, [get added to one](#).
3. Check with a team member to determine the names of the server, project collection, and project to connect to.
 - [Visual Studio 2019](#)
 - [Visual Studio 2017](#)
 - [Visual Studio 2015](#)

Visual Studio 2019

Select the connect icon in Team Explorer to open up the **Connect** page. Choose the **Connect to Team Project** link to select a project to connect to.



The **Connect to a Project** dialog appears and shows the projects you can connect to, along with the repos in those projects.



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



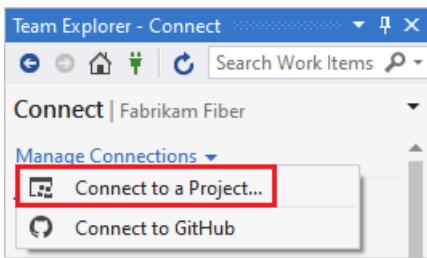
Select a project from the list and select **Connect**.

Change sign-in credentials

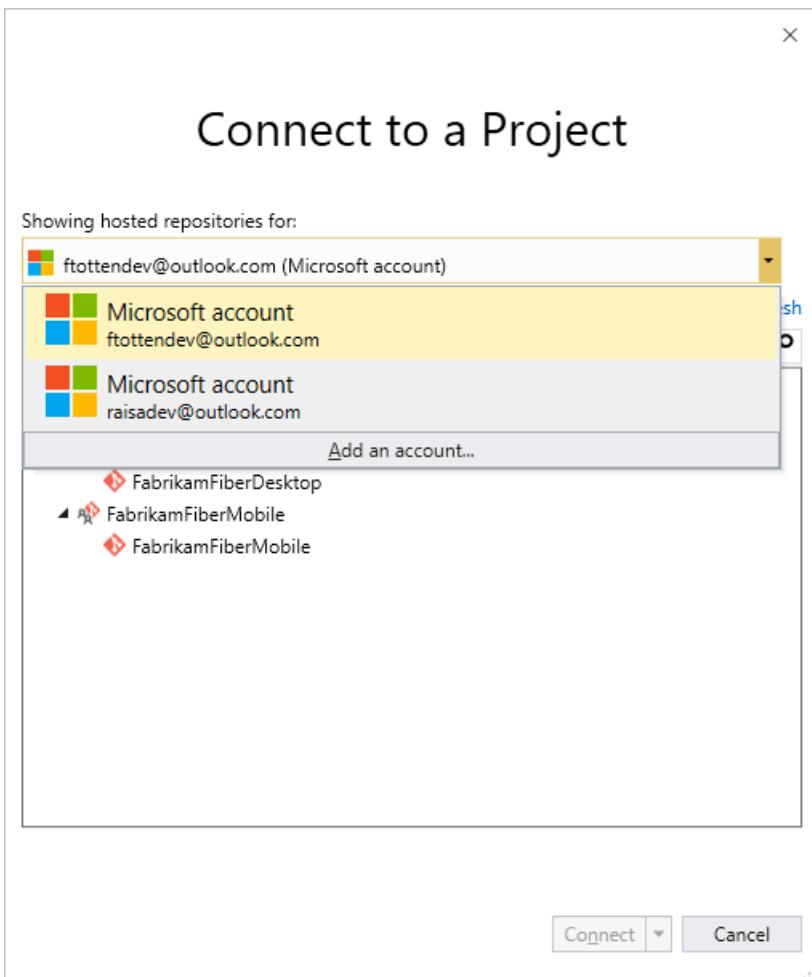
- Visual Studio 2019
- Visual Studio 2017
- Visual Studio 2015

Visual Studio 2019

1. From the Connect page, choose the **Connect to a Project** link to sign in with different credentials.

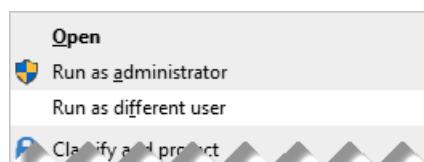


Select a different user from the drop-down or select **Add an account...** to access a project using different sign-in credentials.



2. Sign in using an account that is associated with an Azure DevOps project, either a valid Microsoft account or GitHub account.

To run Visual Studio under sign-in credentials that are different from your signed-in Windows account, open the context menu for **devenv.exe** to access your run as options. If you don't see the **run as** option as shown in the following example, you may need to press SHIFT before right-clicking to see the run as options.



You can locate the executable in the following folder:

```
*Drive*:\\Program Files (x86)\\Microsoft Visual Studio xx.0\\Common7\\IDE\\
```

User accounts and licensing for Visual Studio

To connect to a project, you need your user account added to the project. This is typically done by the [organization owner \(Azure DevOps Services\)](#) or a [project administrator](#).

Azure DevOps Services provides access to the first 5 account users free. After that, you need to [pay for more users](#).

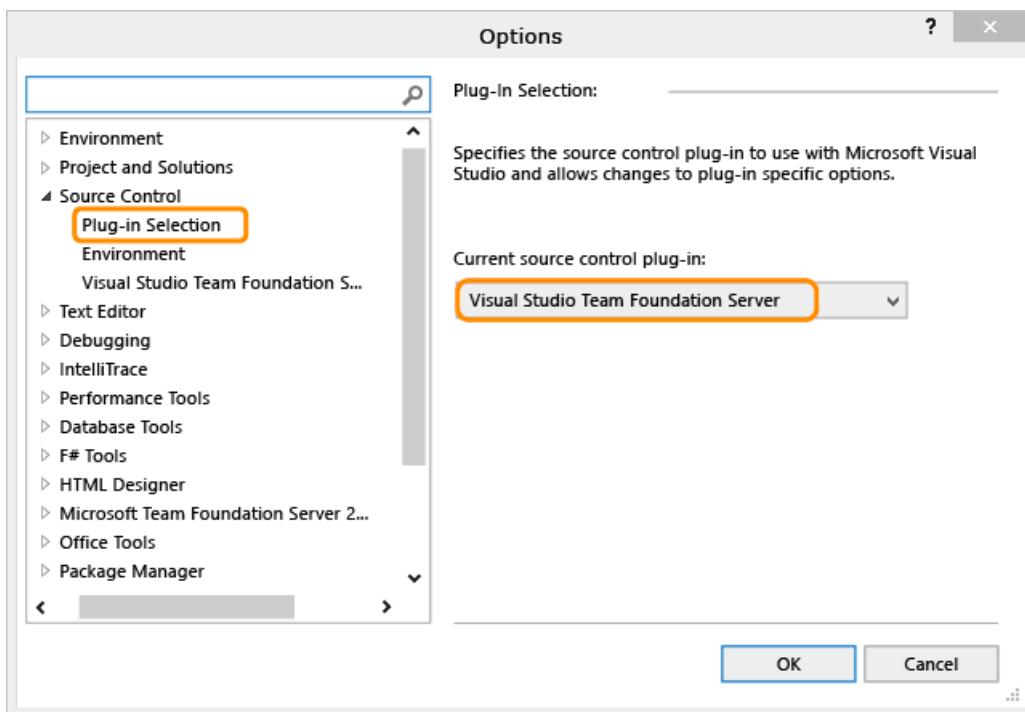
For on-premises TFS, each user account must have a TFS client access license (CAL). All Visual Studio subscriptions and paid Azure DevOps Services users include a TFS CAL. Find out more about licensing from the [Team Foundation Server pricing page](#).

In addition, you can provide access to Stakeholders in your organization who have limited access to select features as described in [Work as a Stakeholder](#).

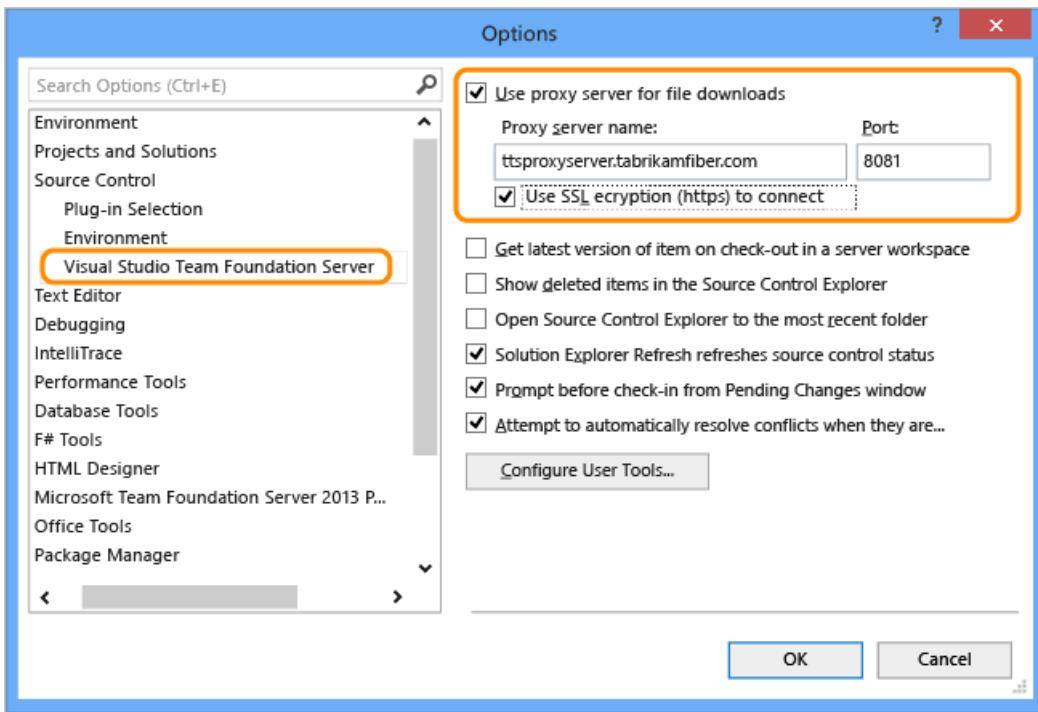
Configure Visual Studio to connect to TFS Proxy

If your remote team uses a [TFS 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. First, make sure that you have connected to TFS as described [in the previous section](#).
2. From the Visual Studio **Tools** menu, open the Options dialog and expand the Source Control folder. On the Plug-in Selection page, confirm that Visual Studio Team Foundation Server is selected.



3. On the Visual Studio Team Foundation Server page, enter the name and port number for the TFS Proxy server. Select the **Use SSL encryption (https) to connect** checkbox.



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

To **Configure User Tools** 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](#).

What other clients support connection to Azure DevOps?

In addition to connecting through a web browser, Visual Studio, Eclipse, Excel, and Project you can connect to a project from these clients:

- [Visual Studio Code](#)
- [Visual Studio Community](#)
- [Eclipse: Team Explorer Everywhere](#)
- [Azure Test Plans](#) (formerly Test Manager)
- [Microsoft Feedback Client](#)

Requirements and client compatibility

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

Determine your platform version

See [Feedback and support](#).

Next steps

Learn more about how to:

- [Work in web portal](#)
- [Work in Team Explorer](#)
- [Work in Office Excel or Project](#)
- [Troubleshoot connection](#)

If all you need is a code repository and bug tracking solution, then start with the [Git get started guide](#) and [Manage bugs](#).

To start planning and tracking work, see [Get started with Agile tools to plan and track work](#).

Authenticate access with personal access tokens

6/18/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

Personal access tokens (PATs) are alternate passwords that you can use to authenticate into Azure DevOps. In this article, we walk you through how to create or revoke PATS.

Azure DevOps uses enterprise-grade authentication to help protect and secure your data. Clients like Visual Studio and Eclipse (with the Team Explorer Everywhere plug-in) also support Microsoft account and Azure AD authentication. Since PATs are an alternate form of user authentication, using a PAT gives you the same access level. If you create a PAT with a narrower scope, your access is limited to that particular scope.

For non-Microsoft tools that integrate into Azure DevOps but don't support Microsoft account or Azure AD authentication, you must use PATs. Examples include Git, NuGet, or Xcode. To set up PATs for non-Microsoft tools, use [Git credential managers](#) or create them manually.

Create personal access tokens to authenticate access

1. Sign in to either your organization in Azure DevOps (<https://dev.azure.com/{yourorganization}>) or your Team Foundation Server web portal (<https://{server}:8080/tfs/>).
2. From your home page, open your profile. Go to your security details.

Azure DevOps Services

TFS 2017

3. Create a personal access token.

4. Name your token. Select a lifespan for your token.

If you're using Azure DevOps Services, and you have more than one organization, you can also select the organization where you want to use the token.

5. Select the [scopes](#) for this token to authorize for *your specific tasks*.

For example, to create a token to enable a [build and release agent](#) to authenticate to Azure DevOps Services or TFS, limit your token's scope to **Agent Pools (read, manage)**.

6. When you're done, make sure to *copy the token*. You'll use this token as your password.

NOTE

Remember that this token is your identity and acts as you when it's used. Keep your tokens secret and treat them like your password.

To keep your token more secure, use credential managers so that you don't have to enter your credentials every time. Here are some recommended credential managers:

- Git: [Git Credential Manager for macOS and Linux](#) or [Git Credential Manager for Windows](#) (requires [Git for Windows](#))
- NuGet: [NuGet Credential Provider](#)

Revoke personal access tokens to remove access

When you don't need your token anymore, just revoke it to remove access.

1. From your home page, open your profile. Go to your security details.

Azure DevOps Services



Azure DevOps Server (formerly TFS)



2. Revoke access.



See the following examples of using your PAT.

Username: `anything` Password: `your PAT here`

or

```
git clone https://anything:<PAT>@dev.azure.com/yourOrgName/yourProjectName/_git/yourRepoName
```

To learn more about how security and identity are managed, see [About security and identity](#).

To learn more about permissions and access levels for common user tasks, see [Default permissions and access for Azure DevOps](#).

For administrators to revoke organization user PATs, see [Revoke other users' personal access tokens](#).

Frequently asked questions

What is my Azure DevOps Services URL?

<https://dev.azure.com/{yourorganization}>

Where can I learn more about how to use PATs?

For examples of how to use PATs, see [Git credential managers](#), [REST APIs](#), [NuGet on a Mac](#), and [Reporting clients](#).

What notifications will I get about my PAT?

Users receive two notifications during the lifetime of a PAT, one at creation and the other seven days before the expiration.

The following notification is sent at PAT creation:

A new personal access token was added to your organization

[Learn more](#) about why you're receiving this email. If you did not make this change, your credentials may have been compromised and we suggest changing your password.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 10/30/2018

Origination IP

User agent

We sent you this notification due to a default subscription

Sent from Azure DevOps.

The following notification is sent - a PAT is near expiration:

One of your personal access tokens will be expiring on 8/4/2018.

Click below to manage your personal access tokens.

[Manage personal access tokens](#)

Summary

Token name Sentry integration

Scopes

Expiring on 8/4/2018

We sent you this notification due to a default subscription

Sent from Azure DevOps.

What do I do if I get an unexpected PAT notification?

An administrator or a tool might have created a PAT on your behalf. See the following examples:

- When you connect to an Azure DevOps Services Git repo through git.exe, it creates a token with a display name like "git: <https://MyOrganization.visualstudio.com/> on MyMachine."
- When you or an admin sets up an Azure App Service web app deployment, it creates a token with a display name like "Service Hooks :: Azure App Service :: Deploy web app."
- When you or an admin sets up web load testing as part of a pipeline, it creates a token with a display name like "WebAppLoadTestCDIntToken".
- When a Microsoft Teams Integration Messaging Extension is set up, it creates a token with a display name like "Microsoft Teams Integration".

If you still believe that a PAT exists in error, we suggest that you [revoke the PAT](#). Next, change your password. As an Azure Active Directory user, check with your administrator to see if your organization was used from an unknown source or location.

Revoke personal access tokens for organization users

5/7/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

If an organization user's personal access token (PAT) has been compromised, we recommend taking immediate action. Revoke their access tokens, as a precaution to protect your organization. In this article, we show you how administrators of Azure DevOps organizations can revoke PATs for users.

Prerequisites

Only an organization administrator or project collection administrator (PCA) can revoke user PATs. If you're not a member of the **Project Collection Administrators** group, [get added as one](#). To learn how to find your organization's admin, see [Look up administrators and organization owner](#).

For users, if you want to create or revoke your own PATs, see [Create or revoke personal access tokens](#).

Revoke PATs

1. To revoke the OAuth authorizations, including PATs, for your organization's users, see [Token revocations - Revoke authorizations](#).
2. Use this [PowerShell script](#) to automate calling the new REST API by passing a list of user principal names (UPNs). If you don't know the UPN of the user who created the PAT, use this script, however it must be based on a date range.

NOTE

Keep in mind that when you use a date range any JSON web tokens (JWTs) are also revoked. Also be aware that any tooling that relies on these tokens won't work until refreshed with new tokens.

1. After you've successfully revoked the affected PATs, let your users know. They can recreate their tokens, as needed.

Token expiration

FedAuth tokens

A FedAuth token is issued when you sign-in. It is valid for a seven day sliding window. The expiry automatically extends another seven days whenever you refresh it within the sliding window. If users access the service regularly, only an initial sign-in is needed. After a period of inactivity extending seven days, the token becomes invalid and the user must sign in again.

Personal access tokens

Users can choose an expiry date for their personal access token, not to exceed one year. We recommend you use shorter time periods, generating new PATs upon expiry. Users receive a notification email one week before token expiry. Users can generate a new token, extend expiry of the existing token, or change the scope of the existing token, if needed.

Frequently asked questions (FAQs)

What if a user leaves my company?

A: Once a user is removed from Azure AD, the PATs and FedAuth tokens are invalidated within an hour, since the refresh token is valid only for one hour.

What about JSON web tokens (JWTs)?

A: Revoke JWTs, issued as part of the OAuth flow, via the [PowerShell script](#). However, you must use the date range option in the script.

Related articles

- [How Microsoft protects your projects and data in Azure DevOps](#)
- [Create or revoke your personal access tokens](#)

Troubleshoot adding and deleting organization users

7/3/2019 • 12 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Permissions

Q: Why can't I manage users?

A: To access and manage users, you must have Azure DevOps [project collection administrator or organization owner permissions](#).

Q: How do I find a Project Collection Administrator?

A: If you have at least Basic access, you can find your [Project Collection Administrator](#) in your organization's security settings.

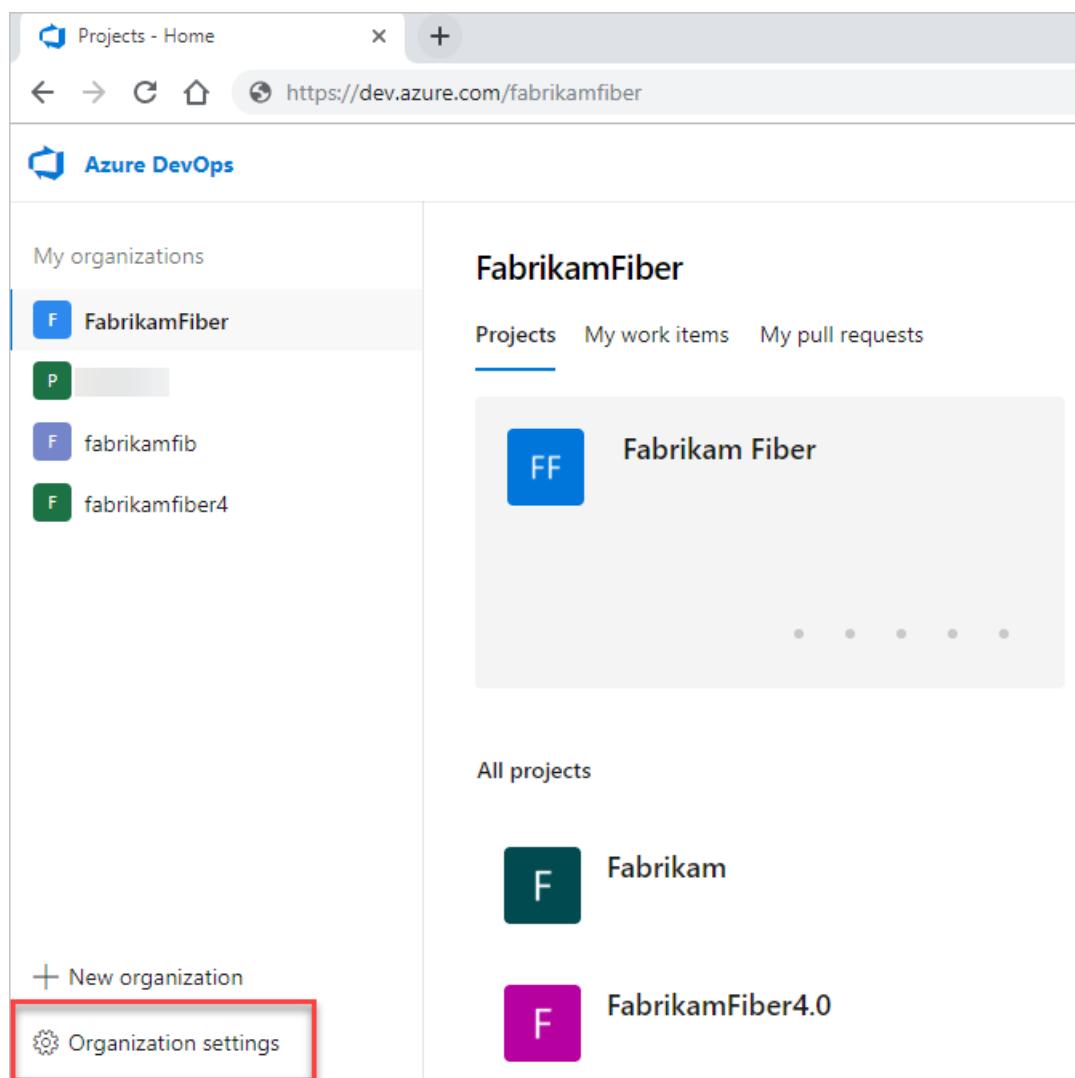
1. See [Show members of the Project Collection Administrators group](#).

1. See [Show members of the Project Administrators group](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your **Organization settings**.



2. Find the current owner.

Q: Why don't users appear or disappear promptly in Azure DevOps after I add or delete them in the Users hub?

A: If you experience delays finding new users or having deleted users promptly removed from Azure DevOps (for example, in drop-down lists and groups) after you add or delete users, [file a problem report on Developer Community](#) so we can investigate.

Visual Studio subscriptions

Q: When do I select "Visual Studio/MSDN Subscriber"?

A: Assign this access level to users who have active, valid [Visual Studio subscriptions](#). Azure DevOps automatically recognizes and validates Visual Studio subscribers who have Azure DevOps as a benefit. You need the email address that's associated with the subscription.

For example, if a user selects **Visual Studio/MSDN Subscriber** but the user doesn't have a valid, active Visual Studio subscription, the user can work only [as a Stakeholder](#).

Q: Which Visual Studio subscriptions can I use with Azure DevOps?

A: See [Azure DevOps benefits for Visual Studio subscribers](#).

Q: Why won't my Visual Studio subscription validate?

A: See [Why won't Azure DevOps recognize my Visual Studio subscription?](#)

Q: Why do Visual Studio subscriber access levels change after a subscriber signs in?

A: Azure DevOps recognizes Visual Studio subscribers. Azure DevOps automatically assigns a user access that's based on the user's subscription and not on the current access level that's assigned to the user.

Q: What happens if a user's subscription expires?

A: If no other access levels are available, users can [work as Stakeholders](#). To restore access, a user must renew their subscription.

Q: What happened to Visual Studio Online Professional?

A: On December 1, 2015, we replaced Visual Studio Online Professional with the [Visual Studio Professional monthly subscription](#).

Although a Visual Studio Online Professional purchase now appears on your monthly invoice as a Visual Studio Professional monthly subscription, you need to transition manually to get the new offering. The transition provides an upgrade by offering access to unlimited organizations (not just one organization) like Visual Studio Online Professional.

The rest stays the same. You get monthly access to the Visual Studio Professional IDE. Pricing remains the same at \$45 per user, per month. Learn more about [Visual Studio subscriptions](#).

If you're purchasing user access to Visual Studio Professional for a specific organization (possible only if you purchased before November 2015) and want to upgrade, do the following:

1. Before the last day of the calendar month, sign in to your organization (
<https://dev.azure.com/{yourorganization}>).
2. Select  **Organization settings**.

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are '+ New organization' and 'Organization settings' (which is highlighted with a red box). The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. Under 'Projects', there are cards for 'Fabrikam Fiber' (blue icon), 'Fabrikam' (dark teal icon), and 'FabrikamFiber4.0' (purple icon). At the bottom of the main area, it says 'All projects'.

3. Select **Billing**.

The screenshot shows the 'Organization Settings' menu. The 'Billing' option is highlighted with a red box. Other options include General, Overview, Projects, Users, Global notifications, Usage, Extensions, and Azure Active Directory.

4. Reduce the number of paid Visual Studio Online Professional users to 0.

This change takes effect on the first day of the next month. For the rest of the current calendar month, you aren't billed for any Visual Studio Online Professional users.

5. On the first day of the next calendar month, go to [Visual Studio Marketplace Subscriptions > Visual Studio Professional - monthly subscription](#), and buy Visual Studio Professional monthly subscriptions for the same users. Learn [how to buy Visual Studio subscriptions](#).

User access

Q: What does "Last Access" mean in the All Users view?

The value in **Last Access** is the last date a user accessed any resources or services. Accessing Azure DevOps includes using *organizationname.visualstudio.com* directly and using resources or services indirectly. For example, you might use the [Azure Artifacts](#) extension, or you might access the service by pushing code to Azure DevOps from a Git command line or IDE.

Q: Can a user who has paid for Basic access join other organizations?

A: No, a user can join only the organization for which the user has paid for Basic access. But a user can join any organization where free users with Basic access are still available. The user can also join as a user with Stakeholder access for free.

Q: Why can't users access some features?

A: Make sure that users have the correct [access level](#) assigned to them.

- Learn [how to manage users and access levels for Azure DevOps](#).
- Learn [how to change access levels for Team Foundation Server](#).

Some features are available only as [extensions](#). You need to install these extensions. Most extensions require you to have at least Basic access, not Stakeholder access. Check the extension's description in the [Visual Studio Marketplace](#), Azure DevOps tab.

For example, to search your code, you can install the free [Code Search extension](#), but you need at least Basic access to use the extension.

To help your team improve app quality, you can install the free [Test & Feedback extension](#), but you get different capabilities based on your access level and whether you work offline or connected to Azure DevOps Services or Team Foundation Server (TFS).

To create test plans, assign the [Basic + Test Plans access level](#). Some [Visual Studio subscribers](#) can use this feature for free, but Basic users need to upgrade to Basic + Test Plans access before they can create test plans.

- Learn [how to get extensions for Azure DevOps](#).
- Learn [how to get extensions for TFS](#).
- Learn [how to buy access to TFS Test](#).

Q: Why does a user lose access to some features?

A: This might happen for different reasons (although the user can continue to [work as a Stakeholder](#)):

- The user's Visual Studio subscription has expired. Meanwhile, the user can [work as a Stakeholder](#), 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. This affects all purchases made with this subscription, including Visual Studio subscriptions. To fix this issue, visit the [Azure account portal](#).
- The Azure subscription used for billing was unlinked from your organization. Learn more about [linking your organization](#).
- Your organization has more users with Basic access than the number of users that you're paying for in Azure. Your organization includes five free users with Basic access. If you need to add more users with Basic access, you can [pay for these users](#).

Otherwise, on the first day of the calendar month, users who haven't signed 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](#).

- The user no longer has access to [features that are available only as extensions](#). This might happen for different reasons:
 - The user's access level no longer meets the extension's requirements. Most extensions require at least Basic access, not Stakeholder access. For more information, see the extension's description in the [Marketplace](#).
 - The extension was uninstalled. Users can [reinstall the extension](#).
 - If the extension is a paid extension, the Azure subscription used for billing might be unlinked from your organization or might no longer be active. Learn more about [linking your organization](#) or visit the [Azure portal](#) to check payment details.

Azure Active Directory and your organization

Q: Why do I have to add users to a directory?

A: Your organization authenticates users and controls access through Azure Active Directory (Azure AD). All users must be directory members to get access.

If you're a directory administrator, you can [add users to the directory](#). If you're not an administrator, work with your directory administrator to add users. Learn more about [how to control access by using a directory](#).

Q: How do I find out whether my organization uses Azure AD to control access?

A: If you have at least Basic access, here's how to find out:

Go your **Organization settings**, and then select the **Azure Active Directory** tab. See the following examples of an organization that is not connected, and then an organization that is connected to Azure AD.

The screenshot shows the Azure DevOps Organization Settings interface. On the left, there's a sidebar with a 'General' section containing links for Overview, Projects, Users, Billing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' link is highlighted with a red box. Below the sidebar, the status 'Not connected' is displayed. On the right, the main content area is titled 'Azure Active Directory' and contains instructions to 'Connect your organization to an Azure Active Directory' with a 'Follow steps and learn more' link and a 'Connect directory' button. The top navigation bar shows the user's name 'fabrikamfiber13' and the path 'Organization Settings / Azure A'.

<p>Organization Settings</p> <p>General</p> <p>Overview</p> <p>Projects</p> <p>Users</p> <p>Auditing</p> <p>Global notifications</p> <p>Usage</p> <p>Extensions</p> <p>Azure Active Directory</p>	<p>Azure Active Directory</p> <p>Your organization is connected to the [REDACTED] Directory directory.</p> <p>[REDACTED] Directory</p> <p>[REDACTED].onmicrosoft.com</p> <p>Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5</p> <p>Disconnect directory</p>
---	--

If your organization is connected to your organization's directory, only users from your organization's directory can join your organization. Learn [how to control organization access by using Azure AD](#).

Q: My organization controls access by using Azure Active Directory. Can I just delete users from the directory?

A: Yes, but deleting a user from the directory removes the user's access to all organizations and other assets associated with that directory. You must have Azure AD global administrator permissions to [delete a user from your Azure AD directory](#).

Q: Why are "no identities found" when I try to add users from Azure AD to my Azure DevOps organization?

A: You're probably a *guest* in the Azure AD that backs your Azure DevOps organization, rather than a *member*. By default, Azure AD guests can't search the Azure AD in the manner required by Azure DevOps. Learn how to [convert an Azure AD guest into a member](#).

Q: How can I convert an Azure AD guest into a member?

A: Select from the following two options:

- Have the Azure AD administrator(s) remove you from the Azure AD and re-add you, making you an Azure AD *member* rather than a *guest* when they do. For more information, see [Can Azure AD B2B users be added as members instead of guests](#).
- [Change the UserType of the Azure AD guest using Azure AD PowerShell](#). This is an advanced process and [is not advised](#), but it allows the user to query Azure AD from the Azure DevOps organization thereafter.

Convert Azure AD UserType from guest to member using Azure AD PowerShell

WARNING

This is an advanced process and [is not advised](#), but it allows the user to query Azure AD from the Azure DevOps organization thereafter.

Prerequisites

The user making the UserType change must have the following:

- A work/school account (WSA)/native user in Azure AD. You can't do this with a Microsoft Account.
- Global administrator permissions

IMPORTANT

We recommend that you create a brand new (native) Azure AD user who is a global admin in the Azure AD, and then complete the following steps with that user. This new user should eliminate the possibility of connecting to the wrong Azure AD. You can delete the new user when you're done.

Process

1. Sign in to the [Azure portal](#) as global administrator for your organization's directory.
2. Go to the tenant that backs your Azure DevOps organization.
3. Check the UserType. Confirm that the user is a guest.

The screenshot shows the 'Identity' section of the Azure portal's user creation form. It includes fields for Name (linkia@meus.com), User name (linkia@meus.com), First name (Linkia), Last name (Default Directory), Photo (a blue globe icon), and a 'Select a file' button. Below these, the 'User type' field is highlighted with a red border and contains the value 'Guest'. Other fields shown include Source (Microsoft Account) and Object ID (an empty input field).

4. Open an Administrative Windows PowerShell prompt.
5. Execute `Install-Module -Name AzureAD`. The [Azure Active Directory PowerShell for Graph](#) downloads from the PowerShell Gallery. You may see prompts about installing NuGet and untrusted repository, as pictured below. If you run into issues please review the system requirements and information at the [Azure Active Directory PowerShell for Graph](#) page.

The screenshot shows an 'Administrator: Windows PowerShell' window. The command `Install-Module -Name AzureAD` is run, followed by several informational messages from the NuGet provider and PowerShellGet. It asks if the user wants to install the NuGet provider and if they trust the untrusted repository. The user responds with 'Y' for both questions.

```
[PS] C:\windows\system32> Install-Module -Name AzureAD
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repository.
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\trevorh\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\windows\system32> -
```

6. Once the installation completes, execute `Connect-AzureAD`. You're prompted to sign in to the Azure AD. Be sure to use an ID that meets the criteria above.
7. Execute `Get-AzureADUser -SearchString "<display_name>"`, where `<display_name>` is part of the entire display name for the user, as seen inside the Azure portal). The command returns four columns for the user found - ObjectId, DisplayName, UserPrincipalName, UserType - and the UserType should say *guest*.
8. Execute `Set-AzureADUser -ObjectId <string> -UserType Member`, where `<string>` is the value of ObjectId returned by the previous command. This should set the user to member status.

9. Execute `Get-AzureADUser -SearchString "<display_name>"` again to verify the UserType has changed. You can also verify this in the Azure Active Directory section of the Azure portal. While not the norm, we have seen it take several hours or even days before this change is reflected inside Azure DevOps. If it doesn't fix your Azure DevOps issue immediately, give it some time and keep trying.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

More support

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot adding members to projects

7/3/2019 • 7 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Q: Why can't I add any more members to my project?

A: Your organization is free for the first five users with Basic access. You can add unlimited Stakeholders and Visual Studio subscribers for no extra charge. After you assign all five free users with Basic access, you can continue adding Stakeholders and Visual Studio subscribers.

To add six or more users with Basic access, you need to [set up billing in Azure](#). Then you can [pay for more users who need Basic access](#), return to your organization, [add these users](#), and [assign them Basic access](#). When billing is set up, you can pay monthly for the extra users' access. And you can cancel at any time.

If you need more Visual Studio subscriptions, learn [how to buy subscriptions](#).

Q: Why can't some users sign in?

A: This problem might happen because users must sign in with Microsoft accounts unless your organization controls access with Azure Active Directory (Azure AD). If your organization is connected to Azure AD, users must be directory members to get access. See [How do I find out if my organization uses Azure Active Directory \(Azure AD\)?](#)

If you're an Azure AD administrator, you can add users to the directory. If you're not, work with the directory administrator to add them. Learn [how to control organization access with Azure AD](#).

Q: Why can't users access some features?

A: Make sure that users have the correct [access level](#) assigned to them.

- Learn [how to manage users and access levels for Azure DevOps](#).
- Learn [how to change access levels for Team Foundation Server](#).

Some features are available only as [extensions](#). You need to install these extensions. Most extensions require you to have at least Basic access, not Stakeholder access. Check the extension's description in the [Visual Studio Marketplace](#), Azure DevOps tab.

For example, to search your code, you can install the free [Code Search extension](#), but you need at least Basic access to use the extension.

To help your team improve app quality, you can install the free [Test & Feedback extension](#), but you get different capabilities based on your access level and whether you work offline or connected to Azure DevOps Services or Team Foundation Server (TFS).

To create test plans, assign [Basic + Test Plans access level](#). Some [Visual Studio subscribers](#) can use this feature for free, but Basic users need to upgrade to Basic + Test Plans access before they can create test plans.

- Learn [how to get extensions for Azure DevOps](#).
- Learn [how to get extensions for TFS](#).
- Learn [how to buy access to TFS Test](#).

Q: Why did some users lose access to certain features?

A: Loss of access might happen for [different reasons](#).

Q: How do I find out whether my organization uses Azure AD to control access?

A: If you have at least Basic access, here's how to find out:

Go to your **Organization settings**, and then select the **Azure Active Directory** tab. See the following examples of an organization that is not connected, and then an organization that is connected to Azure AD.

The screenshot shows the 'Organization Settings' page for an organization that is not connected to Azure Active Directory. The left sidebar lists 'General' sections: Overview, Projects, Users, Billing, Global notifications, Usage, and Extensions. The 'Azure Active Directory' section is highlighted with a red box. The right panel is titled 'Azure Active Directory' and contains the text 'Connect your organization to an Azure Active Directory.' Below it is a 'Follow steps and learn more' link and a 'Connect directory' button.

Connected

The screenshot shows the 'Organization Settings' page for an organization that is connected to Azure Active Directory. The left sidebar includes the 'Azure Active Directory' section, which is also highlighted with a red box. The right panel displays a message stating 'Your organization is connected to the [REDACTED] Directory directory.' It shows a thumbnail of the Azure AD logo, the domain name [REDACTED].onmicrosoft.com, and the Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5. A 'Disconnect directory' button is present at the bottom of this section.

If your organization is connected to your organization's directory, only users from your organization's directory can join your organization. Learn [how to control organization access by using Azure AD](#).

Q: How do I remove users from my organization?

A: Learn [how to delete users](#) across all projects in your organization. If you paid for more users but don't need their organization access anymore, you must reduce your paid users to avoid charges.

Q: Why can't I find members from my connected Azure AD, even though I'm the Azure AD global admin?

A: You're probably a guest in the Azure AD instance that backs Azure DevOps. By default, Azure AD guests can't search in Azure AD. That's why you aren't finding users in your connected Azure AD to add to your organization.

First, check to see if you're an Azure AD guest:

1. Go to the **Settings** section of your organization. Look at the **Azure Active Directory** section at the bottom. Make a note of the tenant that backs your organization.
2. Sign in to the new Azure portal, portal.azure.com. Check your user profile in the tenant from step 1. Check

the **User type** value shown as follows:

The screenshot shows a user creation form for Azure Active Directory. The fields include:

- Identity:
 - Name: linkia@meun.com
 - User name: linkia@meun.com
 - First name: Linkia
 - Last name: Default Directory
- Photo: A placeholder icon of a globe.
- Select a file: A button to upload a photo.
- User type: A dropdown menu set to "Guest", which is highlighted with a red border.
- Source: Microsoft Account.
- Object ID: A long GUID.

If you're an Azure AD guest, do one of the following:

- Have another Azure DevOps admin, who isn't an Azure AD guest, manage the users in Azure DevOps for you. Members of the Project Collection Administrators group inside Azure DevOps can administer users.
- Have the Azure AD admin remove you from the connected Azure AD and re-add you. The admin needs to make you an Azure AD member rather than a guest. See **Can Azure AD B2B users be added as members instead of guests?**
- Change the **User Type** of the Azure AD guest by using Azure AD PowerShell. This is an advanced topic, and we don't advise it. But it works and allows the user to query Azure AD from Azure DevOps thereafter.

1. [Download and install Azure AD PowerShell module.](#)

2. Open PowerShell and run the following cmdlets.

a. Connect to Azure AD:

```
C:\Users\rajr> Connect-AzureAD
```

b. Find the **objectId** of the user:

```
C:\Users\rajr> Get-AzureADUser
```

c. Check the **usertype** attribute for this user to see if they're a guest or member:

```
C:\Users\rajr> Get-AzureADUser -objectId cd7d47bf-1c6e-4839-b765-13edcd164e66
```

d. Change the **usertype** from **member** to **guest**:

```
C:\Users\rajr> Set-AzureADUser -objectId cd7d47bf-1c6e-4839-b765-13edcd164e66 -UserType Member
```

Q: Why don't users appear or disappear promptly in Azure DevOps after I add or delete them in the Users hub?

A: If you experience delays finding new users or having deleted users promptly removed from Azure DevOps (for example, in drop-down lists and groups) after you add or delete users, [file a problem report on Developer Community](#) so we can investigate.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I find a Project Collection Administrator?

A: If you have at least Basic access, you can find your [Project Collection Administrator](#) in your organization's security settings.

1. See [Show members of the Project Collection Administrators group](#).
1. See [Show members of the Project Administrators group](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps Home page. On the left, there's a sidebar titled 'My organizations' with a list of organizations: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and contains tabs for 'Projects', 'My work items', and 'My pull requests'. Under 'Projects', there's a card for 'Fabrikam Fiber' with a blue 'FF' icon. Below it, under 'All projects', are cards for 'Fabrikam' (dark teal 'F') and 'FabrikamFiber4.0' (purple 'F').

2. Find the current owner.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot permissions and access with Azure Active Directory

6/12/2019 • 14 minutes to read • [Edit Online](#)

Azure DevOps Services

General

Q: I made changes to Azure Active Directory (Azure AD), but they didn't seem to take effect

A: Changes made in Azure AD can take up to 24 hours to be visible in Azure DevOps.

Q: Can I use Office 365 and Azure AD with Azure DevOps?

A: Yes.

- Don't have an organization yet? [Create an organization in Azure DevOps](#).
- Already have an organization? [Connect your organization to Azure AD](#).

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: My organization uses Microsoft accounts only. Can I switch to Azure AD?

A. Yes, but before you switch, make sure that Azure AD meets your needs for sharing work items, code, resources, and other assets with your team and partners.

Learn more about the differences in how you [control access with Microsoft accounts or with Azure AD, and how to switch when you're ready](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your **Organization settings**.

The screenshot shows the Azure DevOps interface for managing organizations. On the left, a sidebar lists 'My organizations' with icons and names: 'FabrikamFiber' (selected), 'P', 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings'. The main area displays the selected organization, 'FabrikamFiber', with its logo ('FF') and name. A horizontal ellipsis indicates more projects. Below this, under 'All projects', are two more entries: 'Fabrikam' (with logo 'F') and 'FabrikamFiber4.0' (with logo 'F').

2. Find the current owner.

Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.

Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Understand Azure AD groups

Q: Why can't I assign Azure DevOps permissions directly to an Azure AD group?

A: Because these groups are created and managed in Azure, you can't assign Azure DevOps permissions directly or secure version control paths to these groups. You'll get an error if you try to assign permissions directly.

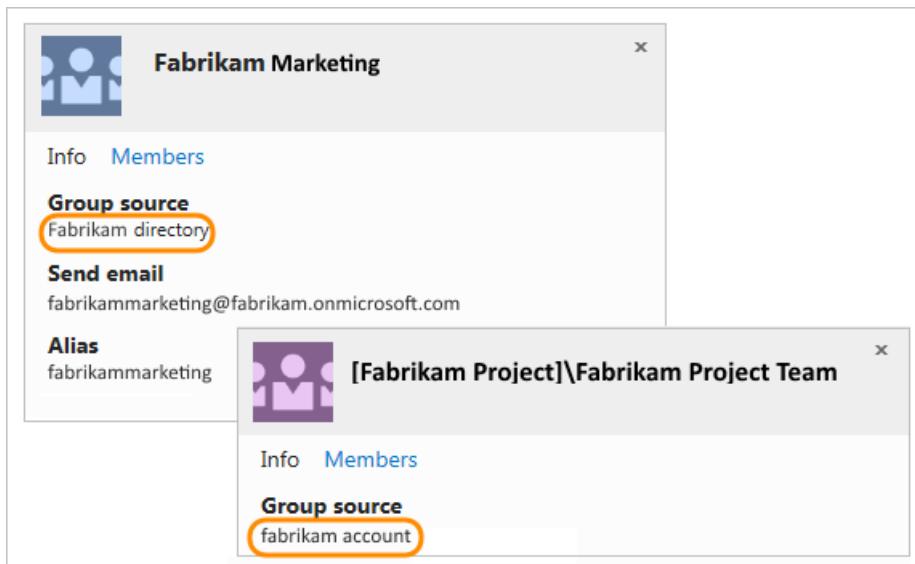
You can add an Azure AD group to the Azure DevOps group that has the permissions you want. Or, you can assign these permissions to the group instead. Azure AD group members inherit permissions from the group where you add them.

Q: Can I manage Azure AD groups in Azure DevOps?

A: No, because these groups are created and managed in Azure. Azure DevOps doesn't store or sync member status for Azure AD groups. To manage Azure AD groups, use the [Azure portal](#), Microsoft Identity Manager (MIM), or the group management tools that your organization supports.

Q: How do I tell the difference between an Azure DevOps group and an Azure AD group?

A: On the group's identity card, check the group's source.



Q: Why doesn't Users show all Azure AD group members?

A: These users have to sign in to your organization before they appear in Users.

Q: How do I assign organization access to Azure AD group members?

A: When these group members sign in to your organization for the first time, Azure DevOps assigns an access level to them automatically. If they have [Visual Studio subscriptions](#), Azure DevOps assigns the respective access level to them. Otherwise, Azure DevOps assigns them the next "best available" [access level](#), in this order: Basic, Stakeholder.

If you don't have enough access levels for all Azure AD group members, those members who sign in get a Stakeholder access.

Q: Why doesn't the Security tab show all members when I select an Azure AD group?

A: The Security tab shows Azure AD group members only after they sign in to your organization, and have an access level assigned to them.

To see all Azure AD group members, use the [Azure portal](#), MIM, or the group management tools that your organization supports.

Q: Why doesn't the team members widget show all Azure AD group members?

A: The team members widget shows only users who previously signed in to your organization.

Q: Why doesn't the team capacity pane show all Azure AD group members?

A: The team capacity pane shows only users who previously signed in to your organization. To set capacity, manually add users to your team.

Q: Why doesn't the team room show offline users?

A: The team room shows Azure AD group members, but only when they're online.

Q: Why doesn't Azure DevOps reclaim access levels from users who aren't Azure AD group members anymore?

Azure DevOps doesn't automatically reclaim access levels from these users. To manually remove their access, go to [Users](#).

Q: Can I assign work items to Azure AD group members who haven't signed in?

A: You can assign work items to any Azure AD member who has permissions for your organization. This also adds that member to your organization. When you add users this way, they'll automatically appear in Users, with the best available access level. They'll also appear in the security settings.

Q: Can I use Azure AD groups to query work items by using the "In Group" clause?

A: No, querying on Azure AD groups is unsupported.

Q: Can I use Azure AD groups to set up field rules in my work item templates?

A: No, but you might be interested in our [process customization plans](#).

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Add users to directory

[Add organization users to your Azure Active Directory](#).

Q: Can I switch current users from Microsoft accounts to work accounts in Azure DevOps?

A: No. Although you can add new work accounts to your organization, they're treated as new users. If you want to access all your work, including its history, you must use the same sign-in addresses that you used before your organization was connected to your Azure AD. You can do this by adding your Microsoft account as a member to your Azure AD.

Q: Why can't I add users from other directories to my Azure AD?

A: You must be a member or have read access in those directories. Otherwise, you can add them [using B2B collaboration through your Azure AD administrator](#). You can also add them by using their Microsoft accounts, or by creating new work accounts for them in your directory.

Q: How do I use my work or school account with my Visual Studio with MSDN subscription?

A: If you used a Microsoft account to activate a [Visual Studio with MSDN subscription](#) that includes Azure DevOps as a benefit, you can add a work or school account. The account must be managed by Azure AD. Learn [how to link work or school accounts to Visual Studio with MSDN subscriptions](#).

Q: Can I control access to my organization for external users in the connected directory?

A: Yes, but only for external users who are [added as guests through Office 365](#) or [added using B2B collaboration by your Azure AD administrator](#). These external users are managed outside the connected directory. To learn more, contact your Azure AD administrator. The following setting doesn't affect [users who are added directly to your organization's directory](#).

Before you start, make sure you have at least Basic access, not Stakeholder.

Complete the following steps to control organization access for external users added through Office 365 or Azure AD B2B collaboration.

1. Go to **Organization settings**.

The screenshot shows the Azure DevOps organization settings interface. On the left, there's a sidebar with 'My organizations' containing 'FabrikamFiber' (selected), 'fabrikamfib', and 'fabrikamfiber4'. Below this are buttons for '+ New organization' and 'Organization settings', with 'Organization settings' highlighted by a red box. The main area is titled 'FabrikamFiber' and shows 'Fabrikam Fiber' as a project. It also lists 'All projects' with 'Fabrikam' and 'FabrikamFiber4.0'. At the bottom of the sidebar, there's a 'Policy' link.

2. Select **Policy** and choose to allow or deny organization access for external users added as guests.

The screenshot shows the 'Organization Settings > Policy' page. The left sidebar has a 'Policy' link selected, which is highlighted by a blue box. The main content area is titled 'Policy' and contains two sections: 'Application connection policies' and 'Security policies'. In the 'Application connection policies' section, three dropdowns are shown: 'Alternate authentication credentials' (set to 'On'), 'Third-party application access via OAuth' (set to 'On'), and 'SSH authentication' (set to 'On'). In the 'Security policies' section, there are two dropdowns: 'External guest access' (set to 'On', highlighted by a red box) and 'Anonymous access to projects' (set to 'Off').

Remove users or groups

Q: How do I remove an Azure AD group from Azure DevOps?

A: Go to your project collection or project. In the bar at the top, select the gear icon, and then select **Security**.

Find the Azure AD group, and delete it from your organization.

The screenshot shows the Azure DevOps Security interface. On the left, there's a sidebar with options like 'Create group' and 'Filter users and groups'. Below that is a tree view under 'Azure DevOps Services Groups' with items like 'Contributors', 'Project Administrators', 'Project Collection Admi...', etc. The main area shows 'Fabrikam > Project Administrators' with tabs for 'Permissions', 'Members', and 'Member of'. Under 'Members', there are two entries: 'Project Collection Build Se...' and 'Christie Church'. The entry for 'Project Collection Build Se...' has a 'Remove' button highlighted with a red box. Both users have purple profile icons and are associated with the 'Fabrikam Project'.

Q: Why am I asked to remove a user from an Azure AD group when I delete that user from my organization?

A: Users can belong to your organization, both as individuals and as members of Azure AD groups that were added to Azure DevOps groups. These users can still access your organization while they're members of these Azure AD groups.

To block all access for these users, remove them from Azure AD groups in your organization, or remove these groups from your organization. Although we'd like to make it possible to block access completely or make exceptions for such users, Azure DevOps doesn't currently have this capability.

Q: If an Azure AD user is removed, will all their related PATs be revoked as well?

A: When users are disabled or removed from your directory, they can no longer access your organization by any mechanism including via PATs, SSH, or any other alternate credentials.

Connect, disconnect, or change Azure AD

- [Connect your organization to Azure AD](#)
- [Disconnect your organization from your directory](#)
- [Change the directory that's connected to Azure DevOps](#)

Q: Can I connect my organization to an Azure AD created from Office 365?

A: Yes. If you can't find your Azure AD created from Office 365, see [Why don't I see the directory that I want to connect?](#)

Q: Why don't I see the directory that I want to connect to? What should I do?

A: This might happen due to any of the following circumstances:

- You don't have [organization Owner permissions](#) to manage directory connections.
- Talk to your Azure AD organization administrator and ask them to make you a member of the organization. It's possible that you're not part of the organization.

Q: Why is my organization already connected to a directory? Can I change that directory?

A: Your organization was connected to a directory when the organization owner created the organization, or sometime after that. When you create an organization with a work or school account, your organization is automatically connected to the directory that manages that work or school account. You can [disconnect your organization](#).

organization from this directory, and reconnect to another directory. You might have to migrate some users.

Q: My alternate credentials don't work anymore. What do I do?

A: This happens after you connect your organization to a directory. Set up your credentials again for the organization that you connected.

Q: Some users are disconnected, but they have matching identities in Azure AD. What should I do?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

The screenshot shows the 'Organization Settings' page in the Azure DevOps portal. On the left, there's a sidebar with various options like General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' option is highlighted with a red box. The main content area is titled 'Azure Active Directory'. It displays a message: '10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory. Delete any unwanted users in Organization settings, and then Resolve for remaining members.' A 'Resolve' button is shown with a red box around it. Below this, it says 'Your organization is connected to the Commerce Test Directory directory.' It shows the connection details: 'Commerce Test Directory', 'mstestvscommerceoutlook.onmicrosoft.com', and 'Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5'. There's also a 'Disconnect directory' button. The entire screenshot is framed by a light gray border.

- Match the identities. Select **Next** when you're done.

Resolve disconnected users



Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.

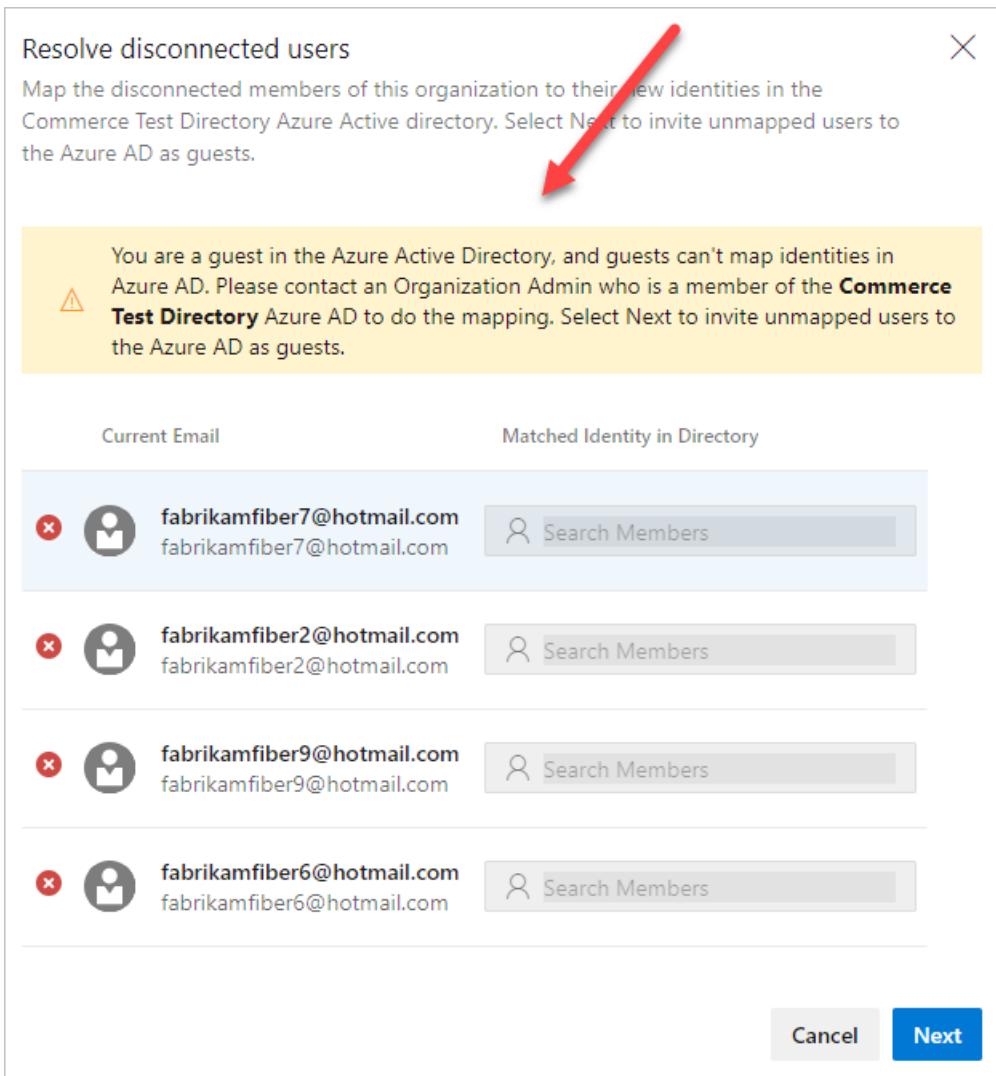
Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	Search Members
CR fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	Search Members

Cancel **Next**

Q: I got an error message when I was resolving disconnections. What should I do?

A:

- Try again.
- You might be a guest in Azure AD. Request that an organization administrator, who is a member of Azure AD, do the mapping. Or, request that an admin of the Azure AD convert you to a member.



- If the error message includes a user in your domain, but you don't see them active in your directory, the user likely left your company. Go to the organization user settings to remove the user from your organization.

Q: When I was trying to invite a new user to my Azure AD, I got a 403 forbidden exception. What do I do?

A: You may be a guest in Azure AD and don't have the right permission to invite users. Go to **External collaboration settings** in Azure AD and move the "Guests can invite" toggle to **Yes**. Refresh Azure AD and try again.

Q: Will my users keep their existing Visual Studio subscriptions?

A: Visual Studio subscription administrators ordinarily assign subscriptions to users' corporate email addresses, so that users can receive welcome email and notifications. If the identity and subscription email addresses match, users can access the benefits of the subscription. As you transition from Microsoft to Azure AD identities, users' benefits still work with their new Azure AD identity. But, the email addresses must match. If the email addresses don't match, your subscription administrator must [reassign the subscription](#). Otherwise, users must [add an alternate identity to their Visual Studio subscription](#).

Q: What if I'm required to sign in when I use the people picker?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: What if my email account isn't found in Azure AD?

A:

- In your Azure DevOps **Organization settings**, select **Azure Active Directory**, and then select **Resolve**.

The screenshot shows the 'Organization Settings' page in Azure DevOps. On the left, there's a sidebar with links like General, Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, and Azure Active Directory. The 'Azure Active Directory' link is highlighted with a red box. The main content area is titled 'Azure Active Directory'. It displays a yellow warning box stating: '10 member(s) of the FabrikamFiber organization can't sign in because they're not in the Commerce Test Directory. Delete any unwanted users in Organization settings, and then Resolve for remaining members.' A 'Resolve' button is highlighted with a red box. Below this, it says 'Your organization is connected to the Commerce Test Directory directory.' It shows the connection details: 'Commerce Test Directory' with a blue triangle icon, the URL 'mstestscommerceoutlook.onmicrosoft.com', and the Tenant Id '97ac18ac-aa35-484a-9f52-90a103a18bc5'. There's also a 'Disconnect directory' button. At the bottom of the main content area, there's a 'Disconnect directory' button.

- Match the identities. Select **Next** when you're done.

The screenshot shows the 'Resolve disconnected users' dialog box. It has a title 'Resolve disconnected users' and a subtitle: 'Map the disconnected members of this organization to their new identities in the Commerce Test Directory Azure Active directory. Select Next to invite unmapped users to the Azure AD as guests.' The main area lists four disconnected users with their current email and matched identity in the directory:

Current Email	Matched Identity in Directory
fabrikamfiber2@hotmail.com fabrikamfiber2@hotmail.com	Search Members
fabrikamfiber3@hotmail.com fabrikamfiber3@hotmail.com	Search Members
fabrikamfiber1@hotmail.com fabrikamfiber1@hotmail.com	Search Members
fabrikamfiber5@hotmail.com fabrikamfiber5@hotmail.com	Search Members

At the bottom right of the dialog box are 'Cancel' and 'Next' buttons.

Q: What if my work items are indicating that the users aren't valid?

A: Clear your browser cache and delete any cookies for the session. Close your browser, and then reopen.

Q: Once my organization is connected to Azure AD, will it update Azure Boards work items, pull requests, and other pieces where I'm referenced in the system with my new ID?

A: Yes, all pieces in the system are updated with the new ID when a user's ID is mapped from their personal email to their work email.

Q: What if I get a warning about members who will lose access to the organization?

A: You can still connect to Azure AD, but try to resolve the mapping issue after you've connected. If you still need help, [contact support](#).

Azure Active Directory Connection

Connect your organization to a directory.

You are signed in as



Jamal Hartnett
fabrikamfiber4@hotmail.com

Azure Active Directory

Commerce Test Directory

 Commerce Test Directory
Tenant Id: 97ac18ac-aa35-484a-9f52-90a103a18bc5

Warning: Some members will lose access to the FabrikamFiber organization

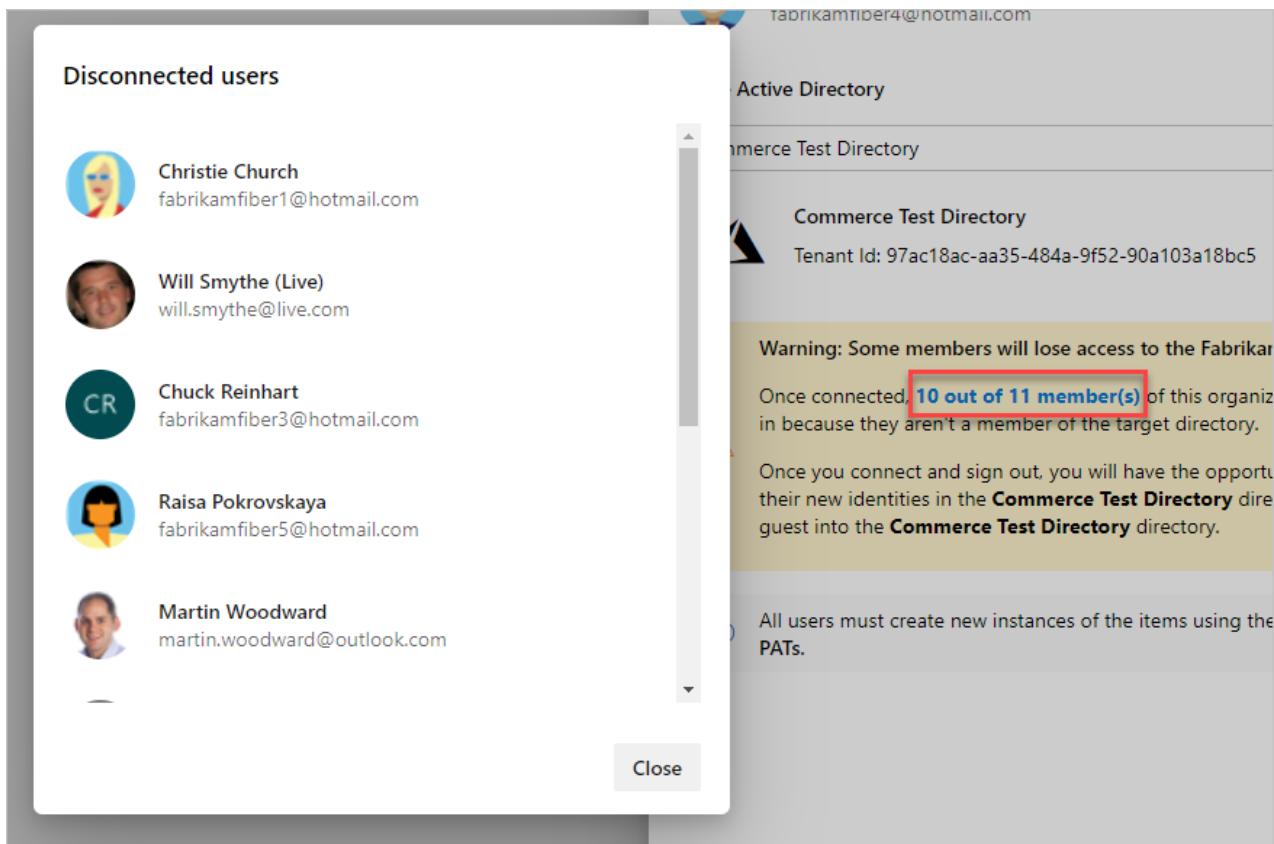
Once connected, **10 out of 11 member(s)** of this organization won't be able to sign in because they aren't a member of the target directory.

 Once you connect and sign out, you will have the opportunity to map these users to their new identities in the **Commerce Test Directory** directory, or to invite them as a guest into the **Commerce Test Directory** directory.

 All users must create new instances of the items using their work account: SSH Keys, PATs.

Cancel **Connect**

Select the bolded text to see which users are affected.



Q: What if I have over 100 users and want to connect to Azure AD?

A: If you have more than 100 users, [contact support](#).

Q: I have more than 100 members in my Azure DevOps organization, how can I connect to an Azure AD?

A: Currently, the in-app feature doesn't support connections for organizations with over 100 members. Please [contact support](#).

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot changing app access policies for your organization

1/31/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: How do personal access tokens differ from alternate authentication credentials?

A: Personal access tokens are a more convenient and secure replacement for alternate authentication credentials. You can limit a token's use to a specific lifetime, to an organization, and to [scopes](#) of activities that the token authorizes. Learn more about [personal access tokens](#).

Q: If I deny access to one authentication method in one organization, does that affect all the organizations that I own?

A: No, you can still use that method in all the other organizations that you own. [Personal access tokens](#) apply to specific organizations or to all organizations, based on your selection when you created the token.

Q: If I deny access to an authentication method, then allow access again, will the apps that need access continue to work?

A: Yes, those apps continue to work.

Q: What apps integrate with Azure DevOps?

A: Find the [apps that integrate with Azure DevOps](#).

Q: How do I find the organization owner?

If you have at least Basic access, you can find the current owner in your organization settings.

1. Go to your [Organization settings](#).

The screenshot shows the Azure DevOps interface for managing organizations. On the left, a sidebar lists 'My organizations' with items: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this are links for 'New organization' and 'Organization settings'. The main area is titled 'FabrikamFiber' and shows a project card for 'Fabrikam Fiber'. A horizontal ellipsis indicates more projects. Below this, under 'All projects', are cards for 'Fabrikam' (dark green F) and 'FabrikamFiber4.0' (purple F). The 'Organization settings' button is highlighted with a red box.

2. Find the current owner.

Q: Why don't I see the organizations that I own after I sign in to my Visual Studio profile on visualstudio.com?

A: Your list of organizations are associated with the identity that you use to sign in to Azure DevOps.

If you're asked to choose between your personal Microsoft account or your work or school account when you sign in, you might have selected the wrong identity.

Try to sign out completely from Azure DevOps, then sign in again and select your other identity.

Closing your browser doesn't always sign you out completely. Here's how you can sign out completely:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see the message "Sign out in progress." After you sign out, you're redirected to the Visual Studio page @visualstudio.microsoft.com.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: Why do I have to choose between a "work or school account" and my "personal account"?

A: This happens when you sign in with an email address (for example, jamalhartnett@fabrikam.com) that's shared by your personal Microsoft account and by your work account or school account. Although both identities use the same sign-in address, they're still separate identities. The two identities have different profiles, security settings, and permissions. When you sign in, you see a page that looks like the following example:



- Select **Work or school account** if you used this identity to create your organization, or if you previously signed in with this identity. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by your organization's directory in Azure AD, which controls access to your organization.

- Select **Personal account** if you used your Microsoft account with Azure DevOps. For example, select this option if you previously signed in to Azure DevOps by using this UI:



Your identity is authenticated by the global directory for Microsoft accounts.

Q: Why can't I sign in after I select "personal Microsoft account" or "work or school account"?

A: When your sign-in address is shared by your personal Microsoft account and by your work account or school account, but your selected identity doesn't have access, you can't sign in. Although both identities use the same sign-in address, they're separate: they have different profiles, security settings, and permissions.

Sign out completely from Azure DevOps by completing the following steps. Closing your browser might not sign you out completely. Sign in again and select your other identity:

1. Close all browsers, including browsers that aren't running Azure DevOps.
2. Open a private or incognito browsing session.
3. Go to this URL: <https://aka.ms/vssignout>.

You see a message that says, "Sign out in progress." After you sign out, you're redirected to the Azure DevOps @dev.azure.microsoft.com webpage.

TIP

If the sign-out page takes more than a minute to sign you out, close the browser and continue.

4. Sign in to Azure DevOps again. Select your other identity.

Q: How do I get help or support for Azure DevOps?

A: You have the following options for support:

- Report a problem with Azure DevOps on [Developer Community](#).
- Provide a suggestion on [Developer Community](#)
- Get advice on [Stack Overflow](#)
- Get support on [Azure DevOps Support](#)
- View the archives of the [Azure DevOps forum](#) on MSDN

Troubleshoot adding administrators to projects and project collections

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: When do I need to add someone to the project collection administrator role in Azure DevOps?

A: It varies. For most organizations that use Azure DevOps, project collection administrators manage the collections that members of the **Team Foundation Administrators** group create. Members of the **Project Collection Administrators** group don't create the collections themselves. Project collection administrators also perform many operations that are required to maintain the collection. Operations include creating team projects, adding users to groups, modifying the settings for the collection, and so on.

Q: What are the optimal permissions to administer a project collection across all of its components and dependencies?

A: Project collection administrators must be members of the following groups or have the following permissions:

- Team Foundation Server: A member of the **Project Collection Administrators** group, or have the appropriate [collection-level permissions](#) set to **Allow**.
- SharePoint Products: If the collection is configured with a site collection resource, then a member of the **Site Collection Administrators** group.
- Reporting Services: If the collection is configured with reporting resources, then a member of the **Team Foundation Content Manager** group.

Q: I'm an admin, but I don't have permission to add a project collection administrator. What do I need?

A: The following permissions are required:

- You must belong to the **Project Collection Administrators** group, or your **View Server-Level Information** and **Edit Server-Level Information** permissions must be set to **Allow**.
- To add permissions for SharePoint Products, you must be a member of the **Site Collection Administrators** or **Farm Administrators** groups for SharePoint Products.
- To add permissions for Reporting Services, you must be a member of the **Content Managers** or **Team Foundation Content Managers** groups for Reporting Services.

IMPORTANT

To perform administrative tasks like creating project collections, your user requires administrative permissions. The service account that the Team Foundation Background Job Agent uses must have certain permissions granted to it. For more information, see [Service accounts and dependencies in Team Foundation Server](#) and [Team Foundation Background Job Agent](#).

Q: Where can I find information about each individual permission?

A: You can find detailed information about individual permissions and their relationship to default security groups in the [Permission and groups reference](#). To give a user project administration permissions, complete the following steps:

1. From the team page, select the settings icon  to go to the team administration page.
2. Add the user to the **Project Administrators** group.

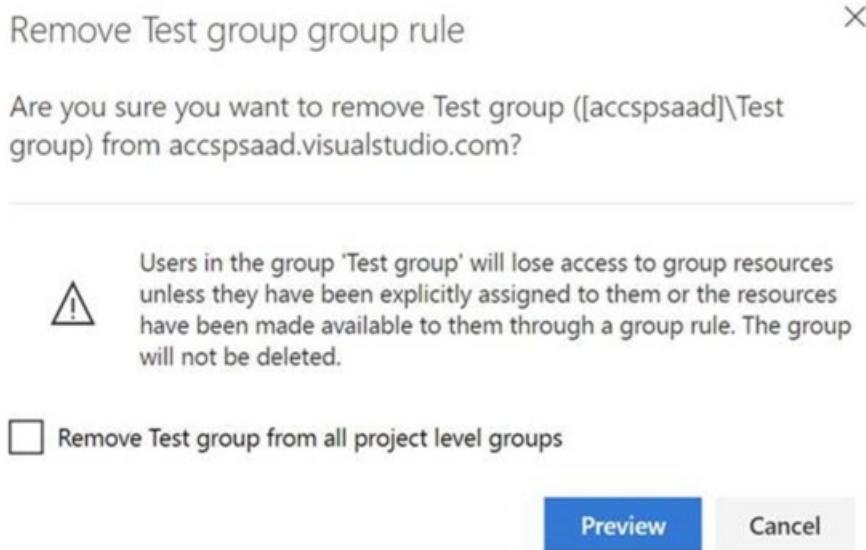
Troubleshoot managing group-based licensing

5/31/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Q: Will my users lose their access level and project membership if I remove a group rule?

A: Users in the group **TestGroup** lose access to group resources if the users haven't been explicitly assigned to the resources or assigned via a different group rule.



Q: Will my Azure DevOps or Azure AD group be deleted if I remove its group rule?

A: No. Your groups won't be deleted.

Q: What does the option "Remove from all project level groups" do?

A: This option removes the Azure DevOps or Azure AD group from any project-level default groups, such as **Project Readers** or **Project Contributors**.

Related articles

- [Migrate to group-based resource management](#)
- [Assign access levels and extensions to users by group membership](#)

Troubleshoot connecting to a project

7/2/2019 • 4 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Troubleshoot connectivity

As a first step in resolving connectivity issues with Azure DevOps, complete the following steps:

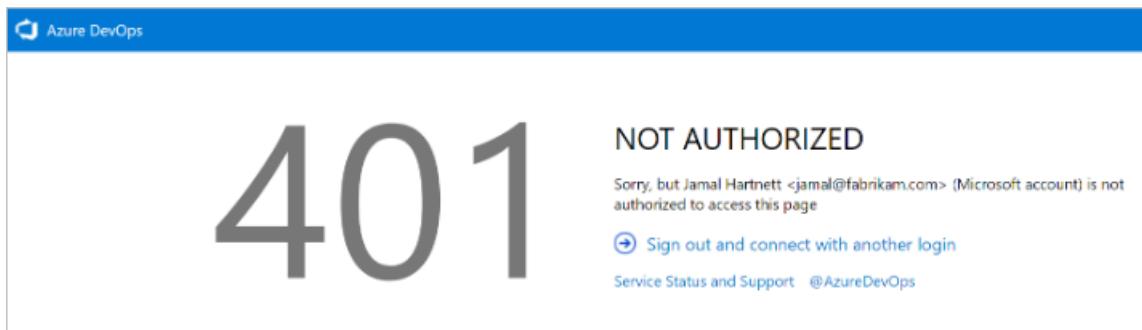
1. Sign out of your browser. To do so, select the [Visual Studio sign out](#) link.
2. Delete the cookies in your browser. To delete cookies in most browsers, press **Ctrl+Shift+Del**.
3. Open Internet Explorer and delete the browser cookies. The Visual Studio IDE uses Internet Explorer cookies.
4. Close 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.

Troubleshoot signing in

Two types of identities can sign in: Microsoft accounts and Azure Active Directory (Azure AD) accounts.

Depending on your account, you might experience one of the following errors.

401 - Not Authorized



The most common error page is the *401 Not Authorized* error, which occurs when your identity doesn't have permissions to enter an organization. Common reasons for the error include:

- Your identity isn't a member of the organization.
- Your identity has an invalid or missing license assignment.

If you think you're a member of the organization but are blocked by this error page, [contact customer support](#).

Scenario 1

Your work or school Azure AD 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**.

- ➊ [Sign in with your personal account](#)
- ➋ [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 (Azure AD) that have the same sign-in address exist. You've 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. The work or school Azure AD account might have been created by an administrator when you were added to Office365 or Azure AD.

To sign out of your current work or school Azure AD 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.

TIP

To avoid seeing this prompt, you can rename your Microsoft account. Then, only one identity (your work or school account, or Azure AD account) uses your sign-in address.

Scenario 2

Your personal Microsoft account doesn't have access, but your Azure AD 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 (Azure AD identity) does. The same guidance from Scenario 1 applies, but in reverse.

401 - Work or school, or Personal account

401

NOT AUTHORIZED

jamal@fabrikam.com has multiple accounts associated with it.

Your personal account does not have access to dev.azure.com/Fabrikam/, but **your work or school account does have access**.

- ➊ [Sign in with your work or school account](#)
- ➋ [Sign out and connect with another login](#)

[Service Status and Support](#) | [@AzureDevOps](#)

Mitigation

If you enter your credentials correctly, but are redirected back to the original sign-in page, we recommend clearing all cookies, and then reattempting to sign in. If that doesn't fix the issue, contact customer support.

Troubleshoot TFS connectivity

Here's a list of the most frequently reported connection problems and what to do about them. Complete the list in the order indicated.

1. Verify that you have the required permissions.

If the errors that you receive indicate read-only or blocked actions, you might not have permissions to act on the data.

2. Verify that your computer is connected to the network and that it can access network resources.

3. Verify that TFS hasn't been taken offline. Talk with your TFS administrator.

4. Check whether your project has been moved to another project collection in TFS. If it has been moved, you must create a connection to the new server name.

For additional troubleshooting tips, see [TF31002: Unable to connect to this Team Foundation Server](#).

Switch organizations

When you use two or more organizations that are linked to Azure AD, such as organizations created in the Azure portal, 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 Team Foundation Server** dialog box:

TF31003: Either you have not entered the necessary credentials, or your user account does not have permission to connect to the Team Foundation Server

TF31002: Unable to connect to this Team Foundation 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 Online](#).

Connect to TFS with Secure Sockets Layer

If you connect to a TFS instance that has Secure Sockets Layer (SSL) configured, you must install a certificate and clear the client cache. For details, see [Set up HTTPS with Secure Sockets Layer \(SSL\) for TFS - Configuring client computers](#).

Clear the cache on client computers

When the on-premises TFS configuration changes, such as when you move or split a project collection, you may need to clear the cache.

1. Sign in to your client computer for TFS by using the credentials of the user whose cache you want to clear.

2. Close any open instances of Visual Studio.

3. Open a browser and go to one of the following folders, depending on the operating system that's running on your computer:

- **Windows 10** *Drive:\Users<i>UserName\AppData\Local\Microsoft\Team Foundation\6.0\Cache*
- **Windows 8** *Drive:\Users<i>UserName\AppData\Local\Microsoft\Team Foundation\4.0\Cache*
- **Windows 7 or Windows Vista** *Drive:\Users<i>UserName\AppData\Local\Microsoft\Team*

Foundation\2.0\Cache

4. Delete the contents of the Cache directory, including all subfolders.

TF31002: Unable to connect

5/8/2019 • 5 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

You might receive this error when you try to connect to Azure DevOps Services or an on-premises Azure DevOps Server from Visual Studio.

You receive this error when you try to connect to Azure DevOps Services

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. See Assign licenses to users for details.
Your Azure DevOps Services organization is connected to the Azure Active Directory.	When your Azure DevOps Services organization is connected to a directory that is associated with an Office 365 or Microsoft Azure subscription, only members in the directory can access the account. Check with your directory administrator to have them create an organizational account for you or add your account to the directory as external member .
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, you see a flashing blank sign in dialog box several times. Then, you receive either TF31002 or TF31003 error after you connect to or add a new connection in "Connect to Team Foundation Server" dialog box. To resolve this problem, apply the most recent Visual Studio update . To learn more, see KB Article ID 2958966, You can't switch between different organizational accounts in Visual Studio Online .
You want to sign in to Azure DevOps Services from Visual Studio using different credentials.	See Connect to projects, Sign in with different credentials .

When you try to connect to an on-premises Azure DevOps Server from your client computer

If you determine that you're receiving this error from one computer but not others, or others aren't receiving this error, then check the problem resolutions that are outlined below.

PROBLEM	RESOLUTION
Your password has expired.	Verify that you entered your user ID and password correctly, and that your password hasn't expired.
You've entered an incorrect server URL.	Verify that you've entered the server URL correctly including the server name, port number, and protocol (http/https). See Connect to projects to learn more.
The TFS configuration has changed.	If the configuration for the on-premises Azure DevOps Server has changed, you must create a new connection. You might also need to clear the client cache .
You work remotely and need to connect to a TFS Proxy server to check in files to Team Foundation version control.	Configure Visual Studio to connect to TFS Proxy .
You're connecting to a later version of TFS than your Visual Studio client version.	Your version of Visual Studio or Team Explorer might be incompatible with Team Foundation Server. You might need to install one or more GDR packs. See Requirements and compatibility for details.
Your firewall is blocking TFS services.	See Allow a program to communicate through Windows Firewall .
Visual Studio stops responding when you run a query in Visual Studio.	Your computer might be configured to bypass the proxy server. Verify the configuration of the BypassProxyOnLocal setting on your computer. For more information, see BypassProxyOnLocal Configuration .

Several users can't connect to an on-premises Azure DevOps Server

If the problem occurs on more than one computer, contact your administrator to confirm whether the server is operational and available on the network.

As an administrator, check the event logs for the application-tier server to try to pinpoint the problem. Also, you can use the following table to determine whether the server is misconfigured. In the table, problems that are more likely to occur appear first. Try the resolutions in the order in which they appear, which increases the chance that you can solve the problem quickly.

PROBLEM	RESOLUTION
The <i>TFSService</i> account password has expired or is incorrect.	Many services for Team Foundation Server will stop running when the service account for Team Foundation has expired. For more information, see Change the service account or password for Team Foundation Server .
The application-tier server for Team Foundation is unavailable.	Verify whether each required service is running. If a required service isn't running, you must restart it. If necessary, set it to start automatically. For more information, see Stop and start services, application pools, and websites .
The network is unavailable.	Verify whether your network is operational.
A website identity for Team Foundation is configured incorrectly.	Verify or correct the server binding assignments that are made to websites for Team Foundation.

PROBLEM	RESOLUTION
Access to a website for Team Foundation has been restricted.	Verify or correct restrictions that are made to those websites that are based on IP addresses and domain names.
The firewall or ports are configured incorrectly.	Verify or correct port binding assignments for websites and port assignments for the firewall. First, you should open the administration console for Team Foundation, display the Application Tier page, and review the URL assignments. If necessary, you can click Change URL to modify the URL of a website. Next, you should verify the port assignments for Internet Information Services (IIS) and the ports that are allowed through the firewall. For more information, see Review Server Status and Settings and Verify or Correct Port Assignments .
Trust relationships between domains aren't configured correctly.	If a group of users can't access Team Foundation Server, you might have trust issues between domains.
When users connect to different versions of TFS from Visual Studio, for example, they connect to TFS 2012 and then TFS 2008, they can get the TF31002 error.	<p>This error can occur because the GUIDs for the TFS 2012 collection are the same as TFS 2008. The local client cache gets confused because it tries to maintain the same GUID-based local cache for both the 2008 server and the new Project Collection in 2012.</p> <p>To fix, run the TFSConfig ChangeServerID command. See TFSConfig ChangeServerID command.</p>

If the previous resolutions don't solve the problem, go to the [MSDN Forums - Visual Studio Team System —Team Foundation Server - Administration](#).

Troubleshoot network connections and lists of allowed addresses

7/9/2019 • 2 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

If you are having network connection issues to Azure DevOps, using NuGet, or connecting from Visual Studio 2015 and later versions, it may be because your security appliances are blocking connections now that Visual Studio uses TLS 1.2.

To fix this issue, update the security appliances in order to support TLS 1.2 for the following connections:

List of URLs for sign-in and licensing connections

- <https://management.core.windows.net>
- <https://login.microsoftonline.com>
- <https://login.live.com>
- <https://go.microsoft.com>
- <https://graph.windows.net>
- <https://app.vssps.visualstudio.com>

A more general list of URLs for signing in to Azure DevOps and Azure

- <https://windows.net>
- <https://microsoftonline.com>
- <https://visualstudio.com>
- <https://microsoft.com>
- <https://live.com>
- <https://dev.azure.com>
- <https://management.core.windows.net>
- <https://app.vssps.visualstudio.com>
- <https://vstsagentpackage.azureedge.net>
- <https://cdn.vsassets.io> -- hosts our CDN content
- <https://gallerycdn.vsassets.io> -- hosts Azure DevOps extensions
- <https://static2.sharepointonline.com> -- hosts some resources that we use in "office fabric" UI kit (fonts, etc)
- <https://vstmrblob.vsassets.io> -- hosts our TCM log data

IP range restrictions

To ensure your organization works with any existing firewall or IP restrictions, ensure that dev.azure.com and *dev.azure.com are open and update your allow-listed IPs to include the following IP addresses, based on your IP version. If you're currently allow-listing the 13.107.6.183 and 13.107.9.183 IP addresses, leave them in place, as you don't need to remove them.

IPv4 ranges

- 13.107.6.0/24

- `13.107.9.0/24`
- `13.107.42.0/24`
- `13.107.43.0/24`

IPv6 ranges

- `2620:1ec:4::/48`
- `2620:1ec:a92::/48`
- `2620:1ec:21::/48`
- `2620:1ec:22::/48`

NuGet connections

- `https://azurewebsites.net`
- `https://nuget.org`

NOTE

Privately owned NuGet server URLs may not be included in the list above. You can check the NuGet servers you are using by opening up `%APPData%\Nuget\NuGet.Config`.

Troubleshoot tracing permissions

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps

Q: Why doesn't a user have access to something?

A 1: Their permissions are specified by multiple groups

If one of your users is having permissions issues and you make use of default security groups or custom groups for permissions, administrators can investigate where those permissions are coming from by making use of our permissions tracing. Users can receive their effective permissions either directly or via groups. By following these steps, administrators can understand where exactly those permissions are coming from and adjust them as needed.

1. Go to the **Security** page for the project that the user is having access problems.
2. Enter their name into the box in the upper left-hand corner.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber' project. The user 'Christie Church' has been entered into the search box. The 'Security' tab is selected. On the left, there's a sidebar with 'Create group' and a list of teams and VSTS Groups. Under 'Teams', 'FabrikamFiber-tfvc Team' is selected. On the right, the 'Permissions' section shows the following table:

Permission	Status
Bypass rules on work item updates	Allow (inherited)
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Allow (inherited)
Delete team project	Allow (inherited)

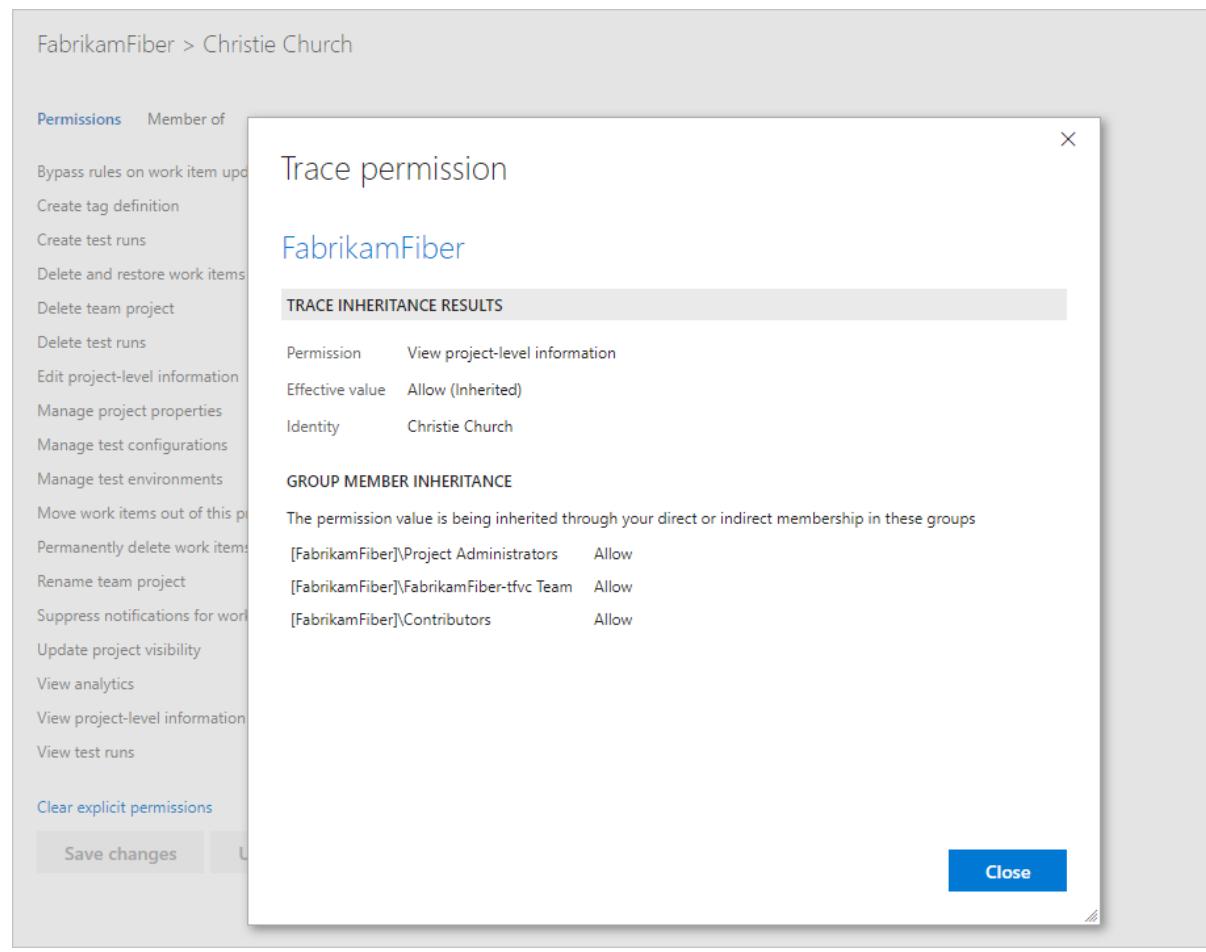
3. You should now have a user-specific view which shows what permissions they have. To trace why a user does or does not have any of the listed permissions, hover over the permission and choose **Why**.

The screenshot shows the 'Security' tab in the Azure DevOps interface. A group named 'Christie Church' is selected. The 'Permissions' section lists various project management actions with their inheritance status. A red box highlights the 'Why?' link next to the 'View project-level information' permission.

Permission	Inheritance Status
Bypass rules on work item updates	Allow (inherited)
Create tag definition	Allow (inherited)
Create test runs	Allow (inherited)
Delete and restore work items	Allow (inherited)
Delete team project	Allow (inherited)
Delete test runs	Allow (inherited)
Edit project-level information	Allow (inherited)
Manage project properties	Allow (inherited)
Manage test configurations	Allow (inherited)
Manage test environments	Allow (inherited)
Move work items out of this project	Allow (inherited)
Permanently delete work items	Allow (inherited)
Rename team project	Allow (inherited)
Suppress notifications for work item updates	Allow (inherited)
Update project visibility	Allow (inherited)
View analytics	Allow (inherited)
View project-level information	Allow (inherited)
View test runs	Allow (inherited)

[Why?](#)

4. The resulting trace lets you know how they are inheriting the listed permission. You can then adjust the user's permissions by adjusting those provided to the groups which they are in.



A 2: Their permissions haven't propagated yet

It can take from 1 hour to 24 hours for Azure AD group memberships or permissions changes to propagate throughout Azure DevOps. If a user is having issues that do not seem to clear up immediately, please wait a day to see if they resolve.

A 3: The user does not have the necessary access level

Access levels enable administrators to provide their users base access to the features they need, and only pay for those features. Several features can only be accessed with a Basic access level or higher. To assign access levels or check the access level of a user in your account, see the following topics:

- For cloud Azure DevOps: [Manage users and access in Azure DevOps](#)
- For on-premises Azure DevOps: [Change access levels](#)

Related articles

- [Grant or restrict access to select features and functions](#)
- [Change individual permissions](#)

Default permissions and access for Azure DevOps

6/26/2019 • 18 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

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 all Azure Boards features. **Stakeholder** access level provides partial support to select features, allowing users to view and modify work items, but not use all features. **Stakeholder** access is available to support free access to a limited set of features by an unlimited set of stakeholders.

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 assign users to an access level and security group:

- Grant **Basic** access or higher and add to the **Contributors** security group full-time workers who contribute to the code base or manage projects.
- Grant **Stakeholder** access and add to the **Contributors** security group managers or users who don't actively contribute to the code base but want to check project status and provide direction, feedback, feature ideas, and business alignment to a team. Also,
- Grant **Stakeholder** access and add to the **Project Administrators** security group users tasked with managing project resources. If they also need to contribute to the code base, then you must assign them **Basic** or higher-level access.
- Grant **Stakeholder** access and add to the **Project Collection Administrators** security group users tasked with managing organization or collection resources. If they also need to contribute to the code base, then you must assign them **Basic** or higher-level access.

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 indicates that the corresponding access level or security group has access to a feature by default.

For a comparison chart of Stakeholder versus Basic access, see the [Feature matrix](#). 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.

Dashboards, charts, reports, and widgets

You can define and manage dashboards from the web portal, **Dashboard**. For an overview of dashboard and chart features, see [Dashboards](#). You set [dashboard permissions at the team level](#) from the team dashboard page.

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	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View work item query charts (from the Queries page)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View dashboards (including work item query charts added to the dashboard)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create work item query and test tracking charts ¹			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add and configure dashboards ¹			With permissions set	<input type="checkbox"/>	<input type="checkbox"/>

Notes:

1. Public project Stakeholders have full access to all features.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View charts and dashboards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create work item and test tracking charts			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add and configure dashboards			With permissions set	<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View team dashboard home page	<input type="checkbox"/>				
Create work item and test tracking charts			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Dashboards and charts

You can pin charts to a team dashboard **Home** page.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View work item query charts (from the Queries page)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View dashboards (including work item query charts added to the dashboard)	<input type="checkbox"/>				
Create work item query and test tracking charts ¹			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add and configure dashboards ¹			With permissions set	<input type="checkbox"/>	<input type="checkbox"/>
---	--	--	----------------------	--------------------------	--------------------------

Notes:

1. Public project Stakeholders have full access to all features.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View charts and dashboards	<input type="checkbox"/>				
Create work item and test tracking charts			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add and configure dashboards			With permissions set	<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	PROJECT ADMINS
View team dashboard home page	<input type="checkbox"/>				
Create work item and test tracking charts			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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. To learn more, 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View a shared Analytics view		<input type="checkbox"/>	<input type="checkbox"/>
Edit and delete Analytics views			<input type="checkbox"/>

Azure Boards

You can plan and track work from the web portal **Boards** hub, and using Eclipse, Visual Studio, Excel, Project, and other clients. For an overview of work tracking features, see [About Agile tools](#).

Users granted Stakeholder access are granted different access to features depending on whether it is a private or a public project. For private projects, Stakeholders have limited access to select work tracking functions, whereas for public projects, Stakeholders enjoy full access to work tracking features. To learn

more, see [About access levels](#), [Stakeholder access](#).

Work tracking

You can plan and track work from the web portal **Work** hub, and using Eclipse, Visual Studio, Excel, Project, and other clients. For an overview of work tracking features, see [About Agile tools](#).

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 [Add administrators, set permissions at the project-level or project collection-level](#).

General work item feature access

You can use work items to track anything you need to track. To learn more, see [Understand how work items are used to track issues, tasks, and epics](#).

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS
View/open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items, add tags to work items <i>(Stakeholders can assign existing tags to work items, but can't add new tags)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Change work item type	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Move work item to another project			<input type="checkbox"/>	<input type="checkbox"/>
Email work items	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Apply a work item template	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Delete work items (able to restore from the Recycle bin)			<input type="checkbox"/>	<input type="checkbox"/>
Permanently delete work items				<input type="checkbox"/>
Provide feedback (through the Microsoft Feedback client)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request feedback			<input type="checkbox"/>	<input type="checkbox"/>

NOTE

You can change the work item type or move work items to another project within a project collection. These features require that the data warehouse is disabled. With the data warehouse disabled, you can use the [Analytics Service](#) to support your reporting needs. To learn more about disabling the data warehouse, see [Disable the data warehouse and cube](#).

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View/open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items, add tags to work items <i>(Stakeholders can assign existing tags to work items, but can't add new tags)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Email work items	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Apply a work item template	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Delete work items (able to restore from the Recycle bin)			<input type="checkbox"/>	<input type="checkbox"/>
Permanently delete work items				<input type="checkbox"/>
Provide feedback (through the Microsoft Feedback client)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request feedback			<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View/open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items, add tags to work items <i>(Stakeholders can assign existing tags to work items, but can't add new tags)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Email work items	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Delete work items (able to restore from the Recycle bin)			<input type="checkbox"/>	<input type="checkbox"/>
Permanently delete work items				<input type="checkbox"/>
Provide feedback (through the Microsoft Feedback client)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request feedback			<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View/open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items, add tags to work items <i>(Stakeholders can assign existing tags to work items, but can't add new tags)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

Email work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permanently delete work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Provide feedback (through the Microsoft Feedback client)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request feedback	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Boards feature access

You use **Boards** to implement Kanban methods. Boards present work items as cards and support quick status updates through drag-and-drop.

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View boards and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a board; update status, reorder, or reparent child tasks through drag-and-drop; update a field on a card	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add child tasks to a checklist	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assign to a sprint (from card menu)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customize a board, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View boards and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a board; update status through drag-and-drop	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assign to a sprint	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customize a board, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS

View backlogs and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a backlog <i>(Stakeholders can only add items to the bottom of the backlog)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Use bulk edit features	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
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			<input type="checkbox"/>	<input type="checkbox"/>
Customize a backlog, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>			<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS
View backlogs and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a backlog <i>(Stakeholders can only add items to the bottom of the backlog)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Use bulk edit features	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Add child items to a backlog item; prioritize or reorder a backlog; parent items using the Mapping pane			<input type="checkbox"/>	<input type="checkbox"/>
Customize a backlog, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>			<input type="checkbox"/>

Sprints feature access

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	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS
View sprint backlogs, taskboards, and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a sprint backlog <i>(Stakeholders can add backlog items to the bottom of a sprint backlog)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a taskboard <i>(Stakeholders can add backlog items but not tasks)</i>			<input type="checkbox"/>	<input type="checkbox"/>

Prioritize/reorder a sprint backlog or taskboard; add child items to a backlog item; reassign items to a sprint using the Planning pane	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View team capacity (work details)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Set team capacity			<input type="checkbox"/>	<input type="checkbox"/>
Use bulk edit features	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Define sprints, set sprint dates				<input type="checkbox"/>
Customize a sprint backlog or taskboard, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>			<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View sprint backlogs, taskboards, and open work items	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a sprint backlog <i>(Stakeholders can add backlog items to the bottom of a sprint backlog)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Add work items to a taskboard <i>(Stakeholders can add backlog items but not tasks)</i>			<input type="checkbox"/>	<input type="checkbox"/>
Prioritize/reorder a sprint backlog or taskboard; add child items to a backlog item; reassign items to another using drag-and-drop			<input type="checkbox"/>	<input type="checkbox"/>
View team capacity (work details)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Set team capacity			<input type="checkbox"/>	<input type="checkbox"/>
Use bulk edit features	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Define sprints, set sprint dates				<input type="checkbox"/>
Customize a sprint backlog or taskboard, configure team settings <i>(Stakeholders assigned as a team administrator or Project Administrator can configure team settings)</i>	<input type="checkbox"/>			<input type="checkbox"/>

Queries and semantic search

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	STAKEHOLDERS	READERS	CONTRIBUTOR S	PROJECT ADMINS
View and run managed queries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create and save managed My queries	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Create and save managed Shared queries <i>(Stakeholders can't save Shared queries even if granted permissions)</i>				<input type="checkbox"/>
View query charts		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create query charts			<input type="checkbox"/>	<input type="checkbox"/>
Powerful semantic work-tracking search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	TEAM ADMINS
View and run managed queries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create and save managed queries <i>(Stakeholders can't save shared queries)</i>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
View query charts		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create query charts			<input type="checkbox"/>	<input type="checkbox"/>

Delivery plans feature access

[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. Users granted **Stakeholder** access for private projects have no access to delivery plans, while users granted **Stakeholder** access for public projects has the same access as regular Contributors granted **Basic** access.

TASK	STAKEHOLDERS	READERS	CONTRIBUTOR S	PROJECT ADMINS
View delivery plans		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create, edit, or delete a delivery plan <i>(Contributors can only edit or delete plans that they create)</i>			<input type="checkbox"/>	<input type="checkbox"/>
Manage permissions for a delivery plan <i>(Contributors can only manage permissions for plans that they create)</i>				<input type="checkbox"/>

Additional permissions

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](#).

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**.

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.

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

TASK	READERS	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Clone, fetch, contribute to pull requests, and explore the contents of a repository	✓	✓	✓	✓
Contribute to a repository, create branches, create tags, manage notes		✓	✓	✓
Create, delete, and rename repositories				✓
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) (<i>not set for any security group</i>)				

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

By default, the project-level Readers groups have read-only permissions.

TASK	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Branch Creation: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓

Contribute: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓
Note Management: Can push and edit Git notes to the repository. They can also remove notes from items if they have the Force permission.	✓	✓	✓
Tag Creation: Can push tags to the repository, and can also edit or remove tags if they have the Force permission.	✓	✓	✓
Administer: Delete and rename repositories If assigned to the top-level Git repositories entry, can add additional repositories. At the branch level, users can set permissions for the branch and unlock the branch. The Administer permission set on an individual Git repository does not grant the ability to rename or delete the repository. These tasks require Administer permissions at the top-level Git repositories entry.			✓
Rewrite and destroy history (force push): Can force an update to a branch and delete a branch. A force update can overwrite commits added from any user. Users with this permission can modify the commit history of a branch.			✓

The Project Collection Build Service can read from all repositories by default. Any pipeline which runs with project collection scope can potentially read any repository in the organization/collection. You can remove this permission for a repository: set "Read" to "Deny" for the Project Collection Build Service.

TFVC

[Team Foundation Version Control \(TFVC\)](#) provides a centralized version control system to manage your source control.

TASK	READERS	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS
Contribute to a centralized version control, including Code Review (Check in, label, lock, merge, pend a change)	Read only	✓	✓	✓
Check in, revise, undo, or unlock other users' changes				✓
Manage branches, manage permissions				✓

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](#).

Build and Release

You can define and manage your builds and releases from the web portal, **Build and Release**. For an overview of pipelines features and functions, see [Continuous integration on any platform](#).

From the web portal, you can set permissions for all or individual build pipelines, release pipelines, task groups, or variable groups. See [Set build and release permissions](#).

NOTE

When the **Free access to Pipelines for Stakeholders** preview feature is enabled for the organization, Stakeholders get access to all **Build and Release** features. This is indicated by the  preview icon shown in the following table. Without this feature enabled, stakeholders can only view and approve releases. To learn more, see [Provide Stakeholders access to edit build and release pipelines](#).

TASK	STAKEHOLDER S	READERS	CONTRIBUTOR S	BUILD ADMINS	PROJECT ADMINNS	RELEASE ADMINNS
View release pipelines	<input type="checkbox"/>					
Define builds with continuous integration	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Define releases and manage deployment s	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Approve releases	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Azure Artifacts (5 users free)	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Queue builds, edit build quality	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Manage build queues and build qualities	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	
Manage build retention policies, delete and destroy builds	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Administer build permissions	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	

Manage release permissions	<input type="checkbox"/>				<input type="checkbox"/>	<input type="checkbox"/>
Create and edit task groups	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manage task group permissions	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Can view library items such as variable groups	<input type="checkbox"/>					
Use and manage library items such as variable groups	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	BUILD ADMINS	PROJECT ADMINS	RELEASE ADMINS
View build and release pipelines	<input type="checkbox"/>					
Define builds with continuous integration			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Define releases and manage deployment s			<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Approve releases	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Azure Artifacts (5 users free)			<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Queue builds, edit build quality			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Manage build queues and build qualities				<input type="checkbox"/>	<input type="checkbox"/>	

Manage build retention policies, delete and destroy builds			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Administer build permissions				<input type="checkbox"/>	<input type="checkbox"/>	
Manage release permissions					<input type="checkbox"/>	<input type="checkbox"/>
Create and edit task groups			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manage task group permissions				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Can view library items such as variable groups		<input type="checkbox"/>				
Use and manage library items such as variable groups				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Azure Test Plans

Test

You can define and manage manual tests from the web portal, **Test Plans** or **Test**. For an overview of manual test features and functions, see [Testing overview](#). You set [test permissions at the project level](#) from **Project Settings>Security**.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	PROJECT ADMINS
Provide feedback using the Test & Feedback extension	✓	✓	✓	✓
Exploratory testing, view test runs		✓	✓	✓
Manage test plans and test suites Manage test configurations and test environments			✓	✓

Exploratory testing, create and delete test runs			✓	✓
Request feedback using the Test & Feedback extension			✓	✓
Azure Test Plans (formerly Test Manager, purchased separately)			✓	✓

Azure Artifacts

You can manage feeds from the web portal, **Artifacts** or **Build and release > Packages**. Feeds have three levels of access: Owners, Contributors, and Readers. Owners can add any type of identity—individuals, teams, and groups—to any access level. To set permissions, see [Secure feeds using permissions](#).

Package management

You can manage feeds from the web portal, **Build and release > Packages**. Feeds have three levels of access: Owners, Contributors, and Readers. Owners can add any type of identity—individuals, teams, and groups—to any access level. To set permissions, see [Secure feeds using permissions](#).

PERMISSION	READER	CONTRIBUTOR	OWNER
List and restore/install packages	✓	✓	✓
Push packages		✓	✓
Unlist/deprecate packages		✓	✓
Delete/unpublish package			✓
Edit feed permissions			✓
Rename and delete 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	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	ORGANIZATION OWNER/PROJECT ADMINS

Set personal notifications or alerts	✓		✓	✓	✓
Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
READMEs	See Note 1	✓	✓	✓	✓
View Project Wikis	✓	✓	✓	✓	✓
View Code Wikis		✓	✓	✓	✓
Provision or create a Wiki					✓
Publish Code as Wiki			✓	See Note 2	See Note 2
View the project page	✓	✓	✓	✓	✓
Edit the project page					✓
Navigate using the Project pages	✓	✓	✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓
Powerful semantic code search	✓	✓	✓	✓	✓
Powerful semantic work tracking search	✓	✓	✓	✓	✓

Notes

1. Can view project READMEs, but not READMEs defined for a repository.
2. Project Admins or Team Admins with contribute permission can publish code as wiki. Project Admins have this permission by default.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	ORGANIZATION OWNER/PROJECT ADMINS
Set personal notifications or alerts	✓		✓	✓	✓
Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
READMEs	See Note 1	✓	✓	✓	✓
View Project Wikis	✓	✓	✓	✓	✓

View Code Wikis		✓	✓	✓	✓
Provision or create a Wiki					✓
Publish Code as Wiki			✓	See Note 2	See Note 2
View the project page	✓	✓	✓	✓	✓
Edit the project page					✓
Navigate using the Project pages	✓	✓	✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓
Powerful semantic code search	✓	✓	✓	✓	✓
Powerful semantic work tracking search	✓	✓	✓	✓	✓

Notes

1. Can view project READMEs, but not READMEs defined for a repository.
2. Project Admins or Team Admins with contribute permission can publish code as wiki. Project Admins have this permission by default.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	ORGANIZATION OWNER/PROJECT ADMINS
Set personal notifications or alerts	✓		✓	✓	✓
Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
Participate in Team (chat) rooms			✓	✓	✓
READMEs <i>Can view project READMEs, but not READMEs defined for a repository.</i>	Partial access	✓	✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	ORGANIZATION OWNER/PROJECT ADMINS
Set personal notifications or alerts	✓		✓	✓	✓

Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
Participate in Team (chat) rooms			✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓

Related notes

- [Add users to a project or team](#)
- [Permissions and groups reference](#)
- [About access levels](#)
- [Web portal navigation](#)

Permissions lookup guide for Azure DevOps

5/24/2019 • 6 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

Use this index to locate the topic on how to manage a specific permission. Most permissions are managed for an object, project, or collection. Other permissions are managed by adding users and groups to a role. To learn more, see [About permissions and groups](#) and [About security roles](#).

Values in parenthesis indicate what level the permission is managed:

- **Object:** Permissions are managed at the object-level
- **Project:** Permissions are managed at the project level
- **Collection:** Permissions are managed at the account or project collection level
- **Role:** Permissions are managed through a security role.
- **Team:** Permissions are managed via the team administrator role.

<p>A</p> <ul style="list-style-type: none"> • Agent queues (Project, Role) • Agent pools (Collection, Role) • Alerts (Collection) • Alerts (Team) • Analytics Service (Project) • Analytics views (Object) • Area path (Object) • Azure Artifacts <p>B</p> <ul style="list-style-type: none"> • Branches, Git (Object) • Branches, TFVC (Object) • Build pipelines (Object) • Build quality, manage (Object) • Build queue, manage (Object) • Build resources (Collection) • Build permissions, manage (Object) • Builds, manage (Object) • Bypass branch policies (Object) <p>C</p> <ul style="list-style-type: none"> • Change work item type (Project) • Check ins, TFVC (Object) • Collection-level information • Configure Azure Boards (Team) • Customize process <p>D</p> <ul style="list-style-type: none"> • Dashboards, manage (Team) • Delete field from account • Delete test artifacts • Delete work items • Delivery plans (Object) • Deployment groups (Object, Role) • Deployment pools (Collection, Role) 	<p>E</p> <ul style="list-style-type: none"> • Edit collection-level information (Collection) • Edit process • Edit project-level information (Project) • Events (Collection) • Extensions (Collection, Role) <p>F-L</p> <ul style="list-style-type: none"> • Feeds • Field, delete (Collection) • Git branch (Object) • Inherited process (Object) • Iteration paths (Object) • Kanban board, customize (Team) • Labels, TFVC (Object) • Library (Object, Role) • Locks, TFVC (Object) <p>M-N</p> <ul style="list-style-type: none"> • Manage project properties (Project) • Marketplace extensions (Collection, Role) • Merge, TFVC (Object) • Move work items (Project) • Notes, Git (Object) • Notifications (Collection) <p>P</p> <ul style="list-style-type: none"> • Policies, Git branch (Object) • Policies, Git repository (Object) • Power BI (Analytics Service) • Process (Collection) • Project properties (Project) • Project-level information 	<p>Q-R</p> <ul style="list-style-type: none"> • Query (Object) • Query folder (Object) • Release pipelines (Object) • Repository, Git (Object) <p>S</p> <ul style="list-style-type: none"> • Secure files (Object, Role) • Service endpoints (Collection, Role) • Service hooks • Shelvesets, TFVC (Collection) • Sprint, define (Object) • Sprints, select (Team) • Suppress notifications work items (Project) <p>T</p> <ul style="list-style-type: none"> • Tags, Git (Object) • Tags, work items (Project) • Task groups (Object) • Team projects (Collection) • Test artifacts, delete • Test configurations (Project) • Test controllers (Project) • Test environments (Project) • Test runs (Project) • TFVC repositories (Object) • Trace settings (Collection) <p>V-W</p> <ul style="list-style-type: none"> • Variable groups (Object, Role) • Work items (Project) • Workspaces (Collection)
---	---	--

- **Object:** Permissions are managed at the object-level
- **Project:** Permissions are managed at the project level
- **Collection:** Permissions are managed at the account or project collection level
- **Role:** Permissions are managed through a security role.
- **Server:** Permissions are managed at the instance level for a server
- **Team:** Permissions are managed via the team administrator role.

<p>A</p> <ul style="list-style-type: none"> • Administer warehouse (Server) • Agent queues (Project, Role) • Agent pools (Collection, Role) • Alerts (Collection) • Alerts (Team) • Analytics Service (Project) • Analytics views (Object) • Area path (Object) • Azure Artifacts <p>B</p> <ul style="list-style-type: none"> • Branches, Git (Object) • Branches, TFVC (Object) • Build pipelines (Object) • Build quality, manage (Object) • Build queue, manage (Object) • Build resources (Collection) • Build permissions, manage (Object) • Builds, manage (Object) • Bypass branch policies (Object) <p>C</p> <ul style="list-style-type: none"> • Change work item type (Project) • Check ins, TFVC (Object) • Collection-level information • Configure Azure Boards (Team) • Create project collection (Server) • Customize process <p>D</p> <ul style="list-style-type: none"> • Dashboards, manage (Team) • Delete field from account • Delete project collection (Server) • Delete test artifacts • Delete work items • Delivery plans (Object) • Deployment groups (Object, Role) • Deployment pools (Collection, Role) 	<p>E</p> <ul style="list-style-type: none"> • Edit collection-level information (Collection) • Edit instance level information (Server) • Edit process • Edit project-level information (Project) • Events (Collection) • Extensions (Collection, Role) <p>F-L</p> <ul style="list-style-type: none"> • Feeds • Field, delete (Collection) • Git branch (Object) • Inherited process (Object) • Iteration paths (Object) • Kanban board, customize (Team) • Labels, TFVC (Object) • Library (Object, Role) • Locks, TFVC (Object) <p>M-N</p> <ul style="list-style-type: none"> • Manage project properties (Project) • Marketplace extensions (Collection, Role) • Merge, TFVC (Object) • Move work items (Project) • Notes, Git (Object) • Notifications (Collection) <p>P</p> <ul style="list-style-type: none"> • Policies, Git branch (Object) • Policies, Git repository (Object) • Power BI (Analytics Service) • Process (Collection) • Project collection (Server) • Project properties (Project) • Project-level information 	<p>Q-R</p> <ul style="list-style-type: none"> • Query (Object) • Query folder (Object) • Release pipelines (Object) • Repository, Git (Object) <p>S</p> <ul style="list-style-type: none"> • Secure files (Object, Role) • Service endpoints (Collection, Role) • Service hooks • Shelvesets, TFVC (Collection) • Sprint, define (Object) • Sprints, select (Team) • Suppress notifications work items (Project) • Synchronization information (Collection) <p>T</p> <ul style="list-style-type: none"> • Tags, Git (Object) • Tags, work items (Project) • Task groups (Object) • Team projects (Collection) • Test artifacts, delete • Test configurations (Project) • Test controllers (Project) • Test environments (Project) • Test runs (Project) • TFVC repositories (Object) • Trace settings (Collection) • Trigger events (Server) <p>U-V-W</p> <ul style="list-style-type: none"> • Use full Web Access features (Server) • Variable groups (Object, Role) • Work items (Project) • Workspaces (Collection)
--	--	--

- **Object:** Permissions are managed at the object-level
- **Project:** Permissions are managed at the project level
- **Collection:** Permissions are managed at the account or project collection level
- **Role:** Permissions are managed through a security role.
- **Server:** Permissions are managed at the instance level for a server
- **Team:** Permissions are managed via the team administrator role.

<p>A</p> <ul style="list-style-type: none"> • Administer warehouse (Server) • Agent queues (Project, Role) • Agent pools (Collection, Role) • Alerts (Collection) • Alerts (Team) • Area path (Object) • Azure Artifacts <p>B</p> <ul style="list-style-type: none"> • Branches, Git (Object) • Branches, TFVC (Object) • Build pipelines (Object) • Build quality, manage (Object) • Build queue, manage (Object) • Build resources (Collection) • Build permissions, manage (Object) • Builds, manage (Object) • Bypass branch policies (Object) <p>C</p> <ul style="list-style-type: none"> • Check ins, TFVC (Object) • Collection-level information • Configure Agile tools (Team) • Create project collection (Server) <p>D</p> <ul style="list-style-type: none"> • Dashboards, manage (Team) • Delete field from account • Delete project collection (Server) • Delete test artifacts • Delete work items • Delivery plans (Object) • Deployment groups (Object, Role) • Deployment pools (Collection, Role) 	<p>E</p> <ul style="list-style-type: none"> • Edit collection-level information (Collection) • Edit project-level information (Project) • Events (Collection) • Extensions (Collection, Role) <p>F-L</p> <ul style="list-style-type: none"> • Feeds • Field, delete (Collection) • Git branch (Object) • Inherited process (Object) • Iteration paths (Object) • Kanban board, customize (Team) • Labels, TFVC (Object) • Library (Object, Role) • Locks, TFVC (Object) <p>M-N</p> <ul style="list-style-type: none"> • Manage project properties (Project) • Marketplace extensions (Collection, Role) • Merge, TFVC (Object) • Notes, Git (Object) • Notifications (Collection) <p>P</p> <ul style="list-style-type: none"> • Policies, Git branch (Object) • Policies, Git repository (Object) • Project collection (Server) • Project properties (Project) • Project-level information 	<p>Q-R</p> <ul style="list-style-type: none"> • Query (Object) • Query folder (Object) • Release pipelines (Object) • Repository, Git (Object) <p>S</p> <ul style="list-style-type: none"> • Secure files (Object, Role) • Service endpoints (Collection, Role) • Service hook • Shelvesets, TFVC (Collection) • Sprint, define (Object) • Sprints, select (Team) • Suppress notifications work items (Project) • Synchronization information (Collection) <p>T</p> <ul style="list-style-type: none"> • Tags, Git (Object) • Tags, work items (Project) • Task groups (Object) • Team projects (Collection) • Test configurations (Project) • Test controllers (Project) • Test environments (Project) • Test runs (Project) • TFVC repositories (Object) • Trace settings (Collection) • Trigger events (Server) <p>U-V-W</p> <ul style="list-style-type: none"> • Use full Web Access features (Server) • Variable groups (Object, Role) • Work items (Project) • Workspaces (Collection)
--	---	---

Edit project-level information

The **Edit project-level information** permission is set through the [Security admin page for a project](#). It includes the ability to perform the following tasks for all team projects defined in the account or collection:

- Create and modify areas and iterations
- Edit check-in policies
- Edit shared work item queries
- Edit project level permission ACL
- Manage process templates
- Customize a project
- Create and modify global lists
- Edit event subscriptions or alerts for teams or project events.

Edit instance-level or collection-level information

The **Edit instance-level information** (formerly **Edit collection level information**) permission is set through the [Security admin page for an account or collection](#). It includes the ability to perform the following tasks for all team projects defined in the account or collection:

- Add and administer teams and all team-related features
- Create and modify areas and iterations
- Edit check-in policies
- Edit shared work item queries
- Edit project level and collection level permission ACLs
- Manage process templates
- Customize a project or process
- Create and modify global lists
- Edit event subscriptions or alerts for teams, team projects, or collection level events.

Related notes

- [Grant or restrict permissions to select tasks](#)
- [About permissions and groups](#)
- [About security roles](#).
- [Permissions and groups reference](#)
- [Add administrators, set permissions at the project-level or project collection-level](#)

Permissions and groups in Azure DevOps

7/1/2019 • 48 minutes to read • [Edit Online](#)

[Azure DevOps Services](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

This article provides a comprehensive reference for each built-in group and permission. It's a lot of information describing each built-in security group as well as each permission.

For a quick reference to default assignments, see [Default permissions and access](#). For an overview of how permissions and security are managed, see [About permissions and groups](#). In addition to security groups, there are also [security roles](#) which provide permissions for select areas.

To learn how to add users to a group or set a specific permission that you can manage through the web portal, see the following resources:

<p>Users and groups</p> <ul style="list-style-type: none">• Add users to an administrator role• Add users to an organization• Add users to a project or a team• Make a user a team admin <p>Wiki</p> <ul style="list-style-type: none">• README & Wiki	<p>DevOps permissions</p> <ul style="list-style-type: none">• Git branch• Git repositories• TFVC• Build pipelines• Release pipelines• Approvals and approvers• Task groups• Variable groups• Role-based resources	<p>Work tracking</p> <ul style="list-style-type: none">• Area and iteration paths• Work item queries and folders• Plan permissions• Customize process <p>Reporting permissions</p> <ul style="list-style-type: none">• Dashboard permissions• Analytics• Analytics views
---	--	---

<p>Users and groups</p> <ul style="list-style-type: none">• Add users to an administrator role• Add users to a project or a team• Make a user a team admin <p>Wiki</p> <ul style="list-style-type: none">• README & Wiki	<p>DevOps permissions</p> <ul style="list-style-type: none">• Git branch• Git repositories• TFVC• Build pipelines• Release pipelines• Approvals and approvers• Task groups• Variable groups• Role-based resources	<p>Work tracking</p> <ul style="list-style-type: none">• Area and iteration paths• Work item queries and folders• Plan permissions• Customize process <p>Reporting permissions</p> <ul style="list-style-type: none">• Dashboard permissions• Analytics• Analytics views• SQL Server Reports
--	--	--

<p>Users and groups</p> <ul style="list-style-type: none">• Add users to an administrator role• Add users to a project or a team• Make a user a team admin <p>Wiki</p> <ul style="list-style-type: none">• README & Wiki	<p>DevOps permissions</p> <ul style="list-style-type: none">• Git branch• Git repositories• TFVC• Build pipelines• Release pipelines• Approvals and approvers• Task groups• Variable groups• Role-based resources	<p>Work tracking</p> <ul style="list-style-type: none">• Area and iteration paths• Work item queries and folders• Plan permissions• Customize process <p>Reporting permissions</p> <ul style="list-style-type: none">• Dashboard permissions• SQL Server Reports
--	--	--

<p>Users and groups</p> <ul style="list-style-type: none"> • Add users to an administrator role • Add users to a project or a team • Make a user a team admin <p>Wiki</p> <ul style="list-style-type: none"> • README & Wiki 	<p>DevOps permissions</p> <ul style="list-style-type: none"> • Git branch • Git repositories • TFVC • Build pipelines • Release pipelines • Approvals and approvers • Task groups • Variable groups • Role-based resources 	<p>Work tracking</p> <ul style="list-style-type: none"> • Area and iteration paths • Work item queries and folders • Plan permissions <p>Reporting permissions</p> <ul style="list-style-type: none"> • Dashboard permissions • SQL Server Reports • SharePoint integration
--	--	---

NOTE

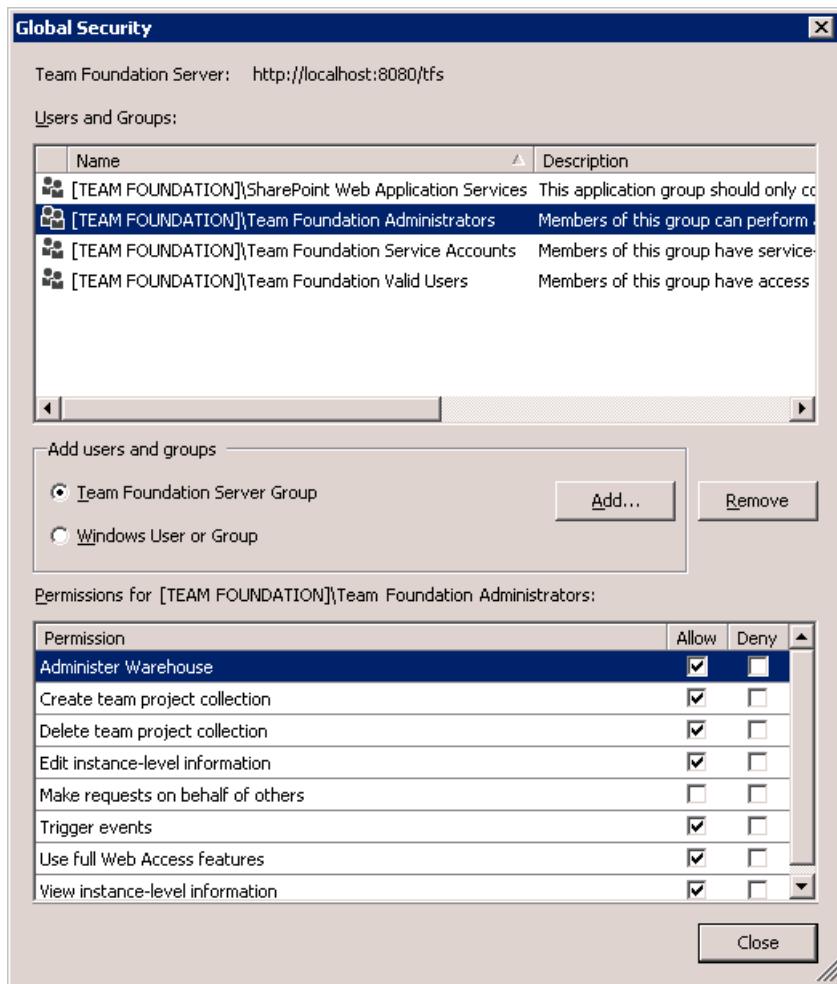
The images you see from your web portal may differ from the images you see in this topic. These differences result from updates made to Azure DevOps. However, the basic functionality available to you remains the same unless explicitly mentioned.

Groups

Permissions can be granted directly to an individual, or to a group. Using groups can make things a lot simpler. The system provides several built-in groups for that purpose. These groups and the default permissions they're assigned are defined at different levels: server (on-premises deployment only), project collection, project, and specific objects. You can also create your own groups and grant them the specific set of permissions that are appropriate for certain roles in your organization.

Server-level groups

When you install Azure DevOps Server or TFS, the system creates default groups that have [deployment-wide, server-level permissions](#). You can neither remove nor delete the built-in server-level groups.



You can't remove or delete the default server level groups.

GROUP NAME	PERMISSIONS	MEMBERSHIP
Team Foundation Administrators	Has permissions to perform all server-level operations.	<p>Local Administrators group (BUILTIN\Administrators) for any server that hosts Azure DevOps/Team Foundation application services.</p> <p>Server \Team Foundation Service Accounts group and the members of the \Project Server Integration Service Accounts group.</p> <p>This group should be restricted to the smallest possible number of users who need total administrative control over server-level operations.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>If your deployment uses SharePoint or Reporting, consider adding the members of this group to the Farm Administrators and Site Collection Administrators groups in SharePoint and the Team Foundation Content Managers groups in Reporting Services.</p> </div>
Team Foundation Proxy Service Accounts	Has service level permissions for Team Foundation Server Proxy, and some service-level permissions.	<p>This group should contain only service accounts and not user accounts or groups that contain user accounts.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Created when you install the TFS proxy service.</p> </div>

Team Foundation Service Accounts	<p>Has service-level permissions for the server instance.</p>	<p>Contains the service account that was supplied during installation</p> <p>This group should contain only service accounts and not user accounts or groups that contain user accounts. By default, this group is a member of Team Foundation Administrators.</p> <p>If you need to add an account to this group after you install Azure DevOps Server or TFS, you can do so using the TFSSecurity.exe utility in the Tools subfolder of your TFS installation directory. The command to do this is</p> <pre>TFSSecurity /g+ "[TEAM FOUNDATION]\Team Foundation Service Accounts" n:domain\username /server:http(s)://tfsservername</pre>
Team Foundation Valid Users	<p>Has permission to view server instance-level information.</p> <p>If you set the View instance-level information permission to Deny or Not set for this group, no users will be able to access the deployment.</p>	<p>Contains all users known to exist in the server instance. You can't modify the membership of this group.</p>
Project Server Integration Service Accounts	<p>Has service level permissions for the Project Server deployments that are configured for inter-operation with the server instance and some TFS service level permissions.</p> <p>Created when you install Project Service integration.</p>	<p>This group should contain only service accounts and not user accounts or groups that contain user accounts. By default, this group is a member of Team Foundation Administrators.</p>
SharePoint Web Application Services	<p>Has service level permissions for the SharePoint Web applications that are configured for use with TFS and some service level permissions for TFS.</p>	<p>This group should contain only service accounts and not user accounts or groups that contain user accounts. Unlike the Service Accounts group, this group is not a member of Team Foundation Administrators.</p>

The full name of each of these groups is **[Team Foundation]\{group name}**. So the full name of the server level administrators group is **[Team Foundation]\Team Foundation Administrators**.

Collection-level groups

When you create an organization or project collection in Azure DevOps, the system creates collection-level groups that have [permissions in that collection](#). You can neither remove nor delete the built-in collection-level groups.

Create group

Filter users and groups

✓ Azure DevOps Groups

- >  Project Collection Administrators
- >  Project Collection Build Administrators
- >  Project Collection Build Service Accounts
- >  Project Collection Proxy Service Accounts
- >  Project Collection Service Accounts
- >  Project Collection Test Service Accounts
- >  Project Collection Valid Users
- >  Security Service Group

fabrikam > Project Collection Administrators | Edit...

Permissions Members Member of

Members of this application group can perform all privileged operations.

Administrator group cannot be modified.

Administer build resource permissions	Allow
Administer process permissions	Allow
Administer shelved changes	Allow
Administer workspaces	Allow
Alter trace settings	Allow
Create a workspace	Allow
Create new projects	Allow
Create process	Allow
Delete field from account	Allow
Delete process	Allow
Delete team project	Allow
Edit instance-level information	Allow
Edit process	Allow
Make requests on behalf of others	Not set
Manage build resources	Allow
Manage test controllers	Allow
Trigger events	Allow
Use build resources	Allow
View build resources	Allow
View instance-level information	Allow
View system synchronization information	Allow

[Clear explicit permissions](#)

GROUP NAME	PERMISSIONS	MEMBERSHIP
Project Collection Administrators	Has permissions to perform all operations for the collection.	<p>Contains the Local Administrators group (BUILTIN\Administrators) for the server where the application-tier services have been installed. Also, contains the members of the CollectionName\Service Accounts group.</p> <p>This group should be restricted to the smallest possible number of users who need total administrative control over the collection. For Azure DevOps, assign to administrators who customize work tracking.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>If your deployment uses SharePoint or Reporting, consider adding the members of this group to the Site Collection Administrators group in SharePoint and the Team Foundation Content Managers groups in Reporting Services.</p> </div>
Project Collection Build Administrators	Has permissions to administer build resources and permissions for the collection.	Limit this group to the smallest possible number of users who need total administrative control over build servers and services for this collection.

Project Collection Build Service Accounts	Has permissions to run build services for the collection.	Limit this group to service accounts and groups that contain only service accounts.
Project Collection Proxy Service Accounts	Has permissions to run the proxy service for the collection.	Limit this group to service accounts and groups that contain only service accounts.
Project Collection Service Accounts	Has service level permissions for the collection and for Azure DevOps Server.	Contains the service account that was supplied during installation. This group should contain only service accounts and groups that contain only service accounts. By default, this group is a member of Team Foundation Administrators and Team Foundation Service Accounts .
Project Collection Test Service Accounts	Has test service permissions for the collection.	Limit this group to service accounts and groups that contain only service accounts.
Project Collection Valid Users	Has permissions to access team projects and view information in the collection.	Contains all users and groups that have been added anywhere within the collection. You cannot modify the membership of this group.

The full name of each of these groups is **[{collection name}]\{group name}**. So the full name of the administrator group for the default collection is **[Default Collection]\Project Collection Administrators**.

Project-level groups

For each project that you create, the system creates the followings project-level groups. These groups are assigned [project-level permissions](#).

The full name of each of these groups is **[{project name}]\{group name}**. For example, the contributors group for a project called "My Project" is **[My Project]\Contributors**.

NOTE

The project-level Release Administrator's group is created at the same time the first release pipeline is defined. It isn't created by default when the project is created.

GROUP NAME	PERMISSIONS	MEMBERSHIP
Build Administrators	Has permissions to administer build resources and build permissions for the project. Members can manage test environments, create test runs, and manage builds.	

Contributors	Has permissions to contribute fully to the project code base and work item tracking. The main permissions they don't have or those that manage or administer resources.	By default, the team group created when you create a project is added to this group, and any user you add to the team will be a member of this group. In addition, any team you create for a project will be added to this group by default, unless you choose a different group from the list.
Readers	Has permissions to view project information, the code base, work items, and other artifacts but not modify them.	Assign to members of your organization who you want to provide view-only permissions to a project. These users will be able to view backlogs, boards, dashboards, and more, but not add or edit anything. Typically, these are members who aren't granted an access level (Basic, Stakeholder, or other level) within the organization or on-premises deployment. who want to be able to view work in progress.
Project Administrators	Has permissions to administer all aspects of teams and project, although they can't create team projects.	Assign to users who manage user permissions, create or edit teams, modify team settings, define area and iteration paths, or customize work item tracking.
Project Valid Users	Has permissions to access the project. <div style="border: 1px solid #ccc; padding: 5px;"><p>If you set the View collection-level information permission to Deny or Not set for this group, no users will be able to access the project.</p></div>	Contains all users and groups that have been added anywhere within the project. You cannot modify the membership of this group.
Release Administrators	Has permissions to manage all release operations. <div style="border: 1px solid #ccc; padding: 5px;"><p>This group is defined after the first release pipeline is created. Valid for TFS-2017 and later versions.</p></div>	Assign to users who define and manage release pipelines.
{team name}	Has permissions to contribute fully to the project code base and work item tracking. The default Team group is created when you create a project, and by default is added to the Contributors group for the project. Any new teams you create will also have a group created for them and added to the Contributors group. <div style="border: 1px solid #ccc; padding: 5px;"><p>You can grant permissions to administer team assets by adding members to the team administrator role.</p></div>	Add members of the team to this group.

Team administrator role

For each team that you add, you can assign one or more team members as administrators. The team admin role isn't a group with a set of defined permissions. Instead, the team admin role is tasked with managing team assets. To learn more, see [Manage teams and configure team tools](#). To add a user as a team administrator, see [Add a team administrator](#).

NOTE

Project Administrators can manage all team administrative areas for all teams.

Permissions

The system manages permissions at different levels—server, collection, project, or object—and by default assigns them to one or more built-in groups. You manage most permissions through the web portal.

Server-level permissions

You manage server-level permissions through the [Team Foundation Administration Console](#) or [TFS Security command-line tool](#). Team Foundation Administrators are granted all server-level permissions. Other server-level groups have select permission assignments.

PERMISSION	DESCRIPTION
Administer warehouse	<p>Can process or change settings for the data warehouse or SQL Server Analysis cube by using the Warehouse Control Web Service.</p> <p>Additional permissions may be required to fully process or rebuild the data warehouse and Analysis cube.</p>
Create project collection	Can create and administer collections.
Delete project collection	Can delete a collection from the deployment. Deleting a collection will not delete the collection database from SQL Server.
Edit instance-level information	<p>Can edit server-level permissions for users and groups, and add or remove server level groups from the collection.</p> <p>Edit instance-level information includes the ability to perform these tasks for all team projects defined in all collections defined for the instance:</p> <ul style="list-style-type: none">• Create and modify areas and iterations• Edit check-in policies• Edit shared work item queries• Edit project level and collection level permission ACLs• Create and modify global lists• Edit event subscriptions (email or SOAP). <p>When set through the menus, the Edit instance-level information permission also implicitly allows the user to modify version control permissions. To grant all these permissions at a command prompt, you must use the <code>tf.exe Permission</code> command to grant the AdminConfiguration and AdminConnections permissions in addition to GENERIC_WRITE.</p>
Make requests on behalf of others	Can perform operations on behalf of other users or services. Only assign to service accounts.
Trigger events	Can trigger server-level alert events. Only assign to service accounts and members of the Team Foundation Administrators group.

Use full Web Access features	Can use all on-premises Web portal features. If the Use full Web Access features permission is set to Deny, the user will only see those features permitted for the Stakeholder group (see Change access levels). A Deny will override any implicit Allow, even for accounts that are members of administrative groups such as Team Foundation Administrators.
View instance-level information	Can view server level group membership and the permissions of those users. The View instance-level information permission is also assigned to the Team Foundation Valid Users group.

Collection-level permissions

You manage collection-level permissions through the [web portal admin context](#) or [TFSSecurity command-line tool](#). Project Collection Administrators are granted all collection-level permissions. Other collection-level groups have select permission assignments.

Permissions	Members	Member of
Members of this application group can perform all privileged operations on the Team Project Collection.		
Administrator group cannot be modified.		
Administer build resource permissions	Allow	
Administer process permissions	Allow	
Administer shelved changes	Allow	
Administer workspaces	Allow	
Alter trace settings	Allow	
Create a workspace	Allow	
Create new projects	Allow	
Create process	Allow	
Delete field from account	Allow	
Delete process	Allow	
Delete team project	Allow	
Edit instance-level information	Allow	
Edit process	Allow	
Make requests on behalf of others	Not set	
Manage build resources	Allow	
Manage test controllers	Allow	
Trigger events	Allow	
Use build resources	Allow	
View build resources	Allow	
View instance-level information	Allow	
View system synchronization information	Allow	

PERMISSION	DESCRIPTION

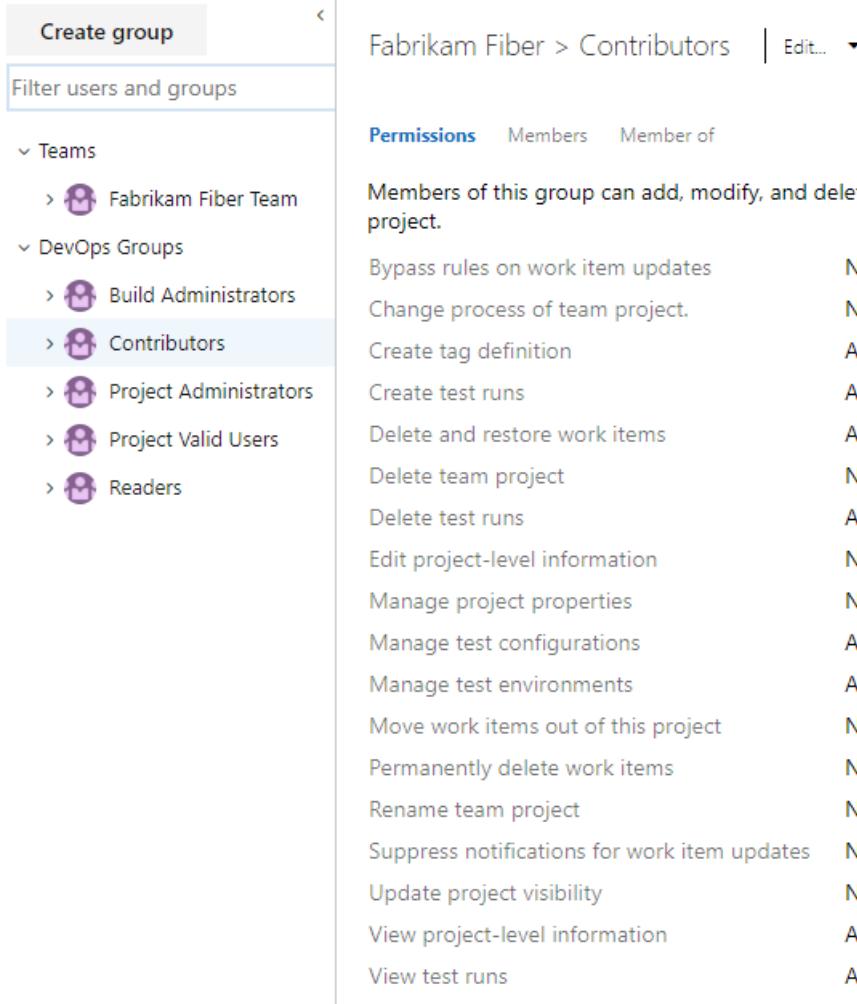
Administer build resource permissions	<p>Can modify permissions for build pipelines at the organization or project collection-level. This includes:</p> <ul style="list-style-type: none"> • Set retention policies • Set resource limits for pipelines • Add and manage agent pools • Add and manage deployment pools
Administer process permissions	<p>Can modify permissions for customizing work tracking by creating and customizing inherited processes.</p> <ul style="list-style-type: none"> • Customize a project • Add and manage processes <p>Applies to Azure DevOps Services and Azure DevOps Server 2019. For Azure DevOps Services, users granted Basic and Stakeholder access are granted this permission by default. >/p></p>
Administer Project Server integration	<p>Can configure the integration of Azure DevOps Server and Project Server to enable data synchronization between the two server products. Applies to TFS 2017 and earlier versions only.</p>
Administer shelved changes	<p>Can delete shelvesets created by other users. Applies when TFVC is used as the source control.</p>
Administer workspaces	<p>Can create and delete workspaces for other users. Applies when TFVC is used as the source control.</p>
Alter trace settings	<p>Can change the trace settings for gathering more detailed diagnostic information about Azure DevOps Web services.</p>
Create a workspace	<p>Can create a version control workspace. Applies when TFVC is used as the source control.</p> <p>The Create a workspace permission is granted to all users as part of their membership within the Project Collection Valid Users group.</p>
Create new projects (formerly Create new team projects)	<p>Can add Azure DevOps projects to an organization or project collection. Additional permissions may be required depending on your on-premises deployment.</p>
Create process	<p>Can create an inherited process used to customize work tracking and Azure Boards. Applies to Azure DevOps Services and Azure DevOps Server 2019 and later versions. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default.</p>
Delete field from account	<p>Can delete a custom field that was added to a process. Applies to Azure DevOps Services and Azure DevOps Server 2019 and later versions. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default.</p>
Delete process	<p>Can delete an inherited process used to customize work tracking and Azure Boards. Applies to Azure DevOps Services and Azure DevOps Server 2019. Azure DevOps Services users granted Basic and Stakeholder access for Azure DevOps Services are granted this permission by default.</p>

Delete team project	<p>Can delete Azure DevOps projects.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Deleting a project will delete all data that is associated with the project. You cannot undo the deletion of a project except by restoring the collection to a point before the project was deleted.</p> </div>
Edit collection-level information	<p>Can add users and groups, and edit collection-level permissions for users and groups.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Edit collection-level information includes the ability to perform these tasks for all projects defined in a collection:</p> <ul style="list-style-type: none"> • Add and administer teams and all team-related features • Create and modify areas and iterations • Edit check-in policies • Edit shared work item queries • Edit project level and collection level permission ACLs • Manage process templates • Customize a project or process • Create and modify global lists • Edit event subscriptions (email or SOAP) on project or collection level events. <p>When you set Edit collection-level information to Allow, users can add or remove collection-level groups and implicitly allows these users to modify version control permissions. To grant all these permissions at a command prompt, you must use the <code>tf.exe Permission</code> command to grant the AdminConfiguration and AdminConnections permissions, in addition to GENERIC_WRITE.</p> </div>
Edit process	<p>Can edit a custom inherited process. Applies to Azure DevOps Services and Azure DevOps Server 2019. Azure DevOps Services users granted Basic and Stakeholder access for Azure DevOps Services are granted this permission by default.</p>
Make requests on behalf of others	<p>Can perform operations on behalf of other users or services. You should assign this permission only to on-premises service accounts.</p>
Manage build resources	<p>Can manage build computers, build agents, and build controllers.</p>
Manage process template	<p>Can download, create, edit, and upload process templates. A process template defines the building blocks of the work item tracking system as well as other sub-systems you access through Azure Boards. Applies to Azure DevOps Servers only.</p>
Manage test controllers	<p>Can register and de-register test controllers.</p>
Trigger events	<p>Can trigger project alert events within the collection. Assign only to service accounts.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Users with this permission can't remove built-in collection level groups such as Project Collection Administrators.</p> </div>
Use build resources	<p>Can reserve and allocate build agents. Assign only to service accounts for build services.</p>
View build resources	<p>Can view, but not use, build controllers and build agents that are configured for an organization or project collection.</p>

View instance-level information or View collection-level information	Can view project collection-level group membership and permissions. If you set the View instance-level information permission to Deny or Not set for this group, no users will be able to access projects in the organization or project collection.
View system synchronization information	Can call the synchronization application programming interfaces. Assign only to service accounts.

Project-level permissions

You manage project-level permissions from the [web portal admin context](#) or using the [TFS Security command-line tool](#). Project Administrators are assigned all project-level permissions. Other project-level groups are assigned a subset of these permissions.



The screenshot shows the 'Create group' interface on the left and the 'Contributors' group details on the right. The left pane shows a tree view of groups under 'Teams' and 'DevOps Groups'. The 'Contributors' group is selected and highlighted in blue. The right pane shows the 'Contributors' group details for the 'Fabrikam Fiber' project. It includes tabs for 'Permissions', 'Members', and 'Member of'. Below the tabs, it says 'Members of this group can add, modify, and delete items within the team project.' A table lists various permissions with their current status:

Permission	Status
Bypass rules on work item updates	Not set
Change process of team project.	Not set
Create tag definition	Allow
Create test runs	Allow
Delete and restore work items	Allow
Delete team project	Not set
Delete test runs	Allow
Edit project-level information	Not set
Manage project properties	Not set
Manage test configurations	Allow
Manage test environments	Allow
Move work items out of this project	Not set
Permanently delete work items	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
View test runs	Allow

PERMISSION	DESCRIPTION

Bypass rules on work item updates	<p>Users with this permission can save a work item that ignores rules, such as assign value rules or conditional rules, defined for the work item type. Scenarios where this is useful are migrations where you don't want to update the by/date fields on import, or when you want to skip the validation of a work item.</p> <p>Rules can be bypassed in one of two ways. The first is through the Work Items - update REST API and setting the <code>bypassRules</code> parameter to <code>true</code>. The second is through the client object model, by initializing in <code>bypassrules</code> mode (initialize <code>WorkItemStore</code> with <code>WorkItemStoreFlags.BypassRules</code>).</p> <p>Users granted Basic and Stakeholder access are granted this permission by default.</p>
Change process of project	<p>Can change the Inheritance process for a project. To learn more, see Create and manage inherited processes. Applies to Azure DevOps Services and Azure DevOps Server 2019. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default.</p>
Create tag definition	<p>Can add tags to a work item. By default, all members of the Contributors group have this permission.</p> <p>All users granted Stakeholder access for a private project can only add existing tags, not add new tags, even if the Create tag definition permission is set to Allow. This is part of the Stakeholder access settings. Azure DevOps Services users granted Stakeholder access for a public project are granted this permission by default.</p>
Create test runs	<p>Can add and remove test results and add or modify test runs. To learn more, see Control how long to keep test results and Run manual tests.</p>
Delete and restore work items or Delete work items in this project	<p>Can mark work items in the project as deleted. Azure DevOps Services users granted Stakeholder access for a public project are granted this permission by default.</p> <ul style="list-style-type: none"> For Azure DevOps and TFS 2015.1 and later versions, the Contributors group has Delete and restore work items at the project-level set to "Allow" by default. For TFS 2015 and earlier versions, the Contributors group has Delete work items in this project at the project-level set to "Not set" by default. This setting causes the Contributors group to inherit the value from the closest parent that has it explicitly set.
Delete shared Analytics view	<p>Can delete Analytics views that have been saved under the Shared area. Applies to Azure DevOps Services and Azure DevOps Server 2019.</p>
Delete project	<p>Can delete a project from an organization or project collection.</p>
Delete test runs	<p>Can delete a test run.</p>

Edit project-level information	<p>Can edit project level permissions for users and groups.</p> <p>Edit project-level information includes the ability to perform these tasks for the project:</p> <ul style="list-style-type: none"> • Create and modify areas and iterations • Edit check-in policies • Edit shared work item queries • Edit project level permission ACLs • Manage process templates • Customize a project • Create and modify global lists • Edit event subscriptions (email or SOAP) on project level events.
Edit shared Analytics view	Can create and modify shared Analytics views . Applies to Azure DevOps Services and Azure DevOps Server 2019.
Manage project properties	Can provide or edit metadata for a project. For example, a user can provide high-level information about the contents of a project. Changing metadata is supported through the Set project properties REST API .
Manage test configurations	Can create and delete test configurations .
Manage test environments	Can create and delete test environments .
Move work items out of this project	Can move a work item from one project to another project within the collection. Applies to Azure DevOps Services and Azure DevOps Server 2019. Users granted Stakeholder access for a public project are granted this permission by default.
Permanently delete work items in this project	Can permanently delete work items from this project. Azure DevOps Services users granted Stakeholder access for a public project are granted this permission by default.
Rename project	Can change the name of the project .
Suppress notifications for work item updates	<p>Users with this permission can update work items without generating notifications. This is useful when performing migrations of bulk updates by tools and want to skip generating notifications.</p> <p>Consider granting this permission to service accounts or users who have been granted the Bypass rules on work item updates permission. You can set the <code>suppressNotifications</code> parameter to <code>true</code> when updating working via Work Items - update REST API.</p> <p>Users granted Stakeholder access for a public project are granted this permission by default.</p>
Update project visibility	Can change the project visibility from private to public or public to private. Applies to Azure DevOps Services only.
View analytics	Can access data available from the Analytics service . For details, see Permissions required to access the Analytics service . Applies to Azure DevOps Services and Azure DevOps Server 2019.
View project-level information	Can view project level group membership and permissions.
View test runs	Can view test plans under the project area path.

Analytics views (object-level)

With shared Analytics views, you can grant specific permissions to view, edit, or delete a view that you create. You manage the security of Analytics views from the [web portal](#).

The screenshot shows the 'Permissions for Work Items - Today' dialog. On the left, there's a sidebar with a search bar and a list of groups and users. On the right, there's an 'ACCESS CONTROL SUMMARY' section with a note about the administrator group. It lists three permissions: Delete shared Analytics views, Edit shared Analytics views, and View shared Analytics views, all set to 'Allow (inherited)'. There are buttons for 'Remove', 'Save changes', and 'Undo changes', and a 'Close' button at the bottom.

The following permissions are defined for each shared Analytics view. All valid users are automatically granted all permissions to manage Analytics views. Consider granting select permissions to specific shared views to other team members or security group that you create. See also, [What are Analytics views?](#)

PERMISSION	DESCRIPTION
Delete shared Analytics views	Can delete the shared Analytics view.
Edit shared Analytics views	Can change the parameters of the shared Analytics view.
View shared Analytics views	Can view and use the shared Analytics view from Power BI desktop.

Build (object-level)

You manage build permissions [for each build defined in the web portal](#) or using the [TFS Security command-line tool](#). Project Administrators are granted all build permissions and Build Administrators are assigned most of these permissions. You can set build permissions for all build definitions or for each build definition.

Permissions for fabrikam build

Permission	Description
Administer build permissions	Allow (inherited)
Delete build definition	Allow (inherited)
Delete builds	Allow (inherited)
Destroy builds	Allow (inherited)
Edit build definition	Allow (inherited)
Edit build quality	Allow (inherited)
Manage build qualities	Allow (inherited)
Manage build queue	Allow (inherited)
Override check-in validation by build	Not set
Queue builds	Allow (inherited)
Retain indefinitely	Allow (inherited)
Stop builds	Allow (inherited)
Update build information	Not set
View build definition	Allow (inherited)
View builds	Allow (inherited)

Permissions in Build follow a hierarchical model. Defaults for all the permissions can be set at the project level and can be overridden on an individual build definition.

To set the permissions at project level for all build definitions in a project, choose **Security** from the action bar on the main page of Builds hub.

To set or override the permissions for a specific build definition, choose **Security** from the context menu of the build definition.

The following permissions are defined in Build. All of these can be set at both the levels.

PERMISSION	DESCRIPTION
Administer build permissions	Can administer the build permissions for other users.
Delete build definition	Can delete build definitions for this project.
Delete builds	Can delete a completed build. Builds that are deleted are retained in the Deleted tab for a period of time before they are destroyed.
Destroy builds	Can permanently delete a completed build.

Edit build definition	<p>Can create and modify build definitions for this project.</p> <p>You turn Inheritance Off for a build definition when you want to control permissions for specific build definitions.</p> <p>When inheritance is On, the build definition respects the build permissions defined at the project level or a group or user. For example, a custom Build Managers group has permissions set to manually queue a build for project Fabrikam. Any build definition with inheritance On for project Fabrikam would allow a member of the Build Managers group the ability to manually queue a build.</p> <p>However, by turning Inheritance Off for project Fabrikam, you can set permissions that only allow Project Administrators to manually queue a build for a specific build definition. This would then allow me to set permissions for that build definition specifically.</p>
Edit build quality	Can add information about the quality of the build through Team Explorer or the web portal.
Manage build qualities	Can add or remove build qualities. <i>Only applies to XAML builds.</i>
Manage build queue	Can cancel, re-prioritize, or postpone queued builds. <i>Only applies to XAML builds</i>
Override check-in validation by build	<p>Can commit a TFVC change set that affects a gated build definition without triggering the system to shelve and build their changes first.</p> <p>Assign the Override check-in validation by build permission only to service accounts for build services and to build administrators who are responsible for the quality of the code. Applies to TFVC gated check-in builds. This does not apply to PR builds. For more information, see Check in to a folder that is controlled by a gated check-in build process.</p>
Queue builds	Can put a build in the queue through the interface for Team Foundation Build or at a command prompt. They can also stop the builds that they have queued.
Retain indefinitely	Can toggle the retain indefinitely flag on a build. This feature marks a build so that the system won't automatically delete it based on any applicable retention policy.
Stop builds	Can stop any build that is in progress, including builds queued and started by another user.
Update build information	Can add build information nodes to the system, and can also add information about the quality of a build. Assign only to service accounts.
View build definition	Can view the build definitions that have been created for the project.
View builds	Can view the queued and completed builds for this project.

Git repository (object-level)

You manage the security of each [Git repository](#) or [branch](#) from the web portal, the [TF command line tool](#), or using the [TFSSecurity command-line tool](#). Project Administrators are granted most of these permissions (which appear only for a project that's been configured with a Git repository). You can manage these

permissions for all Git repositories, or for a specific Git repo.

NOTE

These permissions have changed in TFS 2017 Update 1 and Azure DevOps. If you are using an earlier version of TFS, see the [previous list of permissions](#).

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Bypass policies when completing pull requests	Not set
Bypass policies when pushing	Not set
Contribute	Allow
Contribute to pull requests	Allow
Create branch	Allow
Create repository	Allow
Create tag	Allow
Delete repository	Allow
Edit policies	Allow
Force push (rewrite history, delete branches and tags)	Deny
Manage notes	Allow
Manage permissions	Allow
Read	Allow
Remove others' locks	Allow
Rename repository	Allow

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Contribute	Allow
Create branch	Allow
Create repository	Allow
Create tag	Allow
Delete repository	Allow
Edit policies	Allow
Exempt from policy enforcement	Not set
Force push (rewrite history, delete branches and tags)	Allow
Manage notes	Allow
Manage permissions	Allow
Read	Allow
Remove others' locks	Allow
Rename repository	Allow

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry.

Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit permissions from assignments made at the repository level.

By default, the project level Readers groups have only Read permissions.

Permission	Description
Bypass policies when completing pull requests	<p>Can opt-in to override branch policies by checking Override branch policies and enable merge when completing a PR.</p> <p>Bypass policies when completing pull requests and Bypass policies when pushing replace Exempt From Policy Enforcement. Applies to Azure DevOps Services and Azure DevOps Server 2019.</p>
Bypass policies when pushing	<p>Can push to a branch that has branch policies enabled. Note that when a user with this permission makes a push that would override branch policy, the push automatically bypasses branch policy with no opt-in step or warning.</p> <p>Bypass policies when completing pull requests and Bypass policies when pushing replace Exempt From Policy Enforcement. Applies to Azure DevOps Services and Azure DevOps Server 2019.</p>
Contribute	<p>At the repository level, can push their changes to existing branches in the repository and can complete pull requests. Users who lack this permission but who have the Create branch permission may push changes to new branches. Does not override restrictions in place from branch policies.</p> <p>At the branch level, can push their changes to the branch and lock the branch. Locking a branch blocks any new commits from being added to the branch by others and prevents other users from changing the existing commit history.</p>
Contribute to pull requests	Can create, comment on, and vote on pull requests.
Create branch	Can create and publish branches in the repository. Lack of this permission does not limit users from creating branches in their local repository; it merely prevents them from publishing local branches to the server. When a user creates a new branch on the server, they have Contribute, Edit Policies, Force Push, Manage Permissions, and Remove Others' Locks permissions for that branch by default.
Create repository	Can create new repositories. This permission is only available from the Security dialog for the top-level Git repositories object.
Create tag	Can push tags to the repository.
Delete repository	Can delete the repository. At the top-level Git repositories level, can delete any repository.
Edit policies	Can edit policies for the repository and its branches.
Exempt From policy enforcement	<p>Can bypass branch policies and perform the following two actions:</p> <ul style="list-style-type: none"> • Override branch policies and complete PRs that don't satisfy branch policy • Push directly to branches that have branch policies set <p>Applies to TFS 2015 through TFS 2018 Update 2. (In Azure DevOps it is replaced with the following two permissions)(/azure/devops/release-notes/2018/jul-10-vsts#allow-bypassing-branch-policies-without-giving-up-push-protection); Bypass policies when completing pull requests and Bypass policies when pushing.)</p>
Force push (rewrite history, delete branches and tags)	Can force an update to a branch, delete a branch, and modify the commit history of a branch. Can delete tags and notes.

Manage notes	Can push and edit Git notes.
Manage permissions	Can set permissions for the repository.
Read	Can clone, fetch, pull, and explore the contents of the repository.
Remove others' locks	Can remove branch locks set by other users. Locking a branch blocks any new commits from being added to the branch by others and prevents other users from changing the existing commit history.
Rename repository	Can change the name of the repository. When set at the top-level Git repositories entry, can change the name of any repository.

NOTE

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git repositories** entry. Branches inherit permissions from assignments made at the repository level. By default, the project level Readers groups only have Read permissions.

To manage Git repo and branch permissions, see [Set branch permissions](#).

TFVC (object-level)

You manage the security of each TFVC branch from the [web portal](#) or using the [TFS Security command-line tool](#). Project Administrators are granted most of these permissions which appear only for a project that's been configured to use Team Foundation Version Control as a source control system. In version control permissions, explicit deny takes precedence over administrator group permissions.

These permissions appear only for a project set up to use Team Foundation Version Control as the source control system.

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Administer labels	Not set
Check in	Allow
Check in other users' changes	Not set
Label	Allow
Lock	Allow
Manage branch	Not set
Manage permissions	Not set
Merge	Allow
Pend a change in a server workspace	Allow
Read	Allow
Revise other users' changes	Not set
Undo other users' changes	Not set
Unlock other users' changes	Not set

In version control permissions, explicit deny takes precedence over administrator group permissions.

Permission	Description
Administer labels	Can edit or delete labels created by another user.
Check in	<p>Can check in items and revise any committed change set comments. Pending changes are committed at check-in.</p> <p>Consider adding these permissions to any manually added users or groups that contributes to the development of the project; any users who should be able to check in and check out changes, make a pending change to items in a folder, or revise any committed change set comments.</p>
Check in other users' changes	Can check in changes that were made by other users. Pending changes are committed at check-in.
Check out (up through TFS 2015) Pend a change in a server workspace (TFS 2017 and higher)	<p>Can check out and make a pending change to items in a folder. Examples of pending changes include adding, editing, renaming, deleting, undeleting, branching, and merging a file. Pending changes must be checked in, so users will also need the Check in permission to share their changes with the team.</p> <p>Consider adding these permissions to any manually added users or groups that contributes to the development of the project; any users who should be able to check in and check out changes, make a pending change to items in a folder, or revise any committed change set comments.</p>
Label	Can label items.
Lock	Can lock and unlock folders or files. A folder or file tracked can be locked or unlocked to deny or restore a user's privileges. Privileges include checking out an item for edit into a different workspace or checking in Pending Changes to an item from a different workspace. For more information, see Lock command .
Manage branch	Can convert any folder under that path into a branch, and also take the following actions on a branch: edit its properties, re-parent it, and convert it to a folder. Users who have this permission can branch this branch only if they also have the Merge permission for the target path. Users cannot create branches from a branch for which they do not have the Manage Branch permission.
Manage permissions	<p>Can manage other users' permissions for folders and files in version control.</p> <p>Consider adding this permission to any manually added users or groups that contributes to the development of the project and that must be able to create private branches, unless the project is under more restrictive development practices.</p>
Merge	<p>Can merge changes into this path.</p> <p>Consider adding this permission to any manually added users or groups that contribute to the development of the project and that must be able to merge source files, unless the project is under more restrictive development practices.</p>
Read	Can read the contents of a file or folder. If a user has Read permissions for a folder, the user can see the contents of the folder and the properties of the files in it, even if the user does not have permission to open the files.

Revise other users' changes	<p>Can edit the comments on checked-in files, even if another user checked in the file.</p> <p>Consider adding this permission to any manually added users or groups that are responsible for supervising or monitoring the project and that might or must change the comments on checked-in files, even if another user checked in the file.</p>
Undo other users' changes Merge	<p>Can undo a pending change made by another user.</p> <p>Consider adding this permission to any manually added users or groups that are responsible for supervising or monitoring the project and that might or must change the comments on checked-in files, even if another user checked in the file.</p>
Unlock other users' changes	<p>Can unlock files locked by other users.</p> <p>Consider adding this permission to any manually added users or groups that are responsible for supervising or monitoring the project and that might or must change the comments on checked-in files, even if another user checked in the file.</p>

Area path (object-level)

Area path permissions grant or restrict access to branches of the area hierarchy and to the work items in those areas. You manage the security of each area path from the [web portal](#) or using the [TFS Security command-line tool](#). Area permissions grant or restrict access to create and manage area paths as well as create and modify work items defined under area paths.

Members of the Project Administrators group are automatically granted permissions to manage area paths for a project. Consider granting team administrators or team leads permissions to create, edit, or delete area nodes.

NOTE

Multiple teams may contribute to a project. When that's the case, you can set up teams that are associated with an area. Permissions for the team's work items are assigned by assigning permissions to the area. There are other [team settings](#) that configure the team's agile planning tools.

Permissions for Fabrikam Fiber

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Permission	Setting
Create child nodes	Not set
Delete this node	Not set
Edit this node	Not set
Edit work items in this node	Allow
Manage test plans	Allow
Manage test suites	Allow
View permissions for this node	Allow
View work items in this node	Allow

[Clear explicit permissions](#)

[Remove](#) [Save changes](#) [Undo changes](#)

[Close](#)

PERMISSION	DESCRIPTION
Create child nodes	<p>Can create area nodes. Users who have both this permission and the Edit this node permission can move or re-order any child area nodes. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default for both public and private projects.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that may need to delete, add, or rename area nodes. </div>
Delete this node	<p>Users who have both this permission and the Edit this node permission for another node can delete area nodes and reclassify existing work items from the deleted node. If the deleted node has child nodes, those nodes are also deleted.</p> <p>Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default for both public and private projects.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that may need to delete, add, or rename area nodes. </div>
Edit this node	<p>Can set permissions for this node and rename area nodes. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default for both public and private projects.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that may need to delete, add, or rename area nodes. </div>

Edit work items in this node	Can edit work items in this area node. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default for both public and private projects. Consider adding this permission to any manually added users or groups that may need to edit work items under the area node.
Manage test plans	Can modify test plan properties such as build and test settings. Consider adding Manage test suites permissions to any manually added users or groups that may need to manage test plans or test suites under this area node.
Manage test suites	Can create and delete test suites, add and remove test cases from test suites, change test configurations associated with test suites, and modify suite hierarchy (move a test suite). Consider adding Manage test suites permissions to any manually added users or groups that may need to manage test plans or test suites under this area node.
View permissions for this node	Can view the security settings for this node.
View work items in this node	Can view, but not change, work items in this area node. Azure DevOps Services users granted Basic and Stakeholder access are granted this permission by default for both public and private projects. If you set the View work items in this node to Deny, the user will not be able to see any work items in this area node. A Deny will override any implicit allow, even for accounts that are members of administrative groups such as Team Foundation Administrators.

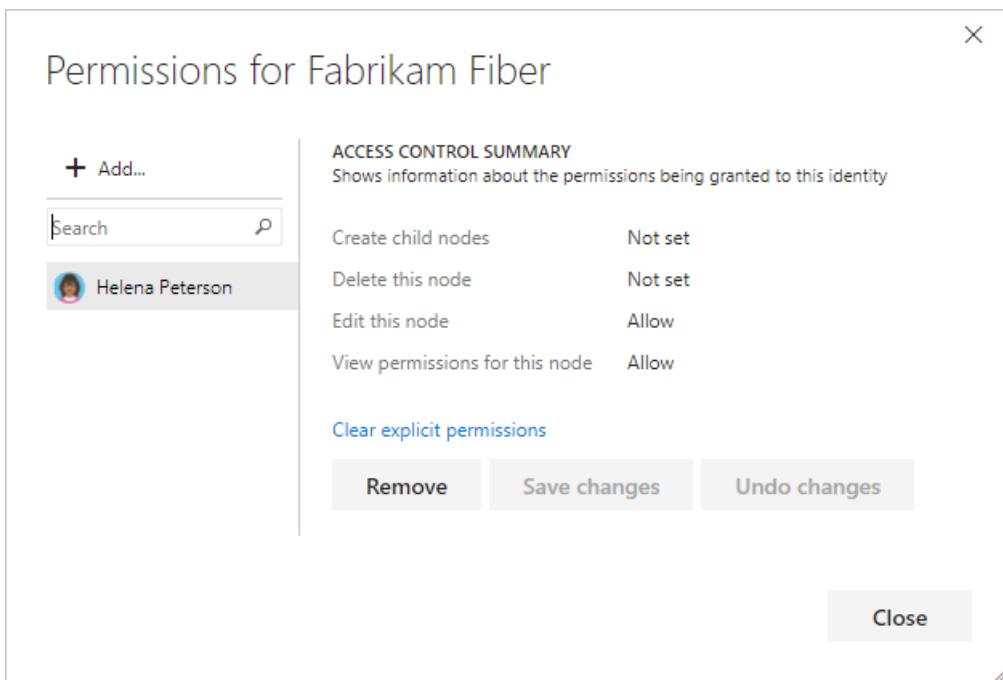
Iteration Path (object-level)

Iteration path permissions grant or restrict access to create and manage iteration paths.

Multiple teams may contribute to a project. When that's the case, you can set up teams that are associated with an area. Permissions for the team's work items are assigned by assigning permissions to the area. There are other [team settings](#) that configure the team's agile planning tools. To learn more, see [Set permissions to restrict access to work items](#).

You manage the security of each iteration path from the [web portal](#) or using the [TFSSecurity command-line tool](#).

Members of the Project Administrators group are automatically granted these permissions for each iteration defined for a project. Consider granting team administrators, scrum masters, or team leads permissions to create, edit, or delete iteration nodes.



Consider granting team administrators, scrum masters, or team leads permissions to create, edit, or delete iteration nodes.

PERMISSION	DESCRIPTION
Create child nodes	<p>Can create iteration nodes. Users who have both this permission and the Edit this node permission can move or re-order any child iteration nodes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that might need to delete, add, or rename iteration nodes. </div>
Delete this node	<p>Users who have both this permission and the Edit this node permission for another node can delete iteration nodes and reclassify existing work items from the deleted node. If the deleted node has child nodes, those nodes are also deleted.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that might need to delete, add, or rename iteration nodes. </div>
Edit this node	<p>Can set permissions for this node and rename iteration nodes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Consider adding this permission to any manually added users or groups that might need to delete, add, or rename iteration nodes. </div>
View permissions for this node	<p>Can view the security settings for this node.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Members of the Project Collection Valid Users, Project Valid Users, or any user or group that has View collection-level information or View project-level information can view permissions of any iteration node. </div>

Work item query and folder (object-level)

You manage query and query folder permissions through the [web portal](#). Project Administrators are granted all of these permissions. Contributors are granted Read permissions only. Consider granting the Contribute permissions to users or groups that require the ability to create and share work item queries for the project.

Permissions for Shared Queries/Current Sprint

Consider granting the Contribute permissions to users or groups that require the ability to create and share work item queries for the project. To learn more, see [Set permissions on queries](#).

To create query charts [you need Basic access](#).

PERMISSION	DESCRIPTION
Contribute	Can view and modify this query or query folder.
Delete	Can delete a query or query folder and its contents.
Manage permissions	Can manage the permissions for this query or query folder.
Read	Can view and use the query or the queries in a folder, but cannot modify the query or query folder contents.

Delivery Plans (object-level)

You manage plan permissions through the [web portal](#). You manage permissions for each plan through its Security dialog. Project Administrators are granted all permissions to create, edit, and manage plans. Valid users are granted View (read-only) permissions.

NOTE

For TFS 2017.2 and later versions, you can access plans by installing the [Delivery Plans Marketplace extension](#).

PERMISSION	DESCRIPTION
Delete	Can delete the selected plan.

Edit	Can edit the configuration and settings defined for the selected plan.
Manage	Can manage the permissions for the selected plan.
View	Can view the lists of plans, open and interact with a plan, but cannot modify the plan configuration or settings.

Process (object-level)

You can manage the permissions for each inherited process that you create through the [web portal](#). You manage permissions for each process through its Security dialog. Project Collection Administrators are granted all permissions to create, edit, and manage processes. Valid users are granted View (read-only) permissions.

PERMISSION	DESCRIPTION
Administer process permissions	Can set or change the permissions for an inherited process.
Delete process	Can delete the inherited process.
Edit process	Can create an inherited process from a system process, or copy or modify an inherited process.

Work item tags

You manage tagging permissions mostly from the [TFS Security command-line tool](#). Contributors can add tags to work items and use them to quickly filter a backlog, board, or query results view.

PERMISSION	DESCRIPTION
Create tag definition	<p>Can create new tags and apply them to work items. Users without this permission can only select from the existing set of tags for the project.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Readers and Contributors inherit the Create tag definition permission as it is set explicitly to Allow for the Project Valid Users group.</p> <p>Although the Create tag definition permission appears in the security settings at the project level, tagging permissions are actually collection level permissions that are scoped at the project level when they appear in the user interface. To scope tagging permissions to a single project when using the TFS Security command, you must provide the GUID for the project as part of the command syntax. Otherwise, your change will apply to the entire collection. Keep this in mind when changing or setting these permissions.</p> </div>
Delete tag definition	<p>Can remove a tag from the list of available tags for that project.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>This permission does not appear in the UI. It can only be set by using the TFS Security command.</p> <p>There is also no UI to explicitly delete a tag. Instead, when a tag has not been in use for 3 days, TFS automatically deletes it.</p> </div>

Enumerate tag definition	<p>Can view a list of tags available for the work item within the project. Users without this permission will not have a list of available tags from which to choose in the work item form or in the query editor.</p> <p>This permissions does not appear in the UI. It can only be set by using the TFS Security command.</p> <p>The View project-level information implicitly allows users to view existing tags.</p>
Update tag definition	<p>Can rename a tag by using the REST API.</p> <p>This permissions does not appear in the UI. It can only be set by using the TFS Security command.</p>

Release (object-level)

If you are working with the Release Management client and server supported for TFS 2015, see [Automate deployments with Release Management](#).

Release (object-level)

You manage permissions [for each release defined in the web portal](#). Project Administrators and Release Administrators are granted all release management permissions. These permissions can be granted or denied in a hierarchical model at the project level, for a specific release pipeline, or for a specific environment in a release pipeline. Within this hierarchy, permissions can be inherited from the parent or overridden.

NOTE

The project-level Release Administrator's group is created at the same time the first release pipeline is defined.

In addition, you can assign approvers to specific steps within a release pipeline to ensure that the applications being deployed meet quality standards.

The following permissions are defined in Release Management. The scope column explains whether the permission can be set at the project, release pipeline, or environment level.

PERMISSION	DESCRIPTION	SCOPES
Administer release permissions	Can change any of the other permissions listed here.	Project, Release pipeline, Environment
Create releases	Can create new releases.	Project, Release pipeline
Delete release pipeline	Can delete release pipeline(s).	Project, Release pipeline
Delete release environment	Can delete environment(s) in release pipeline(s).	Project, Release pipeline, Environment
Delete releases	Can delete releases for a pipeline.	Project, Release pipeline

Permission	Description	Scopes
Edit release pipeline	<p>Can save any changes to a release pipeline, including configuration variables, triggers, artifacts, and retention policy as well as configuration within an environment of the release pipeline. To make changes to a specific environment in a release pipeline, the user also needs Edit release environment permission.</p>	Project, Release pipeline
Edit release environment	<p>Can edit environment(s) in release pipeline(s). To save the changes to the release pipeline, the user also needs Edit release definition permission. This permission also controls whether a user can edit the configuration inside the environment of a specific release instance. The user also needs Manage releases permission to save the modified release.</p>	Project, Release pipeline, Environment
Manage deployments	<p>Can initiate a direct deployment of a release to an environment. This permission is only for direct deployments that are manually initiated by selecting the Deploy action in a release. If the condition on an environment is set to any type of automatic deployment, the system automatically initiates deployment without checking the permission of the user that created the release.</p>	Project, Release pipeline, Environment
Manage release approvers	<p>Can add or edit approvers for environment(s) in release pipeline(s). This permission also controls whether a user can edit the approvers inside the environment of a specific release instance.</p>	Project, Release pipeline, Environment
Manage releases	<p>Can edit the configuration in releases. To edit the configuration of a specific environment in a release instance, the user also needs Edit release environment permission.</p>	Project, Release pipeline
View release pipeline	Can view release pipeline(s).	Project, Release pipeline
View releases	Can view releases belonging to release pipeline(s).	Project, Release pipeline

Default values for all of these permissions are set for team project collections and project groups. For example, **Project Collection Administrators**, **Project Administrators**, and **Release Administrators** are given all of the above permissions by default. **Contributors** are given all permissions except **Administer release permissions**. **Readers**, by default, are denied all permissions except **View release pipeline** and **View releases**.

Task group (Build and Release) permissions

You manage permissions [for task groups from the Build and Release hub](#) of the web portal. Project, Build, and Release Administrators are granted all permissions. Task group permissions follow a hierarchical model. Defaults for all the permissions can be set at the project level and can be overridden on an individual task group definition.

You use task groups to encapsulate a sequence of tasks already defined in a build or a release definition into a single reusable task. You [define and manage task groups](#) in the **Task groups** tab of the **Build and Release** hub.

PERMISSION	DESCRIPTION
Administer task group permissions	Can add and remove users or groups to task group security.
Delete task group	Can delete a task group.
Edit task group	Can create, modify, or delete a task group.

Lab Management

Visual Studio Lab Management permissions are specific to virtual machines, environments, and other resources. In addition, the creator of an object in Lab Management is automatically granted all permissions on that object. You can set these permissions by using the [TFSLabConfig permissions command-line tool](#).

By default, the project Readers groups have only View lab resources (Read) permissions.

NOTE

Lab Management is deprecated for TFS 2017. We recommend that you [use Build and Release Management instead of Lab Management for automated testing](#).

PERMISSION	DESCRIPTION
Delete Environment and Virtual Machines	Can delete environments and templates. The permission is checked for the object that is being deleted.
Delete Environment and Virtual Machines	Can delete environments and templates. The permission is checked for the object that is being deleted.
Delete Lab Locations	Can delete the locations for Lab Management resources, which include collection host groups, collection library shares, project host groups, and project library shares. To delete a location, you must have the Delete Lab Location permission for that location.
Edit Environment and Virtual Machines	Can edit environments and templates. The permission is checked for the object that is being edited.
Environment Operations	Can start, stop, pause, and manage snapshots, in addition to performing other operations on an environment.

Import Virtual Machine	Can import a virtual machine from a VMM library share. This permission differs from Write because it only creates an object in Lab Management and does not write anything to the Virtual Machine Manager host group or library share.
Manage Child Permissions	Can change the permissions of all the child Lab Management objects. For example, if a user has Manage Child Permission for a project host group, the user can change permissions for all the environments under that project host group.
Manage Lab Locations	Can edit the locations of Lab Management resources, which include collection host groups, collection library shares, project host groups, and project library shares. To edit a specific location, you must have the Manage Lab Location permission for that location. This permission for collection level locations (collection host groups and collection library shares) also allows you to create project level locations (project host group and project library share).
Manage Permissions	Can modify the permissions for a Lab Management object. This permission is checked for the object whose permissions are being modified.
Manage Snapshots	Can perform all snapshot management tasks for an environment, which include taking a snapshot, reverting to a snapshot, renaming a snapshot, deleting a snapshot, and reading a snapshot.
Pause Environment	Can pause an environment.
Start	Can start an environment.
Stop	Can stop an environment.
View Lab Resources	Can view information for the various Lab Management resources, which include collection host groups, project host groups, and environment. To view information about a specific lab resource, you must have the View Lab Resources permission for that resource.
Write Environment and Virtual Machines	Can create environments for a project host group. Users who have this permission for a project library share can store environments and templates.

Notifications or alerts

There are no UI permissions associated with [managing email notifications or alerts](#). Instead, they can be managed using the [TFS Security command line tool](#).

- By default, members of the project level **Contributors** group can subscribe to alerts for themselves.
- Members of the **Project Collection Administrators** group, or users who have the **Edit collection-level information** can set alerts in that collection for others or for a team.
- Members of the **Project Administrators** group, or users who have the **Edit project-level information** can set alerts in that project for others or for a team.

You can manage alert permissions using [TFS Security](#).

TFSSecurity Action	TFSSecurity Namespace	Description	Project Collection Administrators and Project Collection Service Accounts
CREATE_SOAP_SUBSCRIPTION	EventSubscription	Can create a SOAP-based web service subscription.	✓

TFSSecurity Action	TFSSecurity Namespace	Description	Project Collection Administrators and Project Collection Service Accounts
GENERIC_READ	EventSubscription	Can view subscription events defined for a project.	✓
GENERIC_WRITE	EventSubscription	Can create alerts for other users or for a team.	✓
UNSUBSCRIBE	EventSubscription	Can unsubscribe from an event subscription.	✓

Related articles

- [About permissions](#)
- [Add users to a project \(Azure DevOps\)](#)
- [Add users to a project \(TFS\)](#)
- [Add users to an administrator role](#)
- [Make a user a team admin](#)
- [Change groups and permissions with TFSSecurity](#)

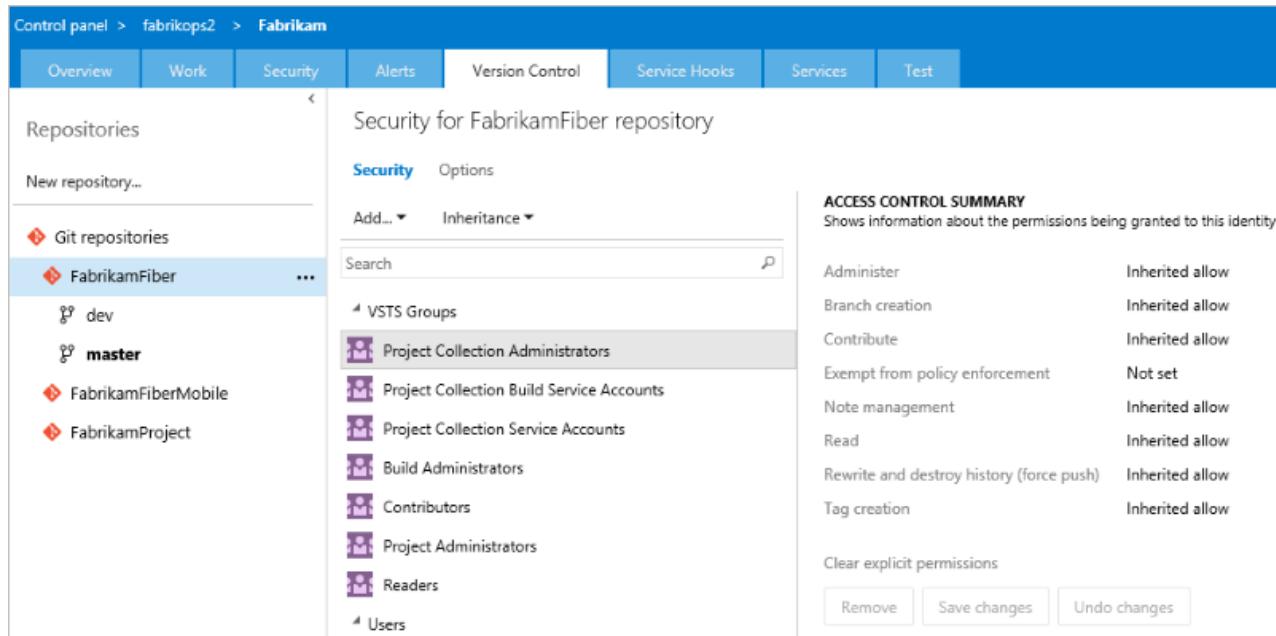
Git permissions prior to TFS 2017 Update 1

5/24/2019 • 2 minutes to read • [Edit Online](#)

[TFS 2017](#) | [TFS 2015](#) | [TFS 2013](#)

In TFS 2017 Update 1 (and Azure DevOps), Git repository permissions have changed. For those customers using previous versions of TFS, here are the old permissions. Those using TFS 2017 Update 1 or Azure DevOps should see the [latest list of permissions](#).

These permissions appear only for a project including a Git repository.



The screenshot shows the TFS Control Panel interface. The top navigation bar includes 'Control panel > fabrikops2 > Fabrikam'. Below this is a horizontal menu bar with tabs: Overview, Work, Security, Alerts, Version Control, Service Hooks, Services, and Test. The 'Version Control' tab is selected. On the left, there's a sidebar with 'Repositories' and a 'New repository...' button. Under 'Git repositories', 'FabrikamFiber' is selected. To its right are buttons for 'dev' and 'master'. Below these are 'FabrikamFiberMobile' and 'FabrikamProject'. The main content area is titled 'Security for FabrikamFiber repository'. It has tabs for 'Security' (which is selected) and 'Options'. Under 'Security', there are buttons for 'Add...' and 'Inheritance...'. A search bar is present. To the right, a section titled 'ACCESS CONTROL SUMMARY' displays a table of permissions:

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Administer	Inherited allow
Branch creation	Inherited allow
Contribute	Inherited allow
Exempt from policy enforcement	Not set
Note management	Inherited allow
Read	Inherited allow
Rewrite and destroy history (force push)	Inherited allow
Tag creation	Inherited allow

Below the table are buttons for 'Clear explicit permissions', 'Remove', 'Save changes', and 'Undo changes'.

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry.

Individual repositories inherit permissions from the top-level **Git Repositories** entry.

Branches inherit permissions from assignments made at the repository level.

By default, the project level Readers groups have only Read permissions.

PERMISSION	DESCRIPTION
Administer	<p>Can rename and delete the repository. If assigned to the top-level Git repositories entry, can add additional repositories.</p> <p>At the branch level, users can set permissions for the branch and unlock the branch.</p> <div style="border: 1px solid #ccc; padding: 5px;"><p>TFS 2013, TFS 2015: The Administer permission set on a individual Git repository does not grant the ability to rename or delete the repository. These tasks require Administer permissions at the top-level Git repositories entry.</p></div>
Branch Creation	<p>Can create and publish branches in the repository.</p> <p>Lack of this permission does not limit users from creating branches in their local repository; it merely prevents them from publishing local branches to the server.</p> <p>When a user creates a new branch on the server, they have Administer, Contribute, and Force permissions for that branch by default.</p>

Contribute	At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.
Note Management	Can push and edit Git notes to the repository. They can also remove notes from items if they have the Force permission.
Read	Can clone, fetch, pull, and explore the contents of the repository.
Rewrite and destroy history (force push)	Can force an update to a branch and delete a branch. A force update can overwrite commits added from any user. Users with this permission can modify the commit history of a branch.
Tag Creation	Can push tags to the repository, and can also edit or remove tags if they have the Force permission.

Data protection overview

5/7/2019 • 25 minutes to read • [Edit Online](#)

Azure DevOps Services

Azure DevOps Services is a cloud-hosted application for your development projects, from planning through deployment. Based on the capabilities of Team Foundation Server, with additional cloud services, Azure DevOps manages your source code, work items, builds, tests, and much more. Azure DevOps uses Azure's Platform as a Service infrastructure and many of Azure's services, including Azure SQL databases, to deliver a reliable, globally available service for your development projects. Because important data is at stake, this white paper discusses the steps that Microsoft takes to keep your projects safe, available, secure, and private. In addition, it describes the role you play in keeping your projects safe and secure.

This article is part of our effort to illuminate how we manage and protect your data and is intended for organization administrators and IT professionals who manage their project assets daily. It will be most useful to individuals who are already familiar with Azure DevOps and want to know more about how Microsoft protects the assets that are stored in Azure DevOps.

Our commitment

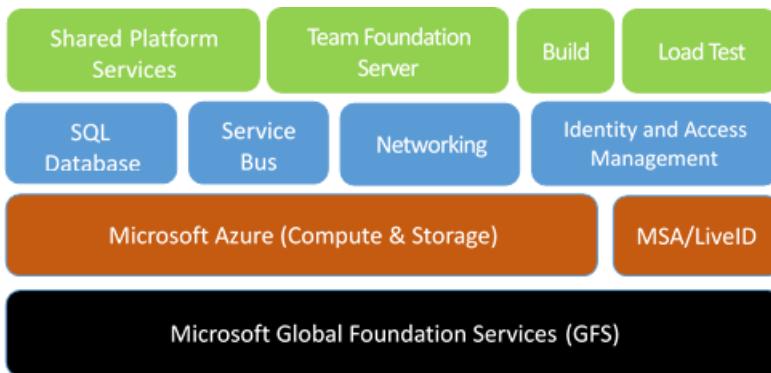
Microsoft is committed to ensuring that your projects remain safe and secure, without exception. When stored in Azure DevOps, your projects benefit from multiple layers of security and governance technologies, operational practices, and compliance policies. We enforce data privacy and integrity both at rest and in transit.

As we look at the broader landscape of threats facing Azure DevOps customers, they boil down to four basic categories: data availability, service availability, service security, and data privacy. We will investigate each of these categories to explore specific threats and explain what Azure DevOps does to address them through both the technology that we use and the way we put it into practice. However, we will first describe how data is stored and how Azure DevOps manages access to your data.

Because proper data protection also requires active engagement of customer administrators and users, we also discuss steps you should take to protect your project assets from unauthorized disclosure and tampering. Much of this has to do with being explicit about granting permissions to user access points in order to have confidence that only the right people are accessing data within Azure DevOps.

Regardless of your approach, you should consider all data potentially "at risk" no matter where it is or how it is being used; this is true for both data in the cloud as well as data stored in a private data center. Thus, it is important to classify your data, its sensitivity / risk horizon, and the damage it could do if it is compromised. You should also categorize your data relative to an overall information security management policy.

Built on Azure



Azure DevOps Services is hosted entirely in Azure data centers and uses many of the core Azure services including Compute, Storage, Networking, SQL Database, Identity and Access Management Services, and Service Bus. This lets us focus on the unique aspects of running Azure DevOps while taking advantage of the state-of-the-art capabilities, protection, and industry certifications available from the Azure platform.

Azure DevOps Services uses Azure Storage as the primary repository for service metadata and customer data. Depending on the type of data and the storage and retrieval needs, we use Azure Blob (binary large objects) storage and Azure SQL data storage. To provide a seamless experience, we work hard to abstract these details from the end user. However, to discuss the details surrounding Azure DevOps approach to data protection, some background in these elements is important.

Azure Blob storage is generally used to store large chunks of unstructured data. All projects use the Azure Blob storage service. This data includes potentially sensitive or private information such as the contents of source files and the attachments on work items. For most projects, the majority of storage in use is this type of unstructured blob storage. For more information, see documentation on [Azure Blob Storage](#).

Azure SQL database storage is used to store the structured and transactional aspects of your organization, including project metadata, the versioned source control history, and work item details. Database storage gives you fast access to the important elements of your project and provides indexes into the blob storage to look up files and attachments. For more information, see documentation on [Azure SQL Database](#).

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 Azure Active Directory](#) (Azure AD) and Microsoft Accounts (MSA, formerly LiveID). During authentication, the user is routed to the authentication provider (Azure AD or MSA) where they provide their credentials. Once the authentication provider has verified the user's credentials, Azure DevOps issues an authentication cookie to the user, which allows them 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 attempts to access, permissions are validated based on the user's explicit permissions as well as permissions inherited through group membership. Administrators can leverage access controls to protect [access to organization](#), project collection, team project, and team scoped data and functionality, as well as to more specific assets like version control folders and work item area paths.

Data availability

Azure DevOps Services leverages many of the Azure storage features to ensure data availability in the case of hardware failure, service disruption, or region disaster. Additionally, the Azure DevOps team follows procedures to protect data from accidental or malicious deletion.

Data redundancy

To protect data in the case of hardware or service failures, Microsoft Azure storage geo-replicates customer data between two locations within the same region that are hundreds of miles apart; for instance, between North and West Europe or between North and South United States (except Brazil). For Azure blobs, customer data is replicated three times within a single region and is replicated asynchronously to a second region hundreds of

miles away. As such, Azure always maintains the equivalent of six copies of your data. This enables us to failover to a separate region in the case of a major outage or disaster while also providing local redundancy for hardware failures within a region. For Azure SQL database storage, daily backups are maintained offsite in the case of a regional disaster.

NOTE

Note the following regarding data redundancy and fail over:

- There is an inherent delta measured in minutes when we replicate your data between the primary and secondary region
- Fail over to the secondary region is a decision that we must make centrally as it impacts all customers on the affected scale unit. Except in extreme circumstances, we'll opt to not fail over so that customer data is not lost
- Azure DevOps offers a 99.9% uptime SLA guarantee and will refund portion of the monthly charges if we miss the SLA in a specific month
- Because there is only one region in Brazil, customer data in Brazil is replicated to South Central US for disaster recovery purposes

Mistakes happen

To protect against accidental deletion of data, either by our customers or by our operation team, we also take point-in-time backups of both the Azure blob and the SQL databases. Our approach to these backups varies based on the storage type. For blobs, we have a separate copy of all blobs and regularly append new changes to each storage account. Since this data is immutable, we don't need to rewrite any existing storage as part of our backup procedures. SQL Azure, on the other hand, handles backups as a standard part of their service which we rely on. In both cases, these backups are also replicated in a paired region to ensure we can recover from a regional outage.

In addition, we perform a "soft delete" for organization deletion operations. This lets us recover entire organizations for up to 30 days after deletion.

Practice is critical

Having multiple, redundant backups of your data is good but without practice, restoring can be unpredictable. It's been said that "backups never fail, it's the restores that do". While technically incorrect, the sentiment is right. The good news is that we regularly practice restoring various data sets from backup. The geo-redundant storage that we get from Azure is tested regularly. In addition, from time to time we restore from backups to recover from human error, such as when a customer has inadvertently deleted a project in Azure DevOps. We have the capability of restoring your organization's data to any point in time over the last 30 days. While our turnaround time sometimes takes more than a day, we have always been able to restore the customer's data given enough time. Since there are many permutations of disaster and data corruption scenarios, we continue to plan and execute new tests on a regular basis to ensure our systems and associated process are up to the challenge.

Service availability

Ensuring that Azure DevOps Services is available for you to access your organization and associated assets is of utmost importance to us.

DDoS protections

In some cases, a malicious distributed denial-of-service (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 not only to withstand attacks from the outside but also from within Azure. For application-specific attacks that can penetrate the Azure defense systems, Azure DevOps establishes application and organization level quotas and throttling to prevent any overuse of key service resources during an attack or accidental misuse of resources.

Live site response

While we strive for the service to be available 100% of the time, sometimes things happen that prevent us from meeting that goal. If this happens, we provide transparency to our users throughout the incident. Our 24x7 operations team is always on hand to rapidly identify the issue and to engage the necessary development team resources. Those resources then address the problem. They also aim to update the service status page and blog within minutes of detecting an issue that affects the service. Once the team has addressed an issue, our "live-site incident" process continues as we identify the root cause of the issue and track the necessary changes to ensure we prevent similar issues in the future.

Azure DevOps live-site management processes are crafted to ensure a deep focus on service health and customer experience. Our processes minimize our time to detect, respond to, and mitigate impacting issues. Ownership for Live site is shared across all engineering disciplines, so there are continual improvements evolving out of direct experience. This means that monitoring, diagnostics, resiliency, and quality assurance processes are improved over time. Live-site management in Azure DevOps is broken into three distinct tracks, shown as follows:

Telemetry	Incident Management	Live-site Review
<ul style="list-style-type: none">▪ Alerts – Define health alerts for failure modes▪ Diagnostics – Deliver instrumentation data and operational reports▪ Troubleshooting Guides – Guidance for investigating an alert is defined by the feature and then refined by the Service Engineer.▪ Failure Mode Testing – The Service Delivery (SD) team performs failure testing to ensure alerts fire as expected▪ Onboarding – The Feature team works with their Service Engineer (SE) to onboard new alerts to the 24 x 7 team.	<ul style="list-style-type: none">▪ Detection – Product alerts detect health issues and start the Live Site Incident (LSI) process▪ Triage – The 24 x 7 team receives all critical alerts and confirms impact using TFS guidance▪ Escalation – Both Dev and Ops have individuals in an on-call rotation. SE is initial escalation path. The SE will call Dev as needed▪ Incident Management – A bridge is managed by the SE who engages Dev. and Partners to troubleshoot▪ Resolution – Communication and service restoration are actively driven until customer impact is eliminated	<ul style="list-style-type: none">▪ Goal – Weekly review of LSI ensures that leadership has visibility into live site health and repeat issues▪ Cadence – Incident from prior week have root cause documented then reviewed on weekly basis▪ Audience – VS Leadership. Partner team when they drive impact. Developer attends to provide details on Service incident▪ Ownership -Dev. owns reviews for App and Deploy issues. SD owns for Platform issues▪ Driving Improvements – Bugs and problem work items are logged for gaps (e.g. – missing alerts) and repeat root cause

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, we will even contact the customer directly to understand their experience and work with them to improve the service from their vantage point.

We understand that availability of our service is an integral part of your team's success. Because of this, we publish a service level agreement (SLA) and provide a financial guarantee to ensure we meet this agreement each month. For more specifics on our SLA and financial guarantees, please see [SLA for Azure DevOps](#).

Sometimes our partner teams or dependencies have incidents that affect Azure DevOps. All our partner teams follow similar approaches to identifying, resolving, and learning from these service outages.

Service security

Ensuring a secure service requires constant vigilance, from proper design and coding techniques, all the way through to the way we operate the service. Along those lines, we actively invest in the prevention of security holes and in breach detection. In the event of a breach, we use security response plans to minimize data leakage, loss or corruption. To learn more about how security and identity are managed, see [About security and identity](#).

Secure by design

To implement industry best practices and stay on the forefront of information security, we engage with various teams within Microsoft including Azure, Global Foundation Services (GFS), and Trustworthy Computing. Microsoft's Security Development Lifecycle (SDL) is at the core of our development process and Microsoft's

Operational Security Assurance (OSA) program guides our cloud operation procedures. The SDL and OSA methodologies address security threats throughout the development process and operation of Azure DevOps. They specify requirements that include threat modeling during service design, following design and code best practices, verifying security with standard tooling and testing, limiting access to operational and customer data, and gating rollout of new features through a rigid approval process.

Because the security landscape is continually changing, it is important for our team to keep current with the latest in best practices. We have annual training requirements for all engineers and operations personnel working on Azure DevOps. In addition, we sponsor informal "brownbag" meetings. These meetings are hosted by our own engineers. After they've solved an issue, they share what they've learned with the rest of the team.

A cloud service is only as secure as the host platform. Azure DevOps uses Azure's Platform as a Service (PaaS) offering for much of our infrastructure. PaaS automatically provides regular updates for known security vulnerabilities. When we host virtual machines in Azure using their Infrastructure as a Service (IaaS) offering, such as for our [hosted build service](#), we regularly update those images to include the latest security patches available from Windows Update. The same update rigor applies for our on-premises machines, including those used for deployment, monitoring, and reporting.

Our team conducts regular security-focused penetration testing of Azure DevOps. Using the same techniques and mechanisms as real malicious attackers, penetration testing tries to exploit the live production services and infrastructure of Azure DevOps. The goal is to identify real-world vulnerabilities, configurations errors or other security gaps in a controlled process. The team reviews the results to identify other areas of improvement and to increase the quality of the preventative systems and training.

Credential security

Your credentials in Azure DevOps are stored using industry best practices. Learn more about [credential storage](#).

Reporting security issues

If during your penetration testing you believe you have discovered a potential security flaw related to the Azure DevOps service, please report it to Microsoft within 24 hours by following the instructions on the [Report a Computer Security Vulnerability](#) page.

IMPORTANT

While notifying Microsoft of penetration testing activities is no longer required, customers must still comply with the [Microsoft Cloud Unified Penetration Testing Rules of Engagement](#).

Azure DevOps Bug Bounty Program

Azure DevOps participates in the [Microsoft Cloud Bounty Program](#) to reward security researchers who report issues to us, and to encourage more people to help us keep Azure DevOps secure. Please visit the [Azure DevOps Bounty Program](#) page for more details.

Restricting access

We maintain strict control over who has access to our production environment and customer data. Access is only granted at the level of least privilege required and only after proper justifications are provided and verified. If a team member needs access to resolve an urgent issue 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. Access requests and approvals are tracked and monitored in a separate system. All access to the system is correlated against these approvals and if unapproved access is detected, an alert is raised for the operations team to investigate.

If the username and password for one of our developers or operation staff were ever stolen, data is still protected because we use two-factor authentication for all remote system access. This means that additional authentication checks via smart card or a phone call to a pre-approved number must take place before any

remote access to the service is permitted.

In addition, secrets that we use to manage and maintain the service, such as RDP passwords, SSL certificates, and encryption keys are managed, stored, and transmitted securely through the Azure Management Portal. Any access to these secrets requires specific permission, which is logged and recorded in a secure manner. All secrets are rotated on a regular cadence and can be rotated on-demand in the case of 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 and all access is monitored and securely logged. To isolate the service from outside tampering, applications such as Outlook and Office, which are often targets of spear-phishing and other types of attacks, are not permitted in this environment.

Intrusion protection & response

To ensure data is not intercepted or modified while in transit between you and Azure DevOps, we encrypt via HTTPS / SSL.

In addition, data we store on your behalf in Azure DevOps is encrypted as follows:

- For data stored in Azure SQL databases, Azure DevOps adopted [Transparent Data Encryption \(TDE\)](#) to protect against the threat of malicious activity by performing real-time encryption of the database, associated backups, and transaction log files at rest.
- Azure Blob Storage connections are encrypted to protect your data in transit. To protect data at rest stored in our Azure Blob Storage, we have adopted [Azure Storage Service Encryption \(SSE\)](#).

To learn more about how we encrypt your data, please visit the following [blog post](#).

To ensure that activities within the service are legitimate, as well as to detect breaches or attempted breaches, we leverage Azure's infrastructure to log and monitor key aspects of the service. In addition, all deployment and administrator activities are securely logged, as is operator access to production storage. Real-time alerts are raised because the log information is automatically analyzed to uncover potentially malicious or unauthorized behavior.

In the case where a possible intrusion has been detected or high priority security vulnerability has been identified, we have a clear security incident response plan. This plan outlines responsible parties, steps required to secure customer data, and how to engage with security experts in Microsoft Security Response Center (MSRC), Global Foundation Services (GFS), Azure and members of the Azure DevOps leadership team. We will also notify any organization owners if we believe their data was disclosed or corrupted so that they can take appropriate steps to remedy the situation.

Finally, to help combat emerging threats, we employ an Assume Breach strategy. A highly specialized group of security experts within Microsoft, known as the Red Team, assumes the role of sophisticated adversaries. This team tests our breach detection and response, enabling us to accurately measure our readiness and the impacts of real-world attacks. This strategy strengthens threat detection, response, and defense of the service. It also allows us to validate and improve the effectiveness of our entire security program.

Data privacy

We want you to have confidence that your data is being handled appropriately and for legitimate uses. Part of that assurance involves appropriately restricting usage so that your data is used only for legitimate reasons.

The General Data Protection Regulation (GDPR)

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. The GDPR's main objective is to strengthen the protection and security of your personal data and replaced the Directive and all

local laws relating to it. Azure DevOps is relied upon as a system of record with strict integrity, traceability, and audit rules. We view all information within Azure DevOps to be business critical and therefore cannot be modified from its original state. These existing obligations affect our delete and retention obligations for GDPR. As such, we do not support GDPR delete requests from within Azure DevOps. We have ensured that when an entire organization is deleted that all associated data and telemetry about that organization and its members are removed from our system (after the requisite 30-day soft-delete period).

To learn more about how Azure DevOps honors Data Subject Requests (DSR), please visit the following [page](#). To learn more about the GDPR regulation, please visit the following page in [Microsoft's Trust Center](#).

Data residency and sovereignty

We know our customers care deeply about data security and privacy. Azure DevOps is available in the following 8 geographies across the world: United States, Canada, Europe, UK, India, Australia, Asia Pacific, and Brazil. While we default your organization to your closest region, you have the option to choose a different region. If you change your mind later, our CSS team can help you migrate your organization to a different region. Azure DevOps will not move or replicate customer data outside of the chosen geography. Our backup procedures geo-replicate customer data between a second region within the same geography except for organizations located in Brazil, these are replicated to South Central US for disaster recovery purposes.

To learn more about data location, see [Azure DevOps data location](#).

Law enforcement access

In some cases, third parties such as law enforcement entities may approach us to obtain access to customer data stored within Azure DevOps. By policy, we will attempt to redirect the requests to the organization owner for resolution. When we are compelled by court order to disclose customer data to a third party, we will make a reasonable effort to notify the organization owner in advance unless we are legally prohibited from doing so.

Some customers require that their data be stored in a particular geographic location to ensure a specific legal jurisdiction for any law enforcement activities. At this time, Azure DevOps can host organizations in 8 geographies across the world: United States, Canada, Europe, UK, India, Australia, Asia Pacific, and Brazil. All customer data such as source code, work items, test results as well as the geo-redundant mirrors and offsite backups are maintained within the selected geography.

Microsoft access

From time to time, Microsoft employees need to obtain access to customer data stored within Azure DevOps. As a precaution, all employees who have or may ever have access to customer data must pass a background check, which verifies previous employment and criminal convictions. In addition, 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.

Since not all data within our system is treated the same, data is classified to distinguish between customer data (what you upload to Azure DevOps), organization data (information used when signing up for or administering your organization), and Microsoft data (information required for or collected through the operation of the service). Based on the classification we control usage scenarios, geolocation requirements, access restrictions and retention requirements.

Microsoft promotional use

From time to time, we want to contact customers to let them know about additional features and services that might be useful. Since not all customers want to be contacted about these offers, we allow you to opt-in and opt-out of marketing email communications. We never use customer data to target specific offers for specific users or organizations. Instead, we leverage organization data and aggregate usage statistics at the organization level to determine groups of organizations that should receive specific offers.

Building confidence

In addition to these protections, we have also taken steps outside of the service itself to help you decide to move forward with Azure DevOps. These include Microsoft's own internal adoption policies, the level of transparency that we provide into the state of our service, and our progress towards receiving certification of our information security management systems. All these efforts are designed to build your confidence in Azure DevOps.

Internal adoption

Teams across Microsoft have begun adopting Azure DevOps internally. The Azure DevOps team moved into an organization in 2014 and uses it extensively. More broadly, we have established guidelines to enable the adoption plans for other teams. Obviously, large teams move more gradually than smaller ones, given their investments in existing DevOps systems. For teams able to move quickly, we have established a project classification approach. It assesses our 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. Additional requirements for internal projects include associating the organization with the Microsoft.com Azure Active Directory to ensure proper user identity lifecycle and password complexity along with requiring the use of two-factor authentication for more sensitive projects.

Transparency

We are convinced that transparency around how we design and operate our service is critical to establishing trust with our customers. This white paper is part of our effort to shed light on how we manage and protect your data. In addition, we maintain a [blog](#) that provides real-time updates whenever a service disruption, planned or unplanned, takes place so you can adjust your activities as needed. Furthermore, Brian Harry, the corporate vice-president in charge of Azure DevOps, maintains an active [blog](#) addressing, among other things, lessons learned by operating the service.

Compliance certifications

For some customers, it is important to understand third-party evaluation of our data security procedures. Towards that end, we have achieved ISO 27001:2013, HIPAA (Health Insurance Portability and Accountability Act) BAA (Business Associate Agreement), EU Model Clauses, SOC 1 Type 2 and SOC 2 Type 2 certifications. The SOC audit for Azure DevOps covers controls for data security, availability, processing integrity, and confidentiality. Azure DevOps' SOC reports are available via the [Microsoft's Service Trust Portal](#). If you don't have access to Microsoft's Service Trust Portal, you can contact [Azure DevOps ServicesSOCReports] (<mailto:Azure DevOps ServicesSOCReports@microsoft.com>) to request a copy of Azure DevOps' SOC Reports.

Steps you can take

Proper data protection requires active engagement of customer administrators and users. Your project data stored within Azure DevOps is only as secure as the end user access points. So, it is important to match the level of permission strictness and granularity for those organizations with the level of sensitivity of your project.

Classify your data

The first step is to classify your data based on its sensitivity / risk horizon, and the damage that could occur if it is compromised. Many enterprises have existing classification methods that can be reused when projects move to Azure DevOps. Refer to these [materials](#) for more information on how to classify your data.

Adopt Azure Active Directory

Another action you can take to improve the security of your end users' credentials is to use Azure Active Directory (Azure AD) instead of Microsoft Accounts (MSA) to manage your organization's access to Azure DevOps. This allows your IT department to manage its end user access policy including password complexity, password refreshes and expiration if the user leaves your organization. Through Active Directory federation, you can directly link Azure Active Directory to your organization's central directory, so you have only one location to manage these details for your enterprise. See the following brief comparison between MSA and

Azure AD characteristics relative to Azure DevOps access:

Properties	MSA	Azure AD
Identity creator	User	Organization
Single user name / password for all work assets	No	Yes
Password lifetime & complexity control	User	Organization
Azure DevOps membership limits	Any MSA	Organization's directory
Traceable identity	No	Yes
Organization & IP ownership	Unclear	Organization
2-factor authentication enrollment	User	Organization
Device-based conditional access	No	Organization

You can learn more about how to [configure this support for your organization](#).

Require two-factor authentication

In some cases, you might want to restrict access to your organization by requiring more than one factor to sign in. Azure AD lets you require multiple factors, such as phone authentication in addition to a username and password, for all authentication requests. You can [learn more](#) about turning on multifactor authentication for Azure AD.

Use BitLocker

For sensitive projects, we also recommend use of BitLocker on your Windows laptop or desktop computer. BitLocker encrypts the entire drive on which Windows and your data reside, keeping everything safe. Once BitLocker is enabled, it automatically encrypts any file you save on that drive. If your laptop or desktop machine were to fall 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 referred to as Basic Authentication). This mechanism allows the end user to set up an alternate username and password for use during Git command line operations. This username and password combination can also be used 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. However, we have taken steps to help you make secure choices. For example, all communication is sent over HTTPS and there are password complexity requirements. Nevertheless, your organization should evaluate if additional policies are required to meet your project security requirements. You can [learn more](#) about disabling alternate authentication credentials altogether for your organization if it doesn't meet your security requirements.

Secure access to your organization

Azure Active Directory (Azure AD) provides the capability for administrators to control access to Azure resources and applications such as Azure DevOps. With conditional access control in place, Azure AD checks for the specific conditions you set for a user to access an application. After access requirements are met, the user is authenticated and can access the application. Visit the [Azure documentation site](#) to learn more about conditional access policy (CAP). Azure DevOps now enforces conditional access policies for custom Azure DevOps authentication mechanisms including personal access tokens (PATs), alternate authentication, OAuth and SSH

keys. If accessing Azure DevOps through a third party client, like git.exe, only IP based policies will be honored; any other policy will automatically fail as the client doesn't pass the necessary information to validate the policy. For example, if a policy requires MFA and the client can't support MFA, the policy will fail and the user will automatically be blocked.

Additional resources

In addition to this white paper, there are other resources available for your review and education. These include:

- [Azure DevOps home page](#)
- [Azure DevOps status](#)
- [Azure DevOps credential storage](#)
- [Azure DevOps data location](#)
- [Developer Services privacy statement](#)
- [Azure DevOps support](#)
- [Developer Services Agreement](#)
- [Azure trust center](#)
- [Microsoft Security Development Lifecycle](#)
- [Create and revoke your PATs](#)
- [Revoke user PATs - for admins](#)
- [Token expiration](#)

(c) 2018 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Data locations for Azure DevOps

4/2/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

Azure DevOps operates in the geographical locations ("geos") listed below. To determine where customer data is stored, you can choose the location of the organization during initial sign up and creation of the organization.

Data locations

Your data is stored within the following locations:

- Australia
- Brazil
- Canada
- East Asia
- Europe
- India
- United Kingdom
- United States

Azure DevOps stores information that is global in nature, such as user identities and profile information, in a data center located in the United States. All customer data, such as source code, work items, and test results, as well as the geo-redundant mirrors and offsite backups, are maintained within the selected geography.

NOTE

Because there is only one region in Brazil, customer data is replicated to south-central United States for disaster recovery and load balancing purposes. For more information, see the [Azure data center map](#).

For builds and releases configured to run on Microsoft-provided macOS agents, Azure DevOps stores associated customer data in the United States in a data center that is owned and managed by a third party with reduced information security certification assurances.

Azure DevOps works with and uses many Microsoft Azure services. For details on customer data retention by location, see the [Azure data center map](#).

Transferring your data

Microsoft does not transfer customer data outside the selected region, except when it is necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements. In such a case, you configure an organization to enable such transfer of your data using preview, beta, or other pre-release services, which typically store your data in the United States, but may store it globally.

NOTE

Microsoft does not control or limit the regions from which you or your users may access your data.

Related articles

- [Get started with Azure DevOps](#)
- [Data protection overview](#)

How we store your credentials for Azure DevOps Services

3/21/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

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](#).

Alternate credentials (basic auth)

- We store two values, a 16-byte password salt and a 32-byte password hash
- Raw password is provided directly by the caller over SSL
- Password salt is randomly generated in-memory on the server side using RNGCryptoServiceProvider each time a password is created or changed
- Password hash is generated in-memory on the server side from the raw password and password salt bytes using Rfc2898DeriveBytes with 1000 iterations
- Salt and hash are stored in a database

Personal access tokens (PATs)

- We store a hash of the PAT
- Raw PAT is generated in-memory on the server side as 32 bytes randomly generated through RNGCryptoServiceProvider then shared with the caller as a base-32-encoded string. This value is NOT stored.
- PAT hash is generated 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 is stored in our database

Secure shell (SSH) keys

- We store a hash of the enclosing organization ID and the SSH public key
- Raw public key is provided directly by the caller over SSL
- SSH hash is generated 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 is stored in our database

OAuth credentials (JWTs)

- These are issued as fully self-describing JSON web tokens (JWTs) and are NOT stored in our service
- The claims in JWTs issued and presented to our service are validated using a certificate stored in our key vault

Add IP addresses and URLs to allow list

7/1/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services

If you or your organization uses security measures, such as a firewall or a proxy server, there are IP addresses and domain URLs that you might want to add to the Allow list. Adding them to the Allow list helps to ensure that you have the best experiences with Azure DevOps.

The endpoint data in the following chart, lists requirements for connectivity from a user's machine to Azure DevOps. It doesn't include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections.

Azure DevOps IP addresses

Ensure the following IP addresses are allowed, so your organization works with any existing firewall or IP restrictions.

IP V4 RANGES	IP V6 RANGES
13.107.6.0/24	2620:1ec:4::/48
13.107.9.0/24	2620:1ec:a92::/48
13.107.42.0/24	2620:1ec:21::/48
13.107.43.0/24	2620:1ec:22::/48

Azure DevOps domains

For domain-based firewalls, ensure the following domains are allowed:

DOMAINS
- dev.azure.com/*
- *.dev.azure.com

Incoming IP addresses

Azure DevOps' incoming traffic hits the service through IP addresses and domains used by Microsoft Azure datacenters or third party providers.

1. To get the list of Azure IP ranges and Service Tags for Public Cloud, see [Azure IP ranges and Service Tags - Public Cloud](#). This link provides the IP address ranges for global Azure as a whole, each Azure region within Public Cloud, and ranges for several Azure Services (Service Tags) such as Storage, SQL, and Azure Traffic Manager in Public Cloud.
2. Azure DevOps leverages Content Delivery Networks (CDNs) to serve static content. Ensure the following CDNs are allowed.

- *.vsassets.io
- *.vsassetcdn.azure.cn
- *.gallerycdn.vsassets.io (Marketplace)
- *.gallerycdn.azure.cn (Marketplace)

We recommend you open port 443 to all traffic on these IP addresses and domains. We also recommend you open port 22 to a smaller subset of targeted IP addresses.

Azure DevOps ExpressRoute connections

If your organization uses ExpressRoute, ensure the following addresses are allowed.

IP V4 RANGES	IP V6 RANGES
13.107.6.175/32	2620:1eca92::175/128
13.107.6.176/32	2620:1eca92::176/128
13.107.6.183/32	2620:1eca92::183/128
13.107.9.175/32	2620:1ec:4::175/128
13.107.9.176/32	2620:1ec:4::176/128
13.107.9.183/32	2620:1ec:4::183/128
13.107.42.18/32	2620:1ec:21::18/128
13.107.42.19/32	2620:1ec:21::19/128
13.107.42.20/32	2620:1ec:21::20/128
13.107.43.18/32	2620:1ec:22::18/128
13.107.43.19/32	2620:1ec:22::19/128
13.107.43.20/32	2620:1ec:22::20/128

For more information about Azure DevOps and ExpressRoute, see [ExpressRoute for Azure DevOps](#).

Connecting Private Build Agents

If you're running a firewall and your code is in Azure Repos, see [Self-hosted Windows agents FAQ](#). This article has information about which URLs and IP addresses your private agent needs to communicate with.

Azure DevOps Import Service

During the import process, we highly recommend that you restrict access to your VM to only IPs from Azure DevOps. To restrict access, only allow connections from the set of Azure DevOps IPs involved in the collection database import process. For information about identifying the correct IPs, see [Azure DevOps Services IPs](#).

Other scenarios

Visual Studio and Azure Services

If you or your organization use security measures, like a firewall or a proxy server, add domain URLs to the Allow list. Open ports and protocols also, for the best experience with Visual Studio and Azure Services. For more information, see [Use Visual Studio and Azure Services - Install and use Visual Studio behind a firewall or proxy server](#).

Other important URLs to consider

List of URLs for sign in and licensing connections

- <https://management.core.windows.net>
- <https://login.microsoftonline.com>
- <https://login.live.com>
- <https://go.microsoft.com>
- <https://graph.windows.net>
- <https://app.vssps.visualstudio.com>

A more general list of URLs for signing into Azure DevOps and Azure

- <https://windows.net>
- <https://microsoftonline.com>
- <https://visualstudio.com>
- <https://microsoft.com>
- <https://live.com>
- <https://management.core.windows.net>
- <https://dev.azure.com>
- <https://aex.dev.azure.com>
- <https://static2.sharepointonline.com> -- hosts some resources that we use in "office fabric" UI kit (fonts, and so on)

NuGet connections

- <https://azurewebsites.net>
- <https://nuget.org>

Security glossary

3/21/2019 • 3 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

The Microsoft Security glossary is a short dictionary of terms used in authenticating users and managing permissions on the Azure DevOps Services and Team Foundation Server platforms.

Access level

Access levels correspond to a licensing level to provide access to certain features. Access to these features is managed by membership to an access level. To learn more, see [About access levels](#).

Authentication

Authentication verifies a user's identify based on the credentials provided when they sign into an organization in Azure DevOps. These services/servers typically integrate with and rely upon the security features provided by additional services such as Active Directory or Azure Active Directory. To learn more, see [About security and identity](#).

Authorization

Authorization refers to the operations performed to verify that the identity which is attempting to connect to a service or server instance has the necessary permissions to access a service, feature, function, object, or method. To learn more, see [About security and identity](#).

Basic member

A user account that has been granted membership to an organization in Azure DevOps instance with Basic access. To learn more, see [About access levels](#).

Collections

A collection is a container for a number of projects in Azure DevOps. A default collection is created when you sign up with Azure DevOps Services or install Team Foundation Server. Within Azure DevOps Services, a collection corresponds to an organization. For on-premises TFS deployments, you can add and manage collections to specify the logical and physical resources available to the projects within the collection.

Learn more: [About projects and scaling your organization](#), [Manage organizations](#) or [Manage project collections in Team Foundation Server](#).

Conditional access

Conditional access provides support for securing Azure DevOps resources backed by an Azure Active Directory (Azure AD) tenant. For example, you can enable multi-factor authentication to help protect against the risk of compromised credentials. To learn more, see [Manage conditional access to Azure DevOps](#).

Inheritance

Permissions that aren't directly allowed or denied for a user, may be inherited. To learn more, see [About permissions and groups](#).

Permission

The assignment made to a user or group to use a feature or function. Permissions are assigned to default security groups. To learn more, see [About permissions and groups](#).

Security group

A method by which you can organize users and other domain objects to simplify administration of permissions and access. Azure DevOps support a number of default security groups as well as the ability to create custom groups. To learn more, see [About permissions and groups](#).

Security role

A security model that limits actions based on membership within a role. To learn more, see [About security roles](#).

Service account

An account used to monitor or manage select services, such as build or test services.

Secure Sockets Layer (SSL)

SSL is a protocol used to strengthen the security of cloud-hosted and on-premises applications by configuring it to use Hypertext Transfer Protocol Secure (HTTPS) with Secure Sockets Layer (SSL).

SSL is always used to protect Azure DevOps data. To learn more, see [Data Protection Overview](#).

For on-premises deployments, SSL is optional. To learn more, see [Setting up HTTPS with Secure Sockets Layer \(SSL\) for Team Foundation Server](#).

Stakeholder

A user account that has been granted membership to an organization in an Azure DevOps instance with Stakeholder access. With Stakeholder access, you can add and modify work items, check project status, manage pipelines, and view and manage dashboards. To learn more, see [Get started as a Stakeholder](#).

Team group

A security group that is defined when a team is created and automatically populated with members as they are added to the team.

Tenant

An Azure Active Directory used to manage access or billing. To learn more, see [Change Azure AD tenant](#)

Valid users

Valid users are users that are recognized by Azure DevOps as being able to connect to the account or a project. When you add accounts of users directly to a built-in group or through a Windows, Active Directory, or Azure Active Directory group, they are automatically added to one of the valid user groups. To learn more, see [About permissions and groups](#).

Notifications

3/21/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

Stay up-to-date with changes as they occur by subscribing to events such as code changes, build completions, or work item assignments.

Overview

- [About notifications](#)
- [Navigation in the notifications UI](#)

Step-by-step tutorials

- [Follow work & pull requests](#)
- [Set your personal notifications](#)
- [Manage team and group notifications](#)

Concepts

- [Events and notifications](#)
- [How email recipients of notifications are determined](#)

How-to guides

- [Manage organization subscriptions](#)
- [Manage organization default delivery settings](#)
- [View notification statistics for your organization](#)
- [Change your preferred email address, used for notifications](#)
- [Use subscription logging for troubleshooting](#)
- [Exclude yourself from notifications of events initiated by you](#)
- [Follow work and pull requests](#)
- [Use @mentions to further discussion](#)
- [Use #ID to link to work items](#)
- [Send notifications to third-party services](#)
- [Get notified with Campfire](#)
- [Get notified with Slack](#)

Reference

- [Default and supported notifications](#)
- [Supported event types](#)
- [FAQs](#)
- [Default permissions and access set for collaboration tools](#)
- [Azure DevOps data protection overview](#)

Resources

- [Git](#)
- [Work items](#)
- [Service Hooks](#)
- [REST API](#)
- [Microsoft Teams Integration](#)

About notifications

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

Notifications help you and your team stay informed about activity that occurs within your Azure DevOps projects. With notifications, you are notified when changes occur to work items, code reviews, pull requests, source control files, and builds. You can be notified via email. For example, you can get notified whenever a bug that you opened is resolved or when a work item is assigned to you.

You receive notifications based on rules or subscriptions. Subscriptions arise from the following instances:

- Out of the box or default
- Created by an administrator for a team or group that you belong to
- Created by you

You can manage your notifications, which you access from your organization menu. Other notifications are managed by an administrator at the following levels:

- Team notifications, managed by a team administrator
- Project notifications, managed by a member of the Project Administrators group
- Organization/collection-level notifications, managed by a member of the Project Collection Administrators group

Preferred email address

Notifications are sent by default to the preferred email address for your organization profile. This is typically the email address you signed into Azure DevOps with, but can be managed via your organization preferences profile page.

NOTE

Your preferred email address applies across all of your organizations and cannot be changed on a per-organization basis.

Integrating with other services

If your team uses an external service to collaborate—such as Campfire, Flowdock, or Slack—you can configure notifications to be sent to these services. These services are supported out of the box:

- [Campfire](#)
- [Flowdock](#)
- [Hipchat](#)
- [Slack](#)
- [Microsoft Teams](#)

You can also use a third-party service like Zapier to send notifications to hundreds of other services. Learn more about [Zapier and Azure DevOps Services integration](#).

On-premises SMTP server

For on-premises Azure DevOps, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Navigating the notifications UI

3/12/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Learn about navigating the notifications user interface.

The notifications pages

There are the following notifications pages:

- Personal
- Team
- Project
- Organization or collection (organization for the cloud and project collection for on-premises)

Permissions to manage notifications at each page default are as follows:

- Organization administrators can manage notifications
- Organization and team administrators can manage team notifications
- Each user can manage their personal notifications

Navigating to the organization-level notifications page

Select the Notifications page under organization settings.

Personal:

```
https://dev.azure.com/{organization}/_notifications
```

Team:

```
https://dev.azure.com/{organization}/{project}/{team}/_admin/_notifications
```

Project:

```
https://dev.azure.com/{organization}/{project}/_admin/_notifications
```

Organization:

```
https://dev.azure.com/{organization}/_admin/_notifications
```

The screenshot shows the Azure DevOps Organization Settings page. On the left, there's a sidebar with 'My organizations' (listing 1esSharedAssets, cloudbuild, codesharing-demo, and codesharing-SU0), 'Related pages' (What's new in DevOps, Documentation, Get help), and a 'New organization' button. A red box highlights the 'Organization settings' button. The main area has a vertical navigation bar on the right with 'General', 'Overview', 'Projects', 'Policy', 'Users', 'Security', 'Notifications' (which is selected and highlighted with a red box), 'Extensions', 'Usage', 'Boards', 'Process', and 'Pipelines'. The 'Notifications' section shows 'Default subscriptions' (with 'Description' and 'Build' items) and a list of notifications like 'Build completes', 'Code (Git)', 'Pull request review', 'Pull request complete', and 'Pull request changes'.

The screenshot shows the Azure DevOps Project Settings page for 'fabrikam-fiber'. The top navigation bar includes 'Search work items in this collection', a user profile, and a '...' button. Below it, there are links for 'Projects', 'My favorites', 'My work items', 'My pull requests', and a gear icon. A red box highlights the project name 'fabrikam-fiber'. The main content area has a 'Projects' section with 'Recent' items (Fabrikam-Fiber, FabrikamFiber, FabrikamFiberWeb, New project, FabrikamProject) and an 'All' section (Fabrikam-Fiber). To the right is a sidebar with 'Projects', 'Settings', 'Policy', 'Process', 'Users', 'Security', 'Build and release', 'Agent Pools', 'Deployment Pools', 'OAuth Configurations', 'Notifications' (highlighted with a red box), 'Extensions', and 'Usage'. A 'New Project' button is also present.

The screenshot shows the Azure DevOps Project Settings page for 'fabrikam-fiber', specifically focusing on the 'Notifications' tab. The top navigation bar includes 'Search work items in this collection', a user profile, and a '...' button. Below it, there are links for 'Projects', 'My favorites', '...', and a gear icon. A red box highlights the project name 'fabrikam-fiber'. The main content area has a 'Notifications' section with 'Default subscriptions', 'Subscribers', 'Statistics', 'Settings', and a 'Help' link. The 'Notifications' tab is active.

Navigating to the team level notifications page

Select the Notifications page under project settings.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber Web' project. The left sidebar has 'Project settings' highlighted with a red box. The main content area shows the 'Notifications' section under 'FabrikamFiber Web Team'. A red box highlights the 'Notifications' link in the left navigation menu. The right side displays various notification rules, such as 'Build completes' and 'Pull request changes'.

The screenshot shows the Visual Studio Team Services interface for the 'FabrikamFiber Team'. The top navigation bar has 'Notifications' highlighted with a red box. The main content area shows the 'Notifications' section under 'FabrikamFiber Team'. A red box highlights the 'Notifications' link in the left navigation menu. The right side displays 'Team Members' and 'Work' sections.

The screenshot shows the Visual Studio Team Services interface for the 'FabrikamFiber Team'. The top navigation bar has 'Notifications' highlighted with a red box. The main content area shows the 'Notifications' section under 'FabrikamFiber Team'. A red box highlights the 'Notifications' link in the left navigation menu. The right side displays 'New subscription', 'Delivery settings', and 'Help' options.

Navigating to the personal notifications page

Select the Notifications page under your profile.

The screenshot shows the Azure DevOps interface for the 'FabrikamFiber Web' project. The left sidebar has 'Work Items' highlighted with a red box. The top right corner shows a user profile icon with a red box. The main content area shows the 'Work Items' section. A red box highlights the 'Notification settings' link in the bottom right corner of the page.

Azure DevOps

My organizations

- 1 esSharedAssets
- C cloudbuild
- C codesharing-demo

User settings

General

Notifications

Usage

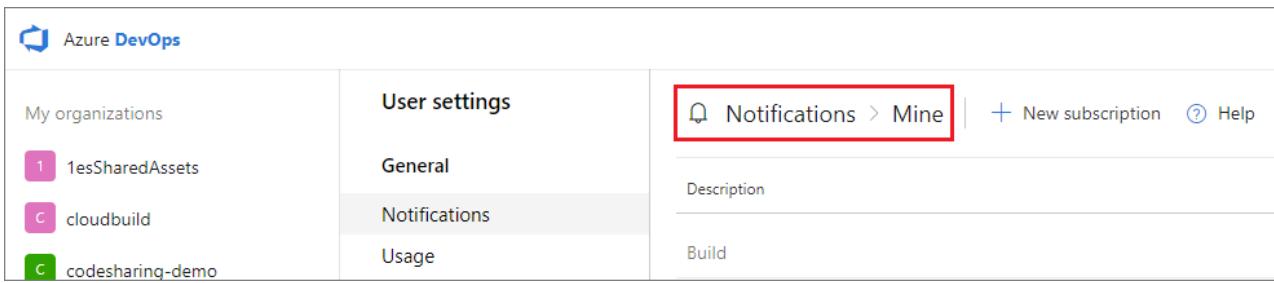
Notifications > Mine

+ New subscription

? Help

Description

Build



FabrikamFiber / Fabrika... Dashboards Code Work ... Search work items in this project

FabrikamFiber Team Overview Edit Refresh

Welcome

Get started using Visual Studio Team Services to make the most of your team dashboard.

Manage Work Add work to your board

Collaborate on code Add code to your repository

Work assigned to Jamal Hartnett (2)

2 Bug

ID	State	Title
3	● Commit...	🐞 ReadMe.txt missing from project
2	● Approved	🐞 Some bug work item here

Notification settings

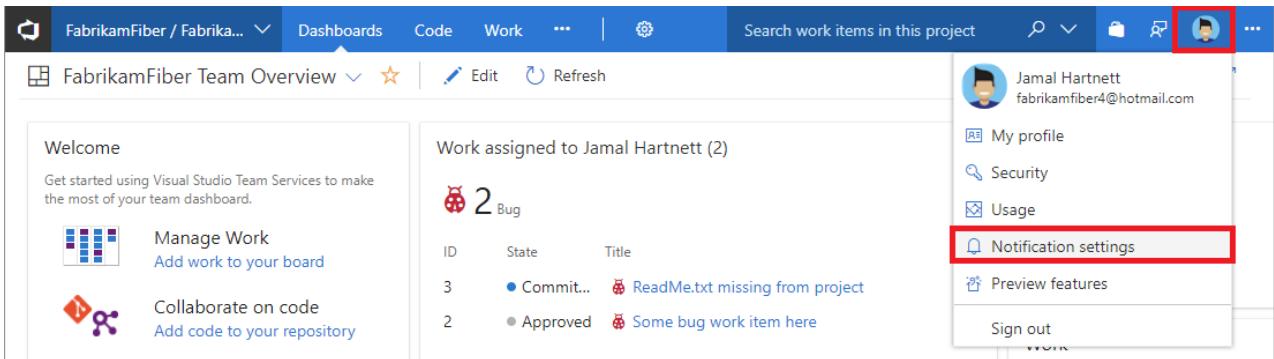
My profile

Security

Usage

Preview features

Sign out



Events, subscriptions, and notifications

3/5/2019 • 2 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) for team members to see the Notifications option from their organization menu and to receive notifications.

Events

Events are raised when certain actions occur, like when a work item is created or a pull request is voted on. See the list of [supported event types](#).

Subscriptions

A notification **subscription** is associated with a [supported event type](#) and includes a set of filters which are used to match events with the subscription. For example, a subscription for a *work item created* event might include a filter which matches only the work item type: *Bug*, or a subscription for a *pull request created* event might include a filter for a specific *repository and branch*.

Default email subscriptions

Many useful email subscriptions are pre-defined and enabled by default in the system. These are known as **default subscriptions**. Default subscriptions are intended to provide out-of-box support for the most common notification scenarios. See the list of [available default subscriptions](#).

An organization or team administrator can choose which of the default subscriptions to make available to their users. Learn how to [manage team notifications](#) or [manage organization level notifications](#).

Individual users can choose to opt out of any default subscription while other team members continue to be subscribed. Learn how to [manage personal notification subscriptions](#).

Custom email subscriptions

Custom email subscriptions can be created by organization or team administrators which apply to all members of the organization or team. Learn how to [manage team notifications](#) or [manage organization notifications](#).

Individuals can also create custom subscriptions which apply only to them. Learn how to [manage personal subscriptions](#).

Custom service hook subscriptions

Service hooks subscriptions can be used to integrate with third party services. When an Azure DevOps Services event matches a service hook subscription, a notification is delivered to the third party service. For example, when an Azure DevOps Services build completes, a notification can be delivered to a Slack channel with links back to the build artifact in Azure DevOps Services. To learn more, see [Integrating with third party services](#).

Notifications

When an **event** occurs in Azure DevOps Services or TFS, its content is compared with every **subscription** of that event type. If the subscription's filter conditions are met by the event, a notification is generated. **A notification is**

generated for every subscription/event match.

Each notification is then delivered based on the delivery properties defined in the subscription (either as an email or as a service hook). [Learn more about email delivery options](#).

How email recipients of notifications are determined

3/5/2019 • 6 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Who receives an email notification when an event matches a subscription involves a number of factors. Not understanding these factors can result in your inbox receiving too many (or too few) emails. The following explains how the type of subscription, its delivery settings, delivery preferences, and other factors determine the set of recipients.

Recipients for custom personal subscriptions

The recipients for a custom personal subscription is the easiest to understand: emails are delivered to the *preferred email address* of the user that owns the subscription or to the email address configured on the subscription.

Preferred email address on a personal subscription (the default)

The screenshot shows the 'New subscription' dialog. It has fields for 'Description' (containing 'A work item I created is changed'), 'Subscriber' (containing 'Jamal Hartnett'), 'Deliver to' (set to 'Preferred email'), and 'Address' (containing 'fabrikamfiber4@hotmail.com'). The 'Deliver to' and 'Address' fields are highlighted with a red border.

Custom email address on a personal subscription

The screenshot shows the 'New subscription' dialog. It has fields for 'Description' (containing 'A work item I created is changed'), 'Subscriber' (containing 'Jamal Hartnett'), 'Deliver to' (set to 'Other email'), and 'Address' (containing 'aCustomEmailAddress@hotmail.com'). The 'Deliver to' and 'Address' fields are highlighted with a red border.

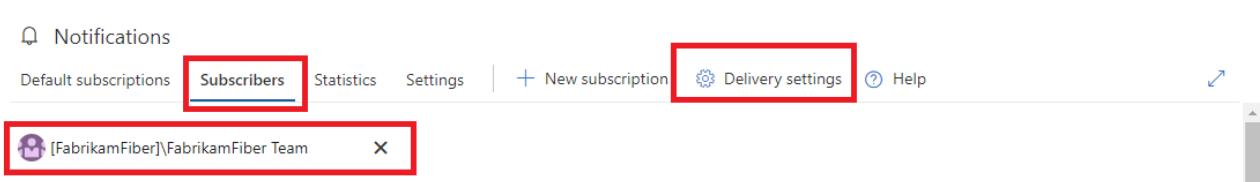
Delivery settings for teams and Azure DevOps Services groups

Before we look at the recipients for team and group subscriptions, let's look at the delivery settings for teams and Azure DevOps Services groups in general. These settings control the default delivery behavior when the team or group is the recipient of a notification and the subscription is configured with a delivery option that looks at the recipient's delivery settings.

NOTE

Teams are just a special type of group. Subscriptions and delivery settings for a team can be managed in the team level settings UI or at the organization level.

Team delivery settings button under organization level settings



Team Delivery settings dialog

Delivery settings

Configure how to deliver notifications that target [FabrikamFiber]\FabrikamFiber Team

- Deliver to email address
- Deliver to individual members
- Do not deliver

Save

Cancel

The following delivery settings are available for a group or team:

- **Deliver to email address:** notifications are delivered to a specific email address.
- **Deliver to individual members:** notifications are delivered to each member of the group or team. This is usually the default option. See the section on "team expansion" below for more details on how this option works.
- **Do not deliver:** notifications are not delivered by default.

If a delivery setting is not explicitly set for a team or group, the value is determined from the [organization-level delivery setting](#) and is either *Deliver to individual members* or *Do not deliver*. Note: the delivery settings dialog does not indicate whether the current selection was explicitly set or if it was inherited.

Recipients for custom team and group subscriptions

The recipients for a custom team or group subscription are controlled by the subscription, but with certain delivery options, the team's default delivery setting is used to determine the set of recipients.

New subscription

The screenshot shows the 'New subscription' dialog. At the top right is a close button (X). Below it, there's a 'Description' field containing 'A work item is created' and a 'Subscriber' field containing 'FabrikamFiber Team' (highlighted with a red box). Under 'Deliver to', there's a dropdown menu set to 'Team preference' (highlighted with a red box), which is expanded to show 'Members of FabrikamFiber Team by role'. Other options like 'Custom email address' and 'Members of FabrikamFiber Team' are also listed. To the right of this is an 'Address' section with a dropdown set to 'FabrikamFiber'. Below these are two tables for clauses:

Operator	Value
Changes from	
<>	[Me]

At the bottom left is a '+ Add new clause' button.

The following delivery options are available for a group or team subscription:

- **Member of team by role:** recipients are members of the team or group that have one of the selected roles (e.g. work item assignee)
- **Team preference:** recipients are determined by the delivery setting of the team or group (*Do not deliver, preferred email address, or members of team*)
- **Custom email address:** recipient is the specified email address
- **Members of team:** recipients are all members of the team or group, except members that have opted out of the subscription. Note: the default delivery setting of each member is honored, including groups that are members of the team or group.

Option: Member of team by role

The email recipient list is determined by members that had a role in the event. For example, the user assigned the work item has the role *Assigned to (new)* while the identity that was previously assigned the work item has the role *Assigned to (previous)*. The full list of roles for each event type are shown in the [supported event types](#).

This screenshot shows the 'Member of team by role' delivery settings. It includes a 'Deliver to' dropdown set to 'Members of FabrikamFiber Team by role' and a 'Roles' dropdown set to 'Assigned to (new), Assigned to (previous), Assi' (with a small error in the screenshot). A checkbox labeled 'Skip initiator' is checked.

The option *Skip initiator*, which appears for most event types, controls whether the user or group that initiated (caused) the event should be explicitly excluded from the set of recipients. In general, this option should be "on" since most users do not want to receive a notification about something they did.

Option: Team preference

The delivery option is taken from the team's delivery setting. It can be one of the following:

- **Deliver to email address:** The email is delivered to the team's preferred email address.
- **Deliver to individual members:** See section below for details of *Members of team*.
- **Do not deliver:** No email is delivered.

This screenshot shows the 'Team preference' delivery settings. It includes a 'Deliver to' dropdown set to 'Team preference' and an 'Address' section with a dropdown set to 'Deliver to individual members'.

The team's delivery setting value is displayed under the *Address* label and can't be changed.

Option: Custom email address

The email is sent to the email address chosen for the subscription.

Deliver to	Address
Custom email address	aCustomerEmailAddress@hotmail.com

Option: Members of team

The team or group membership is expanded to determine the email recipients. In the simple case a team or group expands to a list of individuals and each is included on the **To:** line of the resulting email. However, the results of this expansion can be complicated and are explained in more detail in the [team and group expansion](#) section.

Deliver to	
Members of FabrikamFiber Team	

Recipients for default subscriptions

The delivery option for a default subscription is usually one or more roles. When viewing a default subscription, you'll notice these values can't be changed. The roles and the *Skip initiator* option vary depending on the event type. See [supported event types](#) for a list of roles available for each event type. Note: the *Skip initiator* option is not available for all event types.

Description	Subscriber
Pull request reviewers added or removed	Project Collection Valid Users
Deliver to	Roles
Members of Project Collection Valid Users by role	Creator, Changed reviewers
	<input checked="" type="checkbox"/> Skip initiator

Team and group expansion for email recipients

When a team (or group) is the recipient of a notification and either the subscription or the team's delivery preference indicates that all members of that team should be notified, the team must be "expanded" to determine the actual set of email recipients. This is a potentially recursive process that starts by looking at the team's direct members.

First, only members that have not opted out of the subscription are considered for the final recipient list. Next, any member that is an individual user or mail-enabled group is added to the recipient list. This leaves only Azure DevOps Services groups remaining. For each group, the group's delivery preferences are examined:

- "Do not deliver": no further evaluation is performed on this group and the next member group is evaluated
- "Deliver to email address": the email address is added to the final recipient list
- "Deliver to individual members": the group is expanded (like its parent group) and the same rules for evaluating its members are followed

Let's look at a few scenarios. For these examples, we use the following symbols to denote the types of members:

- I : individual user
- T : nested team or group
- A : mail-enabled Azure Active Directory (Azure AD) group.

Scenario 1: A member with *Do not deliver* preference

The team has members I₁, I₂, and T₁. T₁'s delivery preference is *Do not deliver*.

What happens: only **I1** and **I2** are notified via their preferred email addresses. Members of **T1** are not notified.

Scenario 2: A member with *Deliver to individual members* preference

The team has members **I1**, **I2**, and **T1**. **T1**'s delivery preference is *Deliver to individual members*. **T1** has members **I2** and **I3**.

What happens: **T1** is expanded (because of its delivery preference) and therefore **I1**, **I2**, and **I3** are notified via their preferred email addresses.

Scenario 3: A nested group

The team has members **I1**, **I2**, and **T1**. **T1** has members **I2**, **I3**, and **T2**. **T1**'s delivery preference is *Do not deliver*. **T2** has members **I4** and **I5**. **T2**'s delivery preference is *Deliver to individual members*.

What happens: because **T1** is not expanded (because its delivery preference is "do not deliver"), only **I1** and **I2** are notified via their preferred email addresses.

Scenario 4: A member that is an Azure AD group

The team has members **I1**, **I2**, and **A1**.

What happens: **I1**, **I2**, and **A1** are notified via their preferred email addresses.

Tutorial: Follow a user story, bug, issue, or other work item or pull request

4/16/2019 • 4 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure Repos](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

To get notified of changes made to a work item or a pull request, you can elect to follow them.

This article shows you how to:

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

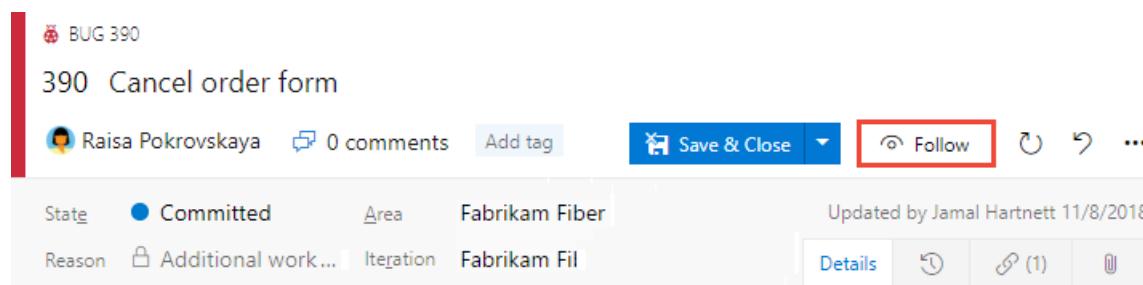
You must configure an [SMTP server](#) in order for team members to receive notifications.

Prerequisites

- You must connect to a project. If you don't have a project yet, [create one](#).
- You must be added to a project as a member of the **Contributors** or **Project Administrators** security group. To get added, [Add users to a project or team](#).
- To view or follow work items, you must be granted **Stakeholder** access or higher. For details, see [About access levels](#). Also, you must have your **View work items in this node** and **Edit work items in this node** permissions set to **Allow**. By default, the **Contributors** group has this permission set. To learn more, see [Set permissions and access for work tracking](#).
- To view or follow pull requests, you must have **Basic** access or higher.
- You must connect to a project. If you don't have a project yet, [create one](#).
- You must be added to a project as a member of the **Contributors** or **Project Administrators** security group. To get added, [Add users to a project or team](#).
- To view or follow work items, you must be granted **Stakeholder** access or higher. For details, see [About access levels](#). Also, you must have your **View work items in this node** and **Edit work items in this node** permissions set to **Allow**. By default, the **Contributors** group has this permission set. To learn more, see [Set permissions and access for work tracking](#).
- To view or follow pull requests, you must have **Basic** access or higher.

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.



The screenshot shows a work item details page for a bug titled "BUG 390". The work item is assigned to "Raisa Pokrovskaya" and has 0 comments. The "Save & Close" button is visible. The "Follow" button is highlighted with a red box. Below the header, there are sections for "State" (Committed), "Area" (Fabrikam Fiber), "Reason" (Additional work...), "Iteration" (Fabrikam Fil), and "Details". The "Details" section includes a clock icon, a link to "(1)", and a refresh icon.

NOTE

The **Follow a work item** feature is available from TFS 2017 and later versions. The **Follow a pull request** feature is available from TFS 2017.1 and later versions. To update your on-premises TFS, visit the [Visual Studio downloads page for Team Foundation Server](#).

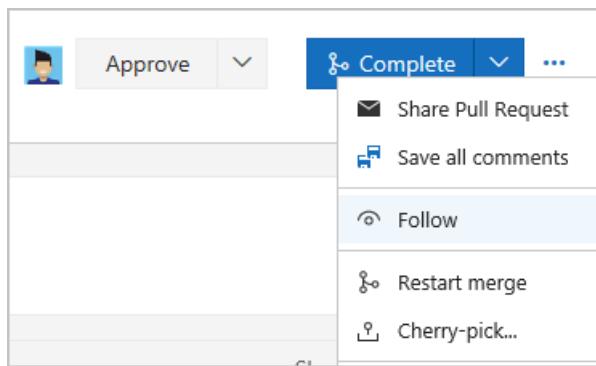
You'll only receive notifications when other members of your team modifies the work item, such as adding to the discussion, changing a field value, or adding an attachment.

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

To stop following changes, choose the  [Following](#) 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 modifies 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](#) 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 Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, the navigation bar includes 'Overview', 'Boards', 'Backlogs', 'Sprints', 'Plans', and 'Code'. The 'Queries' item is selected and highlighted with a red box. The main area is titled 'Queries' and shows a list of 'My Queries' with the following items:

- Active bugs
- All Items
- Assigned to me
- Closed bugs
- Fabrikam Fiber Team - Backlog items
- Followed work items** (highlighted with a red box)
- Following - my query

From this view, you can view all items you're following across all projects. Also, you can perform 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 Azure DevOps interface for the 'Fabrikam Fiber' project. On the left, the navigation bar includes 'Overview', 'Boards', and 'Work Items'. The 'Work Items' item is selected and highlighted with a red box. The main area is titled 'Work Items' and shows a list of followed work items with the following data:

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

Open **Work>Queries** and choose **Followed work items**.

The screenshot shows the 'Queries' section of the Microsoft Team Services interface for the 'Fabrikam Fiber' project. The 'Followed work items' query is selected, highlighted with an orange oval. The results table displays three work items: a Bug titled 'Slow response on form' (resolved), a User Story titled 'Cancel order form' (active), and another User Story titled 'Welcome page' (active). The table includes columns for ID, Work Item Type, Title, and State.

ID	Work Item Type	Title	State
3	Bug	Slow response on form	Resolved
2	User Story	Cancel order form	Active
1	User Story	Welcome page	Active

From this view, you can view all items you're following across all projects. Also, you can perform 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 your Project pages. To learn more, see [Work across projects](#).

Try this next

[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: 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 details, see [Manage team notifications](#).

Manage your notifications

3/5/2019 • 3 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

Feature availability: This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) for team members to see the Notifications option from their organization menu and to receive notifications.

As changes occur to your code base, builds, work items, and other operations, you can receive email notifications. For example, you can set an alert, so you're notified whenever a bug that you opened is resolved or you're assigned to a work item.

In this tutorial, you learn how to do the following tasks:

- View your notifications
- Add a custom subscription
- Unsubscribe or opt out of a team or project subscription

View your personal notifications

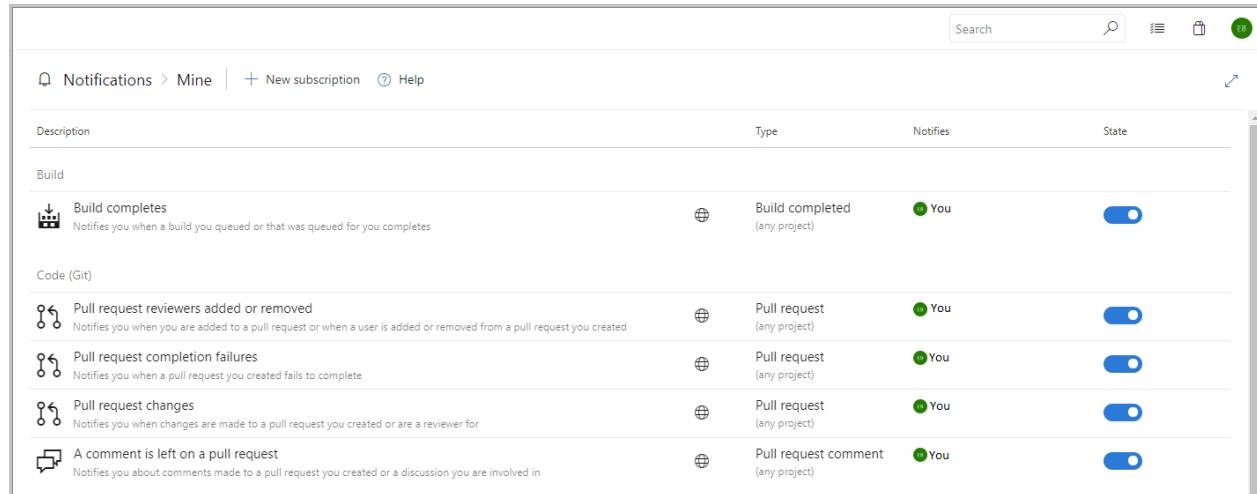
From the web portal, select the icon with your initials or picture, and then select **Notification settings** from the drop-down menu.

The image contains two screenshots of the Azure DevOps web portal. Both screenshots show a user profile icon in the top right corner, which is highlighted with a red box. A dropdown menu appears from the icon, also highlighted with a red box. In both cases, the 'Notification settings' option is listed at the bottom of the menu, also highlighted with a red box. The first screenshot shows the 'Work Items' screen, and the second shows the 'Team Overview' screen.

View all subscriptions

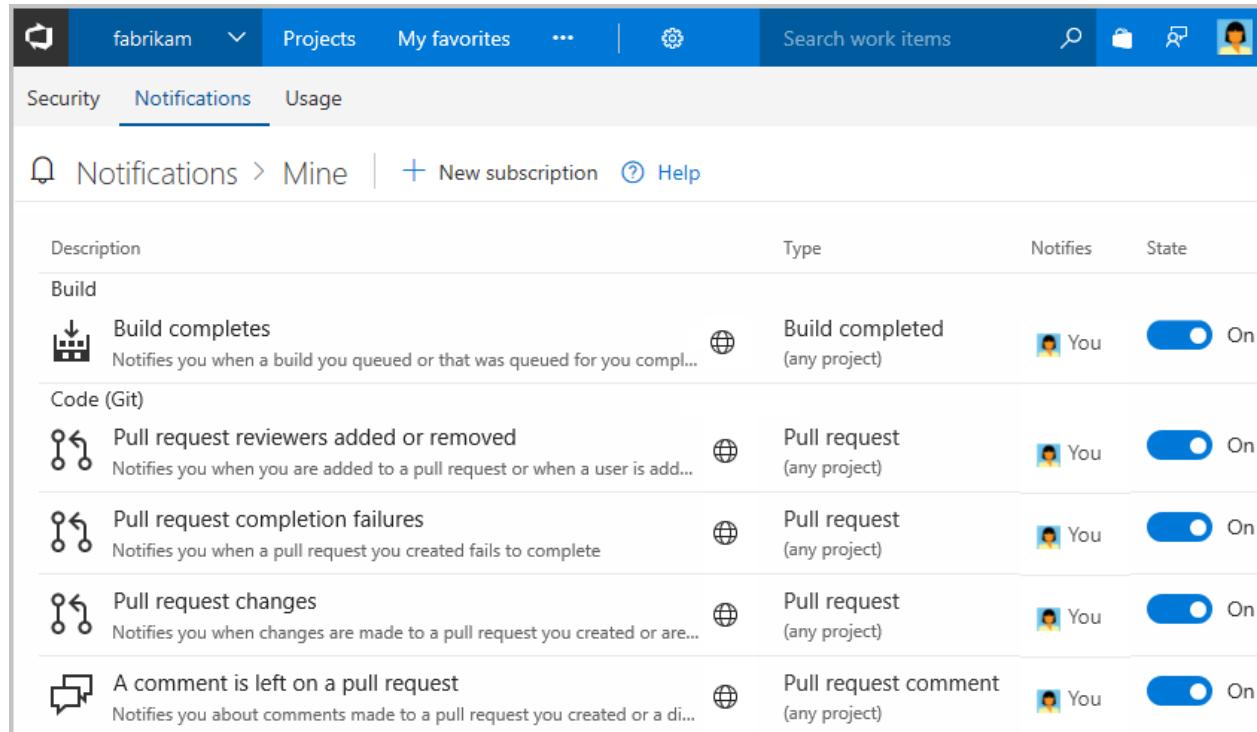
This view shows all subscriptions that you have created or that have been created by an administrator. Subscriptions let you control what you are notified about. Those notifications you're subscribed to are indicated

with the State as **On**.



The screenshot shows the Notifications page with the title "Notifications > Mine". It includes a search bar and navigation links for "New subscription" and "Help". Below the header is a table with columns: Description, Type, Notifies, and State. The table lists several types of notifications:

Description	Type	Notifies	State
Build			
Build completes Notifies you when a build you queued or that was queued for you completes	Build completed (any project)	You	On
Code (Git)			
Pull request reviewers added or removed Notifies you when you are added to a pull request or when a user is added or removed from a pull request you created	Pull request (any project)	You	On
Pull request completion failures Notifies you when a pull request you created fails to complete	Pull request (any project)	You	On
Pull request changes Notifies you when changes are made to a pull request you created or are a reviewer for	Pull request (any project)	You	On
A comment is left on a pull request Notifies you about comments made to a pull request you created or a discussion you are involved in	Pull request comment (any project)	You	On



This screenshot shows the Notifications page for a specific user, indicated by the "fabrikam" dropdown in the top navigation. The "Notifications" tab is selected. The interface is similar to the first screenshot, displaying a list of notification types and their current state (all are set to "On").

A subscription can be just for you, or if you are a team admin, can be shared by everyone in the team.

Add a custom subscription

With custom personal subscriptions, you can define precise criteria for the events you want to receive notifications for. In contrast to a default subscription, which only notifies the users or groups directly associated with an event, a custom subscription can notify you about any event.

1. From your Notifications page, select **New subscription**.

The screenshot shows the 'User settings' page with the 'Notifications' tab selected. The right pane displays a list of notification types under the 'Build' category. A red box highlights the '+ New subscription' button at the top right of the list.

Description	Type
Build completes	Build completed (any project)
Pull request reviewers added or removed	

The screenshot shows the 'Notifications > Mine' page. A red box highlights the '+ New subscription' button at the top right. Below it, there is one notification entry for 'Build completes'.

Description	Type
Build completes	Build completed (any project)

1. Choose the category and template you want to use. For a list of supported templates, see [Default and supported notifications](#).

Here we choose to get notified when a pull request is created within a specific project, Fabrikam Fiber.

The screenshot shows the 'New subscription' dialog. On the left is a sidebar with categories: Build, Code (Git), Code (TFVC), Work, Extension management, and Release. On the right is a main area showing templates for each category. The 'Code (Git)' category is selected, and the 'A pull request is created or updated' template is highlighted with a gray background.

Category	Template
Build	A commit authored by me is pushed
Code (Git)	A commit is pushed by me
Code (TFVC)	A commit is pushed
Work	A pull request is created or updated
Extension management	
Release	

Next **Cancel**

2. Modify the description to help you identify the subscription later. Also choose an email address for notifications to be delivered to. By default, your preferred email address is used. Optionally, include one or more fields to further specify the event criteria.

New subscription

Description	Subscriber																				
A pull request is created or updated from Fabrikam Fiber	Raisa Pokrovskaya																				
Deliver to	Address																				
Preferred email	fabrikamfiber5@hotmail.com																				
Filter																					
<input type="radio"/> Any team project <input checked="" type="radio"/> A specific team project	Fabrikam Fiber																				
Filter criteria	<table border="1"> <thead> <tr> <th colspan="2">And/Or</th> <th>Field</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>+ </td> <td><input type="checkbox"/></td> <td>Status</td> <td>Changes to</td> <td>Abandoned</td> </tr> <tr> <td>+ </td> <td><input type="checkbox"/></td> <td>Reviewers</td> <td>Contains</td> <td>[Fabrikam Fiber]\Web</td> </tr> <tr> <td colspan="5">+ Add new clause</td> </tr> </tbody> </table>	And/Or		Field	Operator	Value	+	<input type="checkbox"/>	Status	Changes to	Abandoned	+	<input type="checkbox"/>	Reviewers	Contains	[Fabrikam Fiber]\Web	+ Add new clause				
And/Or		Field	Operator	Value																	
+	<input type="checkbox"/>	Status	Changes to	Abandoned																	
+	<input type="checkbox"/>	Reviewers	Contains	[Fabrikam Fiber]\Web																	
+ Add new clause																					
Previous Finish Cancel																					

NOTE

The fields available for filtering event criteria differ depending on the category and template you select.

3. Select **Finish** when you're done. The subscription now appears in the list under the category you selected.



Unsubscribe or opt out of a team or OOB subscription

You can choose to not receive notifications for certain team subscriptions by opting out of the subscription.

To unsubscribe from any notification, even one that you've defined, slide the State **On/Off** indicator to the Off position.

For example, here we turn off the Build completes subscription.

Notifications > Mine | [New subscription](#) [Help](#)

Description	Type	Notifies	State
Build			
Build completes Notifies you when a build you queued or that was que...	...	Build completed (any project)	You Off

NOTE

Whether you are an administrator or not, toggling a shared team subscription from your notification settings only impacts you and not other team members.

Related articles

- [Set your preferences](#)
- [Default and supported notifications](#)
- [Follow a specific work item](#)
- [Manage notifications for a team](#)
- [Change your preferred email address](#)

Limitations

- The user interface no longer supports creating plain text email subscriptions.

Manage notifications for a team

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

As changes occur to work items, code reviews, pull requests, source control files, and builds, your team can be notified via email. For example, when a high priority work item is assigned to your team's area path, an email can be sent to the team.

Create a custom email subscription

A subscription lets you control what your team should be notified about and how the team receives those notifications.

1. Open the Notifications page under team settings:

https://dev.azure.com/{organization}/{project}/_admin/_notifications?view=contents

The screenshot shows the Azure DevOps interface for managing project settings. On the left, there's a sidebar with icons for Overview, Boards, Repos, Pipelines, Test Plans, Artifacts, and a prominent 'Project settings' button, which is highlighted with a red box. The main content area shows the 'Notifications' section under the 'FabrikamFiber Web Team' settings. A red box highlights the 'Notifications' link in the left navigation bar. The right pane displays various notification rules, such as 'Build completes' and 'Pull request changes', each with a description and a small icon.

The screenshot shows the 'FabrikamFiber / Fabrika...' project dashboard. In the left sidebar, under 'Work', the 'Notifications' option is highlighted with a red box. The main area displays a 'Welcome' section with links to Manage Work, Collaborate on code, Continuously integrate, and Visualize progress. On the right, there's a 'Team Members' section with two user icons and a '+' button, and a 'Work' section with links to Backlog, Board, Task board, and Queries.

2. Select **New subscription**. If you're not a team administrator, [get added as one](#). You need to be a team, project, or project collection administrator to create team alerts.

The screenshot shows the 'Project Settings > Notifications > FabrikamFiber Web Team' page. The 'Notifications' tab is selected in the left sidebar. At the top right, there is a red box around the '+ New subscription' button. Other tabs in the sidebar include General, Overview, Teams, Security, Service hooks, and Dashboards. The main area shows a 'Build' section with a 'Build completes' notification rule.

The screenshot shows the 'MyFirstProject' project dashboard. The 'Notifications' tab is selected in the top navigation bar. A red box highlights the '+ New subscription' button at the top right of the notifications section. Other tabs in the top navigation include Overview, Work, Security, Version Control, Policies, Agent Queues, Service Hooks, and Wiki. The main area shows a 'Notifications' section with a 'MyFirstProject Team' link and a 'Build completes' notification rule.

3. Select the type of activity you want your team to be notified of.

New subscription

Category	Template
Build	A commit is pushed
Code (Git)	A pull request is created or updated
Code (TFVC)	A pull request my team is a reviewer on is updated
Work	
Extension management	
Release	

Next Cancel

4. Provide a description to help you identify the subscription later.

Description	Subscriber
A pull request is created or updated	MyFirstProject Team

5. Choose which team members should receive a notification:

Deliver to	Roles
Members of MyFirstProject Team	Creator, Reviewers, Changed re
<input checked="" type="checkbox"/> Skip initiator Members of MyFirstProject Team by role	

You can choose one of the following delivery options:

- Team members by role:** only certain team members associated with the event are notified. For example, for work item changes, you might only want the current assignee of the work item to receive a notification.
- Team preference:** use the team's default delivery preference. Learn how to [manage delivery settings below](#).
- Custom email address:** send an email to a specified email address.
- All team members:** send an individual email to each member of the team.

For certain activities and when **Team members by role** is selected, you can choose to have the user that initiated the activity receive a notification. This is controlled by the **Skip initiator** checkbox. By default, this box is checked meaning the user that initiates the change is not notified about it.

6. Choose whether you want to receive notifications about activity in all projects or only a specific project.

Filter
<input type="radio"/> Any team project <input checked="" type="radio"/> A specific team project
MyFirstProject

7. Optionally configure additional filter criteria.

Filter criteria

And/Or	Field	Operator	Value
+ X	Status	Changes to	Completed
+ X	Source branch name	Contains	features/

[Add new clause](#)

8. Select **Finish** to save the new subscription.

Manage team delivery settings

Choose the default method for your team to receive notifications by updating the **team delivery settings**.

1. Open the Notifications page under team settings:

https://dev.azure.com/{organization}/{project}/_admin/_notifications?view=contents

Azure DevOps

regius / FabrikamFiber Web / Settings

Project Settings > Notifications > FabrikamFiber Web Team

- General
- Teams
- Security
- Notifications** (highlighted with a red box)
- Service hooks
- Dashboards

Notifications > FabrikamFiber Web Team

Description

Build

Build completes

Code (Git)

Pull request reviewers added or removed

Pull request changes

Project settings

2. Choose **Delivery settings**:

regius / FabrikamFiber Web / Settings

Project Settings > Notifications > FabrikamFiber Web Team

- General
- Teams
- Security
- Notifications** (highlighted with a red box)
- Service hooks

Notifications > FabrikamFiber Web Team

[New subscription](#) [Delivery settings](#) [Help](#)

Build completes

3. Choose which option best fits your team's needs:

X

Delivery settings

Configure how to deliver notifications that target [MyFirstProject]\MyFirstProject Team

Deliver to email address

Deliver to individual members

Do not deliver

Save

Cancel

Related articles

- [Manage personal notification settings](#)

Manage notifications for an organization

5/30/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

In this article, learn about managing notifications for your organization.

TIP

We don't support organization-wide notifications. As an alternative, you can provide an email distribution list that goes to your entire organization.

Organization level notifications page

See [Navigating the UI](#) to learn how to locate this page.

The organization notifications page consists of the following sections:

- Default subscriptions - view all [default notification subscriptions](#)
- Subscribers - view notification subscriptions for a specific group, team, or individual
- Statistics - view the most active subscriptions and top event initiators
- Settings - manage organization level settings such as delivery preferences

Organization notifications page: Default subscriptions

The `Default subscriptions` section lists all default subscriptions available to the organization. The globe icon on a notification subscription indicates the subscription is a default subscription.

Members of the **project collection administrators** group have permission to enable/disable any default subscription in this view. Any member project collection valid users have permission to view the details of the default subscription. The view and enable options are available in the context menu (`...`) associated with each individual subscription.

The screenshot shows the 'Default subscriptions' section of the Notifications page. It lists several notification types under 'Build' and 'Code (Git)'. Each entry includes an icon, a description, and a 'Type' column. A red box highlights the 'Default subscriptions' tab at the top, and another red box highlights the '...' button next to the 'Build completed' entry.

Description	Type
Build	
Build completes	Build completed (any project)
Pull request reviewers added or removed	Pull request (any project)
Pull request completion failures	Pull request (any project)
Pull request changes	Pull request (any project)
A comment is left on a pull request	Pull request comment (any project)
Code (Git)	
Pull request reviewers added or removed	Pull request (any project)
Pull request completion failures	Pull request (any project)
Pull request changes	Pull request (any project)
A comment is left on a pull request	Pull request comment (any project)

Organization notifications page: Subscribers

The **Subscribers** section begins with an empty identity search box. Enter any group, team, or individual to view the list of subscriptions associated with the specified identity.

The screenshot shows the 'Subscribers' section of the Notifications page. It features a search bar labeled 'Search users and groups' and a message 'Get started by selecting a user or group'. A red box highlights the 'Subscribers' tab at the top.

All notification subscriptions for the chosen identity are listed in this view. Management options are available from the context menu (...) associated with each subscription. Note, the icon on subscription row indicates a default subscription.

The screenshot shows the 'Subscribers' section for the identity '[FabrikamFiber]\FabrikamFiber Team'. It lists three notification subscriptions: 'Build completes', 'Pull request reviewers added or removed', and 'Pull request changes'. Each subscription is associated with the team's name. A red box highlights the 'Subscribers' tab at the top.

Description	Type	Notifies
Build		
Build completes	Build completed (any project)	[FabrikamFiber]\FabrikamFiber Team
Pull request reviewers added or removed	Pull request (any project)	[FabrikamFiber]\FabrikamFiber Team
Pull request changes	Pull request (any project)	[FabrikamFiber]\FabrikamFiber Team
Code (Git)		

Organization notifications page: Statistics

The **Statistics** section shows the most active notification subscriptions and the top event initiators (group, team, or individual). The statistics are only for the current day and reset at 00:00 UTC. A benefit of these statistics is identifying unintended high volume subscriptions or event initiators.

The screenshot shows the 'Notifications' page with the 'Statistics' tab selected. A red box highlights the 'Most active subscriptions' section, which displays a table of notifications. Another red box highlights the 'Top event initiators' section, which also displays a table of notifications.

Most active subscriptions

Description	Notifications	Event type	Channel
A work item is created (153851)	2	Work item	Email
Build completed / Web Hooks Post via HTTP	1	Build completed	ServiceHooks
Work item created / Web Hooks Post via HTTP	1	Work item	ServiceHooks
Build completes	1	Build completed	User

Top event initiators

User or group	Event type	Events
Jamal Hartnett	Work item	2
Jamal Hartnett	Build completed	1
Jamal Hartnett	Build completed (legacy)	1
Jamal Hartnett	Build completed (legacy V2)	1

Organization notifications page: Settings

The **Settings** section allows organization level notification settings to be managed by any member of the **project collection administrators** group. All teams and groups inherit the *Default delivery option* setting, which is why it isn't explicitly set at the team or group level.

The screenshot shows the 'Notifications' page with the 'Settings' tab selected. A red box highlights the 'Default delivery option' setting, which is currently set to 'Deliver to individual members'. Below this, there is a link to 'Delivery Settings'.

Default delivery option for groups in this project collection (can be set for individual groups in Delivery Settings)

Deliver to individual members

[Delivery Settings](#)

Manage organization notification settings

5/30/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

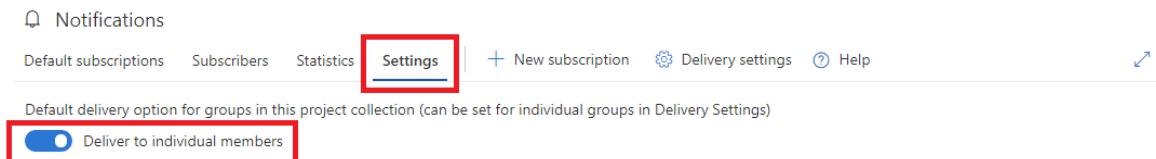
NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [configure an SMTP server](#) for team members to see the Notifications option from their organization menu and to receive notifications.

You can choose to allow or block delivery of emails for all subscriptions owned by a team or a group. This is a default setting which applies only if the team or group has not explicitly set the option.

Manage the default delivery setting

1. [Navigate to the organization notifications settings page](#).
2. Select the **Settings** tab.
3. Configure the default the delivery setting.



Analyze organization-level notifications statistics

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) for team members to see the Notifications option from their organization menu and to receive notifications.

Notification statistics show the top 10 most active subscriptions and the top event initiators in your organization for the current day. Administrators should periodically review statistics to ensure there are no unintended high volume subscriptions or event initiators.

View notification statistics for organization

1. [Navigate to the organization notifications settings page](#).
2. Select the **Statistics** tab.
3. Analyze the most active subscriptions and top event initiators.

The screenshot shows the 'Notifications' section of the organization settings. The 'Statistics' tab is selected. The 'Most active subscriptions' table lists four entries:

Description	Notifications	Event type	Channel
A work item is created (153851)	2	Work item	Email
Build completed / Web Hooks Post via HTTP	1	Build completed	ServiceHooks
Work item created / Web Hooks Post via HTTP	1	Work item	ServiceHooks
Build completes	1	Build completed	User

The 'Top event initiators' table lists four entries, all associated with the user 'Jamal Hartnett':

User or group	Event type	Events
Jamal Hartnett	Work item	2
Jamal Hartnett	Build completed	1
Jamal Hartnett	Build completed (legacy)	1
Jamal Hartnett	Build completed (legacy V2)	1

Notes:

- A context menu (⋮) on the most active subscriptions provides the option to edit, disable, or delete the subscription
- Both email and service hooks subscriptions are eligible for the most active subscriptions
- The integer subscription ID is shown in the description for a custom email subscription
- Results are not a sliding 24-hour window and reset at the beginning of each day (00:00 UTC)

Change your preferred email address for notifications

3/5/2019 • 2 minutes to read • [Edit Online](#)

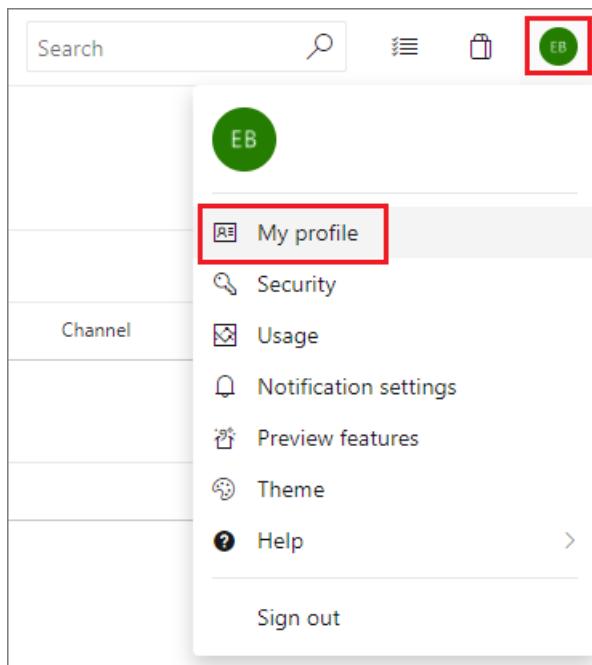
Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

You can change your preferred email address for notifications from your organization preferences profile page. Notifications are sent by default to the preferred email address for your organization profile. This is typically the email address you signed into Azure DevOps Services or Team Foundation Server (TFS) with.

NOTE

Your preferred email address applies across all of your organizations and cannot be changed on a per-organization basis.

1. To change your preferred email address, open your organization menu and select **My profile**.



The screenshot shows the profile and information page for a user named 'Raisa'. At the top right is a user profile icon with initials 'RA' and the name 'Raisa' followed by the email 'fabrikamfiber5@hotmail.com'. Below it is a list of options: 'My profile' (highlighted with an orange box), 'Notification settings', 'Security', 'Usage', 'Preview features', and 'Sign out'. The 'My profile' option is highlighted with an orange border.

1. From your profile and information page, select **Edit profile**.
2. Update the address and select **Save changes**.

Related articles

- [Manage personal notifications](#)
- [Manage team notifications](#)
- [Manage organization notifications](#)

How to use subscription logging

5/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018

NOTE

This topic applies to Azure DevOps Services, TFS 2018 Update 2, and later versions. For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Subscription logging is a valuable tool for troubleshooting. It provides diagnostic information from the notifications pipeline and is disabled by default. Once enabled, up to 25 logs, or one hour's worth of logs, are collected for the subscription.

Enabling subscription logging

IMPORTANT

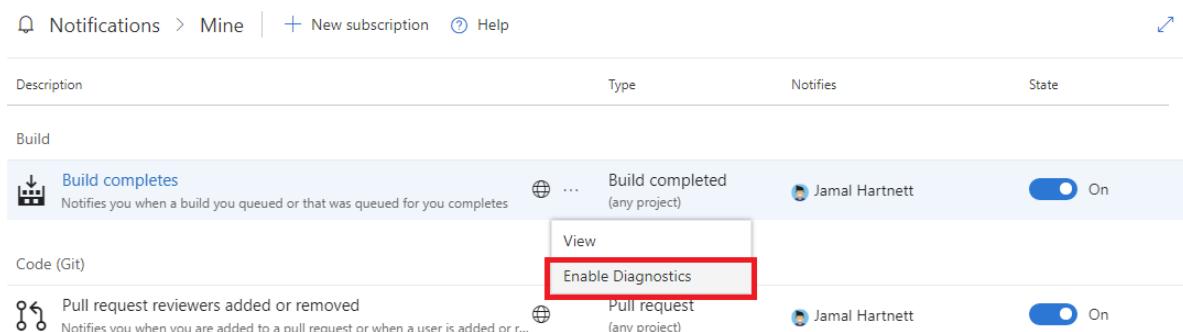
There is a known issue in TFS 2018 Update 2 and TFS 2018 Update 3, where enabling subscription logging for default (globe icon) subscriptions may cause issues with notification delivery. If you're on one of those two versions, it's recommended that you not enable subscription logging for default subscriptions.

Complete the following steps to enable subscription logging:

1. Enable diagnostics for your organization by entering the following URL in your browser:

`https://dev.azure.com/{organization}/_notifications?diagnostics=true`

2. The option *Enable Diagnostics* appears in the subscription context menu.



View subscription diagnostic logs for event matching

Get all subscription event processing logs by entering the following URL in your browser:

`https://{{organization}}/_apis/notification/DiagnosticLogs/{{event ID}}/entries?startTime={{date}}&endTime={{date}}`

- *organization* is your organization (for example, dev.azure.com/fabrikam-fiber)
- *date* is a date time specification (for example, **2018-06-29** or **2018-06-29 02:00**)
- *event ID* is **915f48f2-1b64-40d9-a43f-fe2528b4f296** for work item events, or
- *event ID* is **9a688110-9e33-4cdc-affd-75d16303e7f1** for Git events, or

- *event ID* is **a4804dcf-4bb6-4109-b61c-e59c2e8a9ff7** for any other event type

The result is JSON-formatted logging information.

View subscription diagnostic logs for notification delivery

Retrieve all notification delivery logs in a given time frame by entering the URL in your browser.

```
https://{{organization}}/_apis/notification/DiagnosticLogs/{{event ID}}/entries?startTime={{date}}&endTime={{date}}
```

- *organization* is your organization (for example, dev.azure.com/fabrikam-fiber)
- *date* is a date time specification (for example, **2018-06-29** or **2018-06-29 02:00**)
- *event ID* is **631f49b3-46e1-42ec-8fff-081bd176c18a** for work item events, or
- *event ID* is **8833fc71-42ca-441b-ab12-25314877772d** for Git events, or
- *event ID* is **a96d6177-beef-477a-a2ee-2c31433214d0** for any other event type

The result is JSON-formatted logging information.

Exclude yourself from notification emails from events you initiated

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

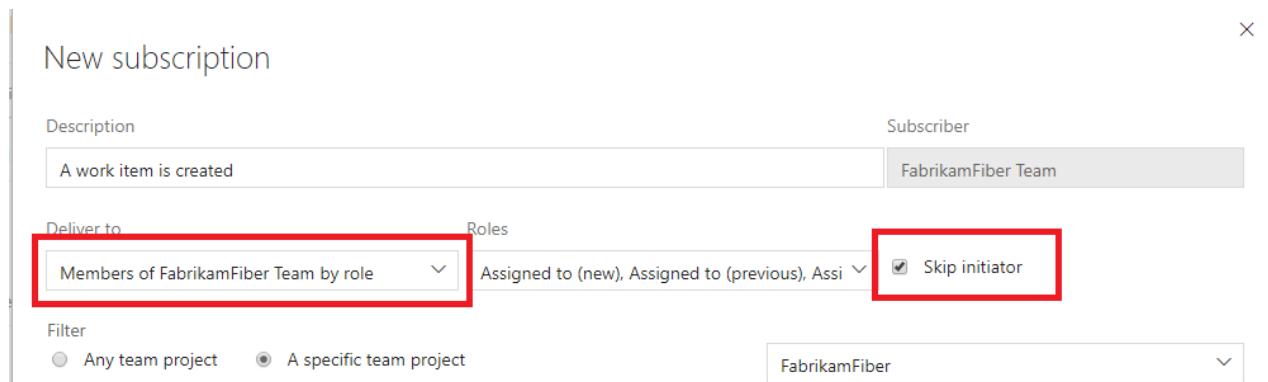
NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

The option *Skip initiator* is available when creating a team role-based notification subscription. This option causes emails to be skipped for the initiator of the event which triggered the email.

For example, if your team has a subscription set up for a *pull request created* event and a user creates a pull request in the project, that user doesn't receive the *pull request created* notification email, but the other members of the team do.

This option can be beneficial for users who don't want to be notified of events they just triggered, but has caused some users to feel they missed an email when their teammates received the email and they didn't. Leave it up to your team to decide which option is best.



Use @mentions in work items and pull requests

6/13/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

The **@mention** control allows you to quickly pull someone into a work item or pull request.

NOTE

The **@mention** control is available from TFS 2015 Update 2 and later versions.

For team members to receive notifications, [you must configure an SMTP server](#).

When you're leaving a code comment in a pull request, you can enter @ to trigger the **@mention** identity picker. From the identity selector, you see a list of those people that you've recently mentioned. Choose one of those names or enter the name of the person you are looking for to perform a directory search.

To filter the list, enter the user name or alias until you've found a match.

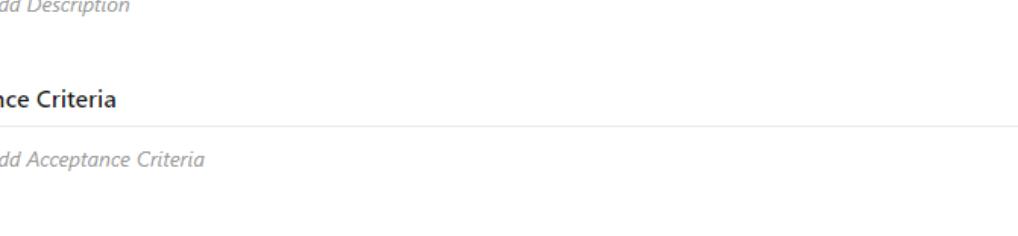
Description

Click to add Description

Acceptance Criteria

Click to add Acceptance Criteria

Discussion



EB @jamal hartnett

JH Jamal Hartnett fabrikamfiber4@hotmail.com

Showing 1 result

EB Elijah Batkoski commented just now

Fixed additional bug

You can also use group mentions. Enter the name of a team or a security group, choose the search icon, and then select from the options listed.

To **@mention** a user you've never selected previously, just continue to enter the entire name to perform your search against the full directory.

Names of those that you mention appear in **blue text**. Choose the **@mention link name** to open the user's contact card, which can provide you additional context for why they were pulled into the conversation.

Description

Click to add Description

Acceptance Criteria

Click to add Acceptance Criteria

Discussion



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



Elijah Batkoski commented just now
@Jamal Hartnett could you check this out?



Elijah Batkoski commented 2 minutes ago
Fixed additional bug

Upon completion of your selection and text entry, your **@mention** user receives an email alerting them about the mention.

Fri 7/24/2015 3:47 PM

Visual Studio Online

Christie Church mentioned you in a pull request

To Jamal Hartnett

Who's Who + Get more apps

Christie Church mentioned you in a pull request

Comment

@Jamal Hartnett can you check this out

Use the **@mention** control in pull request discussions, commit comments, changeset comments, and shelveset comments.

Related articles

- [Work item form controls](#)
- [Pull requests](#)

Use #ID to link to work items

5/24/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

Use the **#ID** control to quickly link objects to work items.

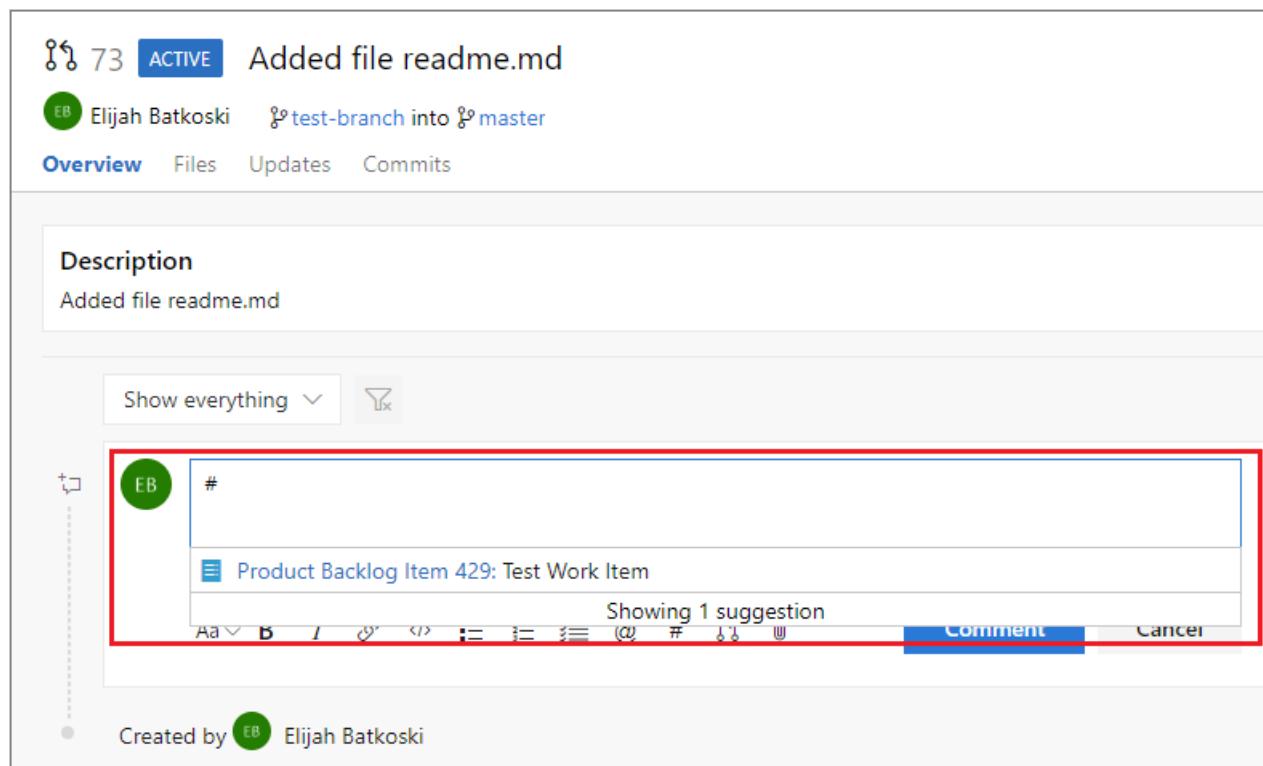
NOTE

The **#ID** special control feature is available from TFS 2015 Update 1 and later versions.

Link a pull request to a work item

When you are leaving a code comment in a pull request, you can enter **#** to trigger the **#ID** work item picker. The picker displays a list of 50 work items that you have recently modified or that are assigned to you.

You can narrow the list of suggested work items by entering keywords that match the work item type, ID, or title, or you can enter the exact work item ID.



The screenshot shows a pull request details page. At the top, it says "73 ACTIVE Added file readme.md". Below that, it shows the author "Elijah Batkoski" and the branches "test-branch" and "master". Under the pull request number, there's a "Description" section with the text "Added file readme.md". Below the description, there's a search bar with "Show everything" and a filter icon. A red box highlights a dropdown menu where the character "#" has been typed, triggering a list of suggestions. The suggestion list shows one item: "Product Backlog Item 429: Test Work Item". At the bottom of the suggestion list, it says "Showing 1 suggestion". Below the suggestion list, there are icons for font size, bold, italic, etc., followed by "Comment" and "Cancel" buttons. At the very bottom, it says "Created by Elijah Batkoski".

To further filter the list, continue to enter keywords until you've found a match. You can enter up to five keywords.

Link to work items in pull requests, comments, and commits

You can also use the **#ID** control in pull request discussions, commit comments, changeset comments, and shelveset comments.

NOTE

Requires TFS 2015 Update 2 or a later version.

Link to work items from a Wiki page

Use the **#ID** control to link to a work item from within a Wiki page.

To learn more about the built-in wiki, see [Add & edit wiki pages](#).

Related articles

- [Link work items](#)
- [Save work with commits](#)
- [Pull requests](#)
- [Check in your work to the team code base](#)

Integrate third party services

3/5/2019 • 2 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Integrate with your favorite services by notifying them when events happen in Azure DevOps Services. See the following examples:

- [Send Azure DevOps Services notifications to a Slack channel](#)
- [Send Azure DevOps Services notifications to a Microsoft Teams channel](#)
- [Send Azure DevOps Services notifications to a Trello board](#)
- [Send Azure DevOps Services notifications to a HipChat room](#)
- [Send Azure DevOps Services notifications to Azure Service Bus](#)

Or, integrate with any endpoint by [Sending Azure DevOps Services notifications to a generic WebHook](#). Learn about all the integration options.

Not getting emails from Azure DevOps subscriptions or notifications

3/27/2019 • 4 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

An email is generated when an [event](#) occurs within Azure DevOps Services, which matches a notification subscription. For more information about notification subscriptions, see the [notifications overview](#).

Learn why you may not be receiving an expected subscription or notification email.

If you're not receiving an expected notification email, it could be for one of the following reasons.

- The email was delivered to an unchecked folder
- The subscription is disabled or opted-out
- The event doesn't match the specified subscription filter conditions
- The subscription is defined to not send emails to the initiator of an event
- The organization level *do not deliver* setting is impacting email delivery
- The team or group level *do not deliver* setting is impacting email delivery
- You're not a member of the group or team receiving the email
- You're a member of an AD group and the subscription contains a @Me clause
- You don't have permission to view the event details, which are included in the email

Complete the following steps to determine if any resolve the issue.

Step 1: Check other email folders including the junk folder

Ensure the email wasn't delivered to a different email folder.

Step 2: Locate the subscription and ensure it's enabled

Navigate to your personal subscriptions and locate the subscription, which you feel should have produced an email, but didn't. [Learn how to navigate to your personal subscriptions](#).

If the subscription is grayed-out in the user interface, then it's disabled. The following screenshot shows the first subscription enabled and the second disabled.

Code (Git)				
	Pull request reviewers added or removed Notifies you when you are added to a pull request or when a user is added or remo...		Pull request (any project)	Jamal Hartnett <input checked="" type="checkbox"/> On
	Pull request completion failures Notifies you when a pull request you created fails to complete		Pull request (any project)	Jamal Hartnett <input type="checkbox"/> Off

A default subscription is disabled when an administrator opts out at the organization or team level, or if an individual opts out in their personal subscription settings. Custom subscriptions are disabled when an administrator disables the subscription at the organization or team level, or when an individual disables a personal custom subscription.

Step 3: Closely inspect the subscription filter conditions

An email is only generated if an Azure DevOps Services event matches *all* of the filter conditions of the

subscription. You can view the filter conditions by selecting the subscription link in the subscription user interface. You can view the filter conditions even if you don't have permission to change them. Closely inspect *all* filter conditions to see if they matched the Azure DevOps Services event.

Step 4: Check the "Skip initiator" option on the subscription

The checkbox option on a subscription causes the initiator of the Azure DevOps Services event to be excluded from the recipient list of the generated email, while all others receive the event. For example, consider a subscription for a *work item changed* event. You can choose to avoid being emailed for changes you make to the work item. [Learn more about excluding the initiator from notifications.](#)

Step 5: Check "Do not deliver" setting for the organization

Navigate to the organization level notifications page and select the tab. [See how to manage notification settings.](#) If the *delivery setting* is set to , then all teams or groups that don't have explicit delivery settings inherit this value. This setting alone doesn't necessarily indicate an email isn't delivered, but it could contribute to the problem. Continue with the next step to determine if a group or team delivery setting is inheriting this value and blocking delivery to your group or team.

Step 6: Check "Do not deliver" setting for your team or group

If the team or group defines a delivery setting for **Deliver to individual members**, it's still possible the team contains other groups. The other groups have a different delivery setting. To learn more about how team membership expands and how some members of the team could receive an email while others don't, see [How email recipients of notifications are determined.](#)

Step 7: Check your configured email address

Check if your preferred email address is set to the address you're expecting the email. This is a user profile setting. Hover over profile icon to view your preferred email address. [Learn how to view the configured email address.](#)

Step 8: Is this a team subscription, which contains a "@Me" filter clause?

If a team or group subscription contains an @Me filter clause and the target email recipients that contains an AD group, no members of the AD group match the filter clause. AD groups are not expanded for filter matching.

Step 9: Do you have permission to see the event artifact?

Recipients who don't have permission to view the artifact, don't receive an email, which contains event artifact data, such as a work item. The only way to know if an email was *filtered* is to view notification delivery logs. Learn more about [enabling and retrieving subscription and delivery logging.](#)

Contact customer support

If you're not able to resolve the issue with the previous steps, consider contacting [customer support](#)

Why did I get this email

3/5/2019 • 2 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

If you're receiving a notification email that you didn't expect, it could be for one of the following reasons:

- The email is sent to a group of which you are a member
- The email was triggered by a different subscription than you expected

Please perform the following steps to determine if any resolve the issue:

Step 1: Inspect the 'To:' line on the email

Either your email address is on this line, or you are a member of a group included on it. Users receiving unexpected emails are often included as part of a group which is receiving the email. The subscription administrator might have configured the email delivery preferences to a wider than anticipated group.

Step 2: Inspect the footer of the unexpected email

All emails have a footer which contains a link to view the subscription which triggered the email. Select the link and view the subscription. You received the email because this subscription to which your are subscribed. If it's a organization or team subscription, you have the option to opt out of the subscription.

We sent you this notification due to a default subscription | [View](#) | [Unsubscribe](#)

Sent from Visual Studio Team Services.

Contact customer support

If you're not able to resolve the issue with the steps above, consider contacting [customer support](#).

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#)

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

Learn why you may not be receiving an expected notification email, and how to check the notification statistics.

Emails from Azure DevOps Services subscriptions or notifications are delayed

An email is generated when an [event](#) occurs within Azure DevOps Services which matches a notification subscription. See the [notifications overview](#) for more information about notification subscriptions.

If you're not receiving an expected notification email, it could be for the following reason:

- Your organization is creating a very large volume notifications

Please perform the following step to determine if it resolves the issue.

Step 1: Check the notification statistics for unexpectedly high volume

Poorly defined subscription filters or duplicate subscriptions might cause an unexpected high volume of notifications, causing a delay in the processing or delivery of emails. [Learn how to view and analyze notification statistics](#)

Contact customer support

If you're not able to resolve the issue with the steps above, consider contacting [customer support](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

NOTE

This topic applies to Azure DevOps Services, TFS 2017 Update 1, and later versions. If you work from an on-premises TFS 2017 or earlier versions, see [Set alerts, get notified when changes occur](#). For on-premises TFS, [you must configure an SMTP server](#) in order for team members to see the Notifications option from their organization menu and to receive notifications.

If you've reviewed the troubleshooting sections and can't resolve your issue, please consider opening a free support ticket.

Contacting support

When you're contacting support for notification issues, it's good to have answers to the following questions:

1. When did you start noticing the problem?
2. What emails are you not getting that you expect?
3. Are you getting other types of emails?
4. Is it just you or are others also not getting emails they expect?
5. Can you supply IDs such as work item, build, or pull request IDs of recent events and an approximate time of the event?
6. Can you forward a sample email of a delayed or unexpected email? If not, copy and provide the URL from the View Result button on an email.

It's best to have a recent event for the email or service hook notification in question. Full details about the event and notification delivery are retained for a few days and are beneficial when resolving a notification issue. You might be asked to reproduce the issue with a new event and provide the time/date of the event and IDs (build, pull request, etc) associated with the event.

Default and supported notifications

3/5/2019 • 3 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

Default subscriptions are configured to send notifications to certain roles or user groups with specific associations to an event. For example, "reviewer" is a role on a pull request event. "Assignee (current)" is a role that reflects the current Assigned To user of a changed work item.

The roles that receive a notification for a particular default subscription are reflected in the description of the subscription, for example, "*Notifies you when a build you queued or that was queued for you completes*". Role-based subscriptions contain a Roles field which you can view by opening the subscription. Only users or groups that belong to the role listed within the subscription receive a notification for an event matched by the subscription.

Default subscriptions only send targeted notifications. That is, the recipient is always somehow associated with the event that triggered the notification. For example, the default subscription for work item updates only sends an email notification to the person assigned to the work item.

Out-of-the-box (OOB) or default subscriptions

The following events generate a notification to all subscribers by default. To unsubscribe from any one notification, see [Unsubscribe from a notification](#).

Within the personal notifications page, OOB subscriptions appear with the following image: .

CATEGORY	TYPE	BUILD	DESCRIPTION
Build	Build completed	Build completes	Notifies you when a build you queued or that was queued for you completes
Code (Git)	Pull request	Pull request reviewers added or removed	Notifies you when you are added to a pull request or when a user is added or removed from a pull request you created
Code (Git)	Pull request	Pull request completion failures	Notifies you when a pull request you created fails to complete
Code (Git)	Pull request	Pull request changes	Notifies you when changes are made to a pull request you created or are a reviewer for
Code (Git)	Pull request comment	A comment is left on a pull request	Notifies you about comments made to a pull request you created or a discussion you are involved in

CATEGORY	TYPE	BUILD	DESCRIPTION
Code (TFVC)	Code review	A code review I am working on changes	Notifies you when a change is made to a code review you're assigned to
Extension management	Extension	Extensions have been modified.	Extensions have been modified.
Extension management	Extension request (batch)	Extensions are requested or requests are updated.	Extensions are requested or requests are updated.
Release	Deployment pending	Manual intervention pending	Notifies you when a manual intervention is pending on you
Release	Deployment completed	Deployment to an owned environment failed	Notifies you when a deployment to an environment you own fails to complete successfully and makes the environment unhealthy
Release	Deployment completed	Deployment to an approved environment failed	Notifies you when a deployment you approved fails to complete successfully and makes the environment unhealthy
Release	Deployment completed	Deployment completion failures	Notifies you when a deployment you requested fails to complete successfully and makes the environment unhealthy
Release	Release approval pending	Deployment approval pending	Notifies you when an approval for a deployment is pending on you
Work	Work item	A work item is moved from this project	Notifies you when the area path for a work item is moved to another project
Work	Work item	A work item assigned	Notifies you when you are assigned or unassigned a work item

Supported subscriptions

You can create subscriptions using the following templates for yourself, a team, or a group. Within the subscription dialog you can specify additional fields based on the category. To learn more, see [Manage personal notifications](#).

CATEGORY	TEMPLATE
Build	A build completes

CATEGORY	TEMPLATE
Build	A build fails
Build	A build controller or agent's status changes
Build	A build's quality changes
Code (Git)	A commit authored by me is pushed
Code (Git)	A commit is pushed by me
Code (Git)	A commit is pushed
Code (Git)	A pull request is created or updated
Code (TFVC)	Code is checked in
Code (TFVC)	Code is checked in with a policy override
Code (TFVC)	A file with a specific extension is checked in
Code (TFVC)	A file under a specific path is checked in
Code (TFVC)	A code review I am working on changes
Work	A work item I created is changed
Work	A work item assigned to me is changed
Work	A work item is changed
Work	A work item is assigned to me
Work	A work item is deleted
Work	A work item is restored
Extension management	An extension is modified
Release	An approval for a deployment is pending
Release	A deployment is completed
Release	A manual intervention for a deployment is pending

Related articles

- [About notifications](#)
- [Manage personal notifications](#)
- [Unsubscribe from a notification](#)

Supported event types

3/5/2019 • 2 minutes to read • [Edit Online](#)

Azure Boards | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

Learn the supported event types for notification subscriptions in Azure DevOps Services and Team Foundation Server (TFS) in the following table. Check out the [Events, subscriptions, and notifications concepts article](#) to learn more about events and event types.

CATEGORY	TYPE	FIELDS	ROLES
Build	Completed	Build controller Build reason Compilation status Definition name Requested by Requested for Status Team project Test status	Last changed by Requested by Requested for Deleted by
Build	Status changed	Changed by Changed time Quality Team project	
Code (Git)	Push	Authored by Branches updated Changes in folder Comment Committed by Pushed by Repository name Team project	Pushed by
Code (Git)	Pull request	Changed by Changes in folder Code under review Created by Event type Policy Bypass Repository name Reviewers Source branch name Status Target branch name Team project Vote	Creator Reviewers Changed reviewers Reset reviewers

CATEGORY	TYPE	FIELDS	ROLES	
Code (TFVC)	Check in	Associated work item Comment Committer File extension File name Folder path Policy override comment Server item Team project	Committer Owner	
Code (TFVC)	Code review	Area path Changed by Closing comment Comment My review status Requested by Review action Review context type Review owner Reviewed item file name Reviewed item parent path Reviewers State Team project Work item id	Requested by New reviewers Reviewers Declined reviewers	
Work item	Created Changed Deleted Restored	Any work item field	Assigned to (new) Assigned to (previous) Assigned to (current) Changed by Created by Authorized as	
Release	Release approval pending	Approval Type Assigned To Environment Name Release Definition Name	Assigned to Environment owner	
Release	Deployment completed	Deployment request reason Deployment requested for Deployment Status Environment Name Environment Owner Last Deployment Status Release Definition Name Release request reason Release requested by	Deployment requested for Environment owner Release requested by Approved by	

CATEGORY	TYPE	FIELDS	ROLES	
Release	Deployment pending	Environment Name Environment Owner Release Definition Name	Manual intervention recipient Environment owner	

Default permissions and access set for collaboration tools

5/8/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017

Collaboration tools encompass READMEs, team project Wikis, notifications, feedback, and semantic search.

Most of these tools are available to you if you're added as a team member or a member of the Contributors group for a team project. The most common built-in groups include Readers, Contributors, and Project Administrators. For a simplified view of all default permissions assigned to built-in groups, see [Default permissions and access](#).

Stakeholders have limited access to view charts and dashboards. To learn more, see [About access levels](#).

Task	Stakeholders	Readers	Contributors	Team Admins	Organization Owner/Project Admins
Set personal notifications or alerts	✓		✓	✓	✓
Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
READMEs	See Note 1	✓	✓	✓	✓
View Project Wikis	✓	✓	✓	✓	✓
View Code Wikis		✓	✓	✓	✓
Provision or create a Wiki					✓
Publish Code as Wiki			✓	See Note 2	See Note 2
View the project page	✓	✓	✓	✓	✓
Edit the project page					✓
Navigate using the Project pages	✓	✓	✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓
Powerful semantic code search	✓	✓	✓	✓	✓
Powerful semantic work tracking search	✓	✓	✓	✓	✓

Notes

1. Can view project READMEs, but not READMEs defined for a repository.
2. Project Admins or Team Admins with contribute permission can publish code as wiki. Project Admins have this permission by default.

TASK	STAKEHOLDERS	READERS	CONTRIBUTORS	TEAM ADMINS	ORGANIZATION OWNER/PROJECT ADMINS
Set personal notifications or alerts	✓		✓	✓	✓
Set team notifications or alerts				✓	✓
Set project-level notifications or alerts					✓
READMEs	See Note 1	✓	✓	✓	✓
View Project Wikis	✓	✓	✓	✓	✓
View Code Wikis		✓	✓	✓	✓
Provision or create a Wiki					✓
Publish Code as Wiki			✓	See Note 2	See Note 2
View the project page	✓	✓	✓	✓	✓
Edit the project page					✓
Navigate using the Project pages	✓	✓	✓	✓	✓
Request feedback		✓	✓	✓	✓
Provide feedback	✓	✓	✓	✓	✓
Powerful semantic code search	✓	✓	✓	✓	✓
Powerful semantic work tracking search	✓	✓	✓	✓	✓

Notes

1. Can view project READMEs, but not READMEs defined for a repository.
2. Project Admins or Team Admins with contribute permission can publish code as wiki. Project Admins have this permission by default.

Manage permissions

To manage permissions for a collaboration tool, see the following articles:

- [Manage README & Wiki permissions \(security\)](#)
- [Set feedback permissions](#)

To manage notifications, see the following articles:

- [Manage personal notifications](#)

- [Manage team notifications](#)

NOTE

There are no UI permissions associated with managing notifications. Instead, you can manage them using the [TFSecurity command line tool](#).

Related articles

- [Work across projects](#)
- [Add a team administrator](#)
- [Permissions and groups reference](#)

FAQs on notifications

3/5/2019 • 2 minutes to read • [Edit Online](#)

[Azure Boards](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

Can I receive emails in plain text?

No. This was supported in earlier versions of Azure DevOps Services and TFS, but all emails are now HTML formatted.

How can I avoid receiving any notifications for activity in an organization?

Because of custom subscriptions created by other users and admins, there is no way to completely avoid receiving any notifications, but you can do the following two actions to minimize the number you receive:

- Unsubscribe from all default and admin-created team and group subscriptions
- Disable or remove all custom subscriptions

Why do some emails have multiple recipients on the To line?

A default or team/group subscription can have multiple recipients depending on how it is configured. Assuming each of these recipients has permission to the resource the event is related to, the recipients are grouped together in one email.

Previously each recipient would receive their own individually-addressed email, which could result in the same user getting multiple emails because of their membership in multiple groups.

Related articles

- [About notifications](#)
- [Manage personal notifications](#)
- [Unsubscribe from a notification](#)

DevOps Settings

6/12/2019 • 2 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Most DevOps settings are made at the project-level. You configure agent and deployment pools, and parallel jobs for many projects at the organization or collection level. For a comprehensive index of all configurable settings, see [About user, team, project, and collection-level settings](#).

Pipelines (Build and Release)

- [Agent pools & queues](#)
- [Service endpoints](#)
- [Retention & limits](#)
- [Deployment pools & groups](#)

Repos (Code)

- [Create & manage Git repositories](#)
- [Manage Git branch policies](#)
- [Manage repository permissions](#)
- [Add TFVC Check-In Policies](#)

Test

- [Set test retention policies](#)

Audit

- [Access, export, and filter audit logs](#)

Agent pools

5/31/2019 • 10 minutes to read • [Edit Online](#)

Azure Pipelines | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

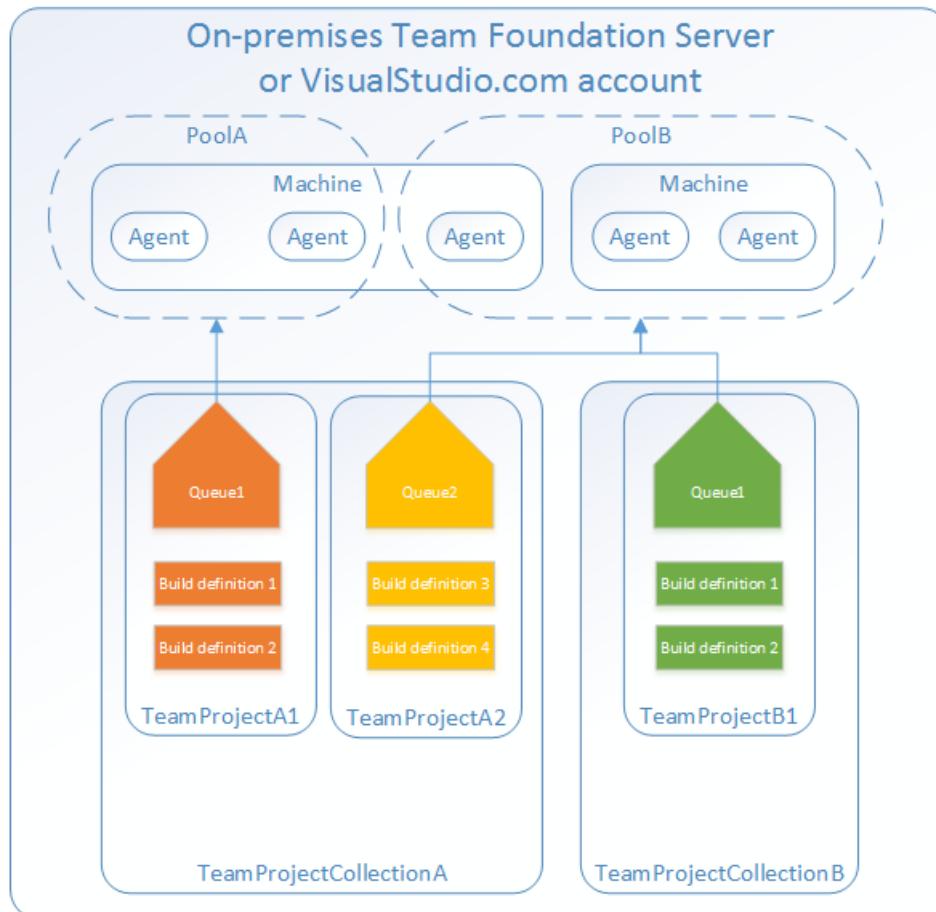
NOTE

In Microsoft Team Foundation Server (TFS) 2018 and previous versions, build and release *pipelines* are called *definitions*, *service connections* are called *service endpoints*, *stages* are called *environments*, and *jobs* are called *phases*.

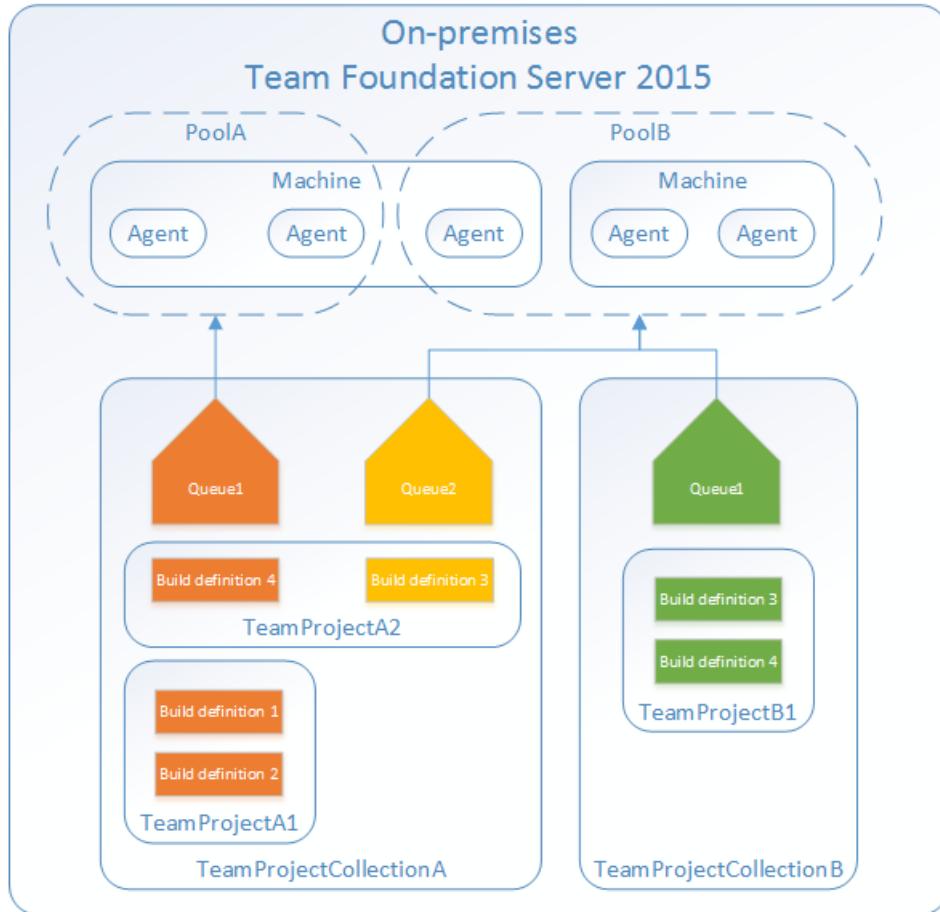
Instead of managing each **agent** individually, you organize agents into **agent pools**. In TFS, pools are scoped to the entire server; so you can share an agent pool across project collections and projects.

An **agent queue** provides access to an **agent pool** within a project. When you create a build or release pipeline, you specify which queue it uses. Queues are scoped to your project in TFS 2017 and newer, so you can only use them across build and release pipelines within a project.

To share an agent pool with multiple projects, in each of those projects, you create an agent queue pointing to the same agent pool. While multiple queues across projects can use the same agent pool, multiple queues within a project cannot use the agent pool. Also, each agent queue can use only one agent pool.



Agent pools are scoped to project collections.



Instead of managing each **agent** individually, you organize agents into **agent pools**. In Azure Pipelines, pools are scoped to the entire organization; so you can share the agent machines across projects. In Azure DevOps Server, agent pools are scoped to the entire server; so you can share the agent machines across projects and collections.

When you create a pipeline, you specify which pool it uses.

You create and manage agent pools from the agent pools tab in admin settings.

If you are an organization administrator, you create and manage agent pools from the agent pools tab in admin settings.

- Azure Pipelines: https://dev.azure.com/{your_organization}/_settings/agentpools
- Azure DevOps Server 2019: https://dev.azure.com/{your_collection}/_settings/agentpools
- TFS 2018: https://{your_server}/DefaultCollection/_admin/_AgentPool
- TFS 2017: https://{your_server}/tfs/DefaultCollection/_admin/_AgentPool
- TFS 2015: http://{your_server}:8080/tfs/_admin/_AgentPool
- That didn't work: [Get the correct URL](#)

You create and manage agent queues from the agent queues tab in project settings.

If you are a project team member, you create and manage agent pools from the agent pools tab in project settings.

- Azure Pipelines: https://dev.azure.com/{your_organization}/{project-name}/_admin/_AgentQueue
- Azure DevOps Server 2019: https://{your_server}/tfs/{collection-name}/{project-name}/_admin/_AgentQueue
- TFS 2018: https://{your_server}/tfs/{collection-name}/{project-name}/_admin/_AgentQueue
- TFS 2017: https://{your_server}/tfs/{collection-name}/{project-name}/_admin/_AgentQueue
- TFS 2015.3: http://{your_server}:8080/tfs/{collection-name}/_admin/_AgentQueue

- TFS 2015 RTM: http://{your_server}:8080/tfs/_admin/_buildQueue
- [The TFS URL doesn't work for me. How can I get the correct URL?](#)

Default agent pools

The following agent pools are provided by default:

- **Default** pool: Use it to register [self-hosted agents](#) that you've set up.
- **Hosted** pool with the following images:
 - **Ubuntu 1604**: Enables you to build and release on Ubuntu 1604 machines without having to configure a self-hosted Linux agent. Agents in this pool do not run in a container, but the Docker tools are available for you to use if you want to run [container jobs](#).
 - **macOS**: Enables you to build and release on Mojave macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored. [Learn more](#)
 - **macOS High Sierra**: Enables you to build and release on High Sierra macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored. [Learn more](#)
 - **Windows 2019 with VS2019**: These machines have Visual Studio 2019 installed on Windows Server 2019 operating system. For a complete list of software installed on these machines, see [Microsoft-hosted agents](#).
 - **VS2017**: These machines have Visual Studio 2017 installed on Windows Server 2016 operating system. For a complete list of software installed on these machines, see [Microsoft-hosted agents](#).
 - **Hosted**: These machines have older versions of Visual Studio installed on Windows Server 2012 R2 operating system. For a complete list of software installed on Microsoft-hosted agents, see [Microsoft-hosted agents](#).
 - **Windows Container**: Enables you to run jobs inside [Windows containers](#). Unless you're building using containers, Windows builds should run in the **Hosted Windows 2019**, **Hosted VS2017** or **Hosted** pools.

By default, all contributors in a project are members of the **User** role on hosted pools. This allows every contributor in a project to author and run pipelines using Microsoft-hosted pools.

Pools are used to run jobs. Learn about [specifying pools for jobs](#).

If you've got a lot of self-hosted agents intended for different teams or purposes, you might want to create additional pools as explained below.

Creating agent pools

Here are some typical situations when you might want to create self-hosted agent pools:

- You're a member of a project and you want to use a set of machines owned by your team for running build and deployment jobs. First, make sure you've the permissions to create pools in your project by selecting **Security** on the agent pools page in your project settings. You must have **Administrator** role to be able to create new pools. Next, select **Add pool** and select the option to create a **new** pool at the organization level. Finally [install](#) and configure agents to be part of that agent pool.
- You're a member of the infrastructure team and would like to set up a pool of agents for use in all projects. First make sure you're a member of a group in **All agent pools** with the **Administrator** role by navigating to agent pools page in your organization settings. Next create a **New agent pool** and select the option to **Auto-provision corresponding agent pools in all projects** while creating the pool. This

setting ensures all projects have access to this agent pool. Finally [install](#) and configure agents to be part of that agent pool.

- You want to share a set of agent machines with multiple projects, but not all of them. First, navigate to the settings for one of the projects, add an agent pool, and select the option to create a **new** pool at the organization level. Next, go to each of the other projects, and create a pool in each of them while selecting the option to **Use an existing agent pool from the organization**. Finally, [install](#) and configure agents to be part of the shared agent pool.
- You're a member of a project and you want to use a set of machines owned by your team for running build and deployment jobs. First, make sure you're a member of a group in **All Pools** with the **Administrator** role. Next create a **New project agent pool** in your project settings and select the option to **Create a new organization agent pool**. As a result, both an organization and project-level agent pool will be created. Finally [install](#) and configure agents to be part of that agent pool.
- You're a member of the infrastructure team and would like to set up a pool of agents for use in all projects. First make sure you're a member of a group in **All Pools** with the **Administrator** role. Next create a **New organization agent pool** in your admin settings and select the option to **Auto-provision corresponding project agent pools in all projects** while creating the pool. This setting ensures all projects have a pool pointing to the organization agent pool. The system creates a pool for existing projects, and in the future it will do so whenever a new project is created. Finally [install](#) and configure agents to be part of that agent pool.
- You want to share a set of agent machines with multiple projects, but not all of them. First create a project agent pool in one of the projects and select the option to **Create a new organization agent pool** while creating that pool. Next, go to each of the other projects, and create a pool in each of them while selecting the option to **Use an existing organization agent pool**. Finally, [install](#) and configure agents to be part of the shared agent pool.

Security of agent pools

Understanding how security works for agent pools helps you control sharing and use of agents.

Roles are defined on each agent pool, and **membership** in these roles governs what operations you can perform on an agent pool.

ROLE ON AN AGENT POOL IN ORGANIZATION SETTINGS	PURPOSE
Reader	Members of this role can view the agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health.
Service Account	Members of this role can use the organization agent pool to create a project agent pool in a project. If you follow the guidelines above for creating new project agent pools, you typically do not have to add any members here.
Administrator	In addition to all the above permissions, members of this role can register or unregister agents from the organization agent pool. They can also refer to the organization agent pool when creating a project agent pool in a project. Finally, they can also manage membership for all roles of the organization agent pool. The user that created the organization agent pool is automatically added to the Administrator role for that pool.

The **All agent pools** node in the Agent Pools tab is used to control the security of *all* organization agent pools.

Role memberships for individual organization agent pools are automatically inherited from those of the 'All agent pools' node. By default, TFS administrators are also administrators of the 'All agent pools' node.

Roles are also defined on each project agent pool, and memberships in these roles govern what operations you can perform on an agent pool at the project level.

ROLE ON A AGENT POOL IN PROJECT SETTINGS	PURPOSE
Reader	Members of this role can view the project agent pool. You typically use this to add operators that are responsible for monitoring the build and deployment jobs in that project agent pool.
User	Members of this role can use the project agent pool when authoring pipelines.
Administrator	In addition to all the above operations, members of this role can manage membership for all roles of the project agent pool. The user that created the pool is automatically added to the Administrator role for that pool.

The **All agent pools** node in the Agent pools tab is used to control the security of *all* project agent pools in a project. Role memberships for individual project agent pools are automatically inherited from those of the 'All agent pools' node. By default, the following groups are added to the Administrator role of 'All agent pools': Build Administrators, Release Administrators, Project Administrators.

The **Security** action in the Agent pools tab is used to control the security of *all* project agent pools in a project. Role memberships for individual project agent pools are automatically inherited from what you define here. By default, the following groups are added to the Administrator role of 'All agent pools': Build Administrators, Release Administrators, Project Administrators.

TFS 2015

In TFS 2015, special **groups** are defined on agent pools, and membership in these groups governs what operations you can perform.

Members of **Agent Pool Administrators** can register new agents in the pool and add additional users as administrators or service accounts.

Add people to the Agent Pool Administrators group to grant them permission manage all the agent pools. This enables people to create new pools and modify all existing pools. Members of Team Foundation Administrators group can also perform all these operations.

Users in the **Agent Pool Service Accounts** group have permission to listen to the message queue for the specific pool to receive work. In most cases you should not have to manage members of this group. The agent registration process takes care of it for you. The service account you specify for the agent (commonly Network Service) is automatically added when you register the agent.

Q & A

If I don't schedule a maintenance window, when will the agents run maintenance?

If no window is scheduled, then the agents in that pool will not run the maintenance job.

I'm trying to create a project agent pool that uses an existing organization agent pool, but the controls are grayed out. Why?

On the 'Create a project agent pool' dialog box, you can't use an existing organization agent pool if it is already referenced by another project agent pool. Each organization agent pool can be referenced by only one project agent pool within a given project collection.

I can't select a Microsoft-hosted pool and I can't queue my build. How do I fix this?

Ask the owner of your Azure DevOps organization to grant you permission to use the pool. See [Security of agent pools](#).

I need more hosted build resources. What can I do?

A: The Microsoft-hosted pools provide all Azure DevOps organizations with cloud-hosted build agents and free build minutes each month. If you need more Microsoft-hosted build resources, or need to run more jobs in parallel, then you can either:

- [Host your own agents on infrastructure that you manage.](#)
- [Buy additional parallel jobs.](#)

Service connections

7/3/2019 • 24 minutes to read • [Edit Online](#)

[Azure Pipelines](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#)

NOTE

In Microsoft Team Foundation Server (TFS) 2018 and previous versions, build and release *pipelines* are called *definitions*, *service connections* are called *service endpoints*, *stages* are called *environments*, and *jobs* are called *phases*.

You will typically need to connect to external and remote services to execute tasks in a job. For example, you may need to connect to your Microsoft Azure subscription, to a different build server or file server, to an online continuous integration environment, or to services you install on remote computers.

You can define service connections in Azure Pipelines or Team Foundation Server (TFS) that are available for use in all your tasks. For example, you can create a service connection for your Azure subscription and use this service connection name in an Azure Web Site Deployment task in a release pipeline.

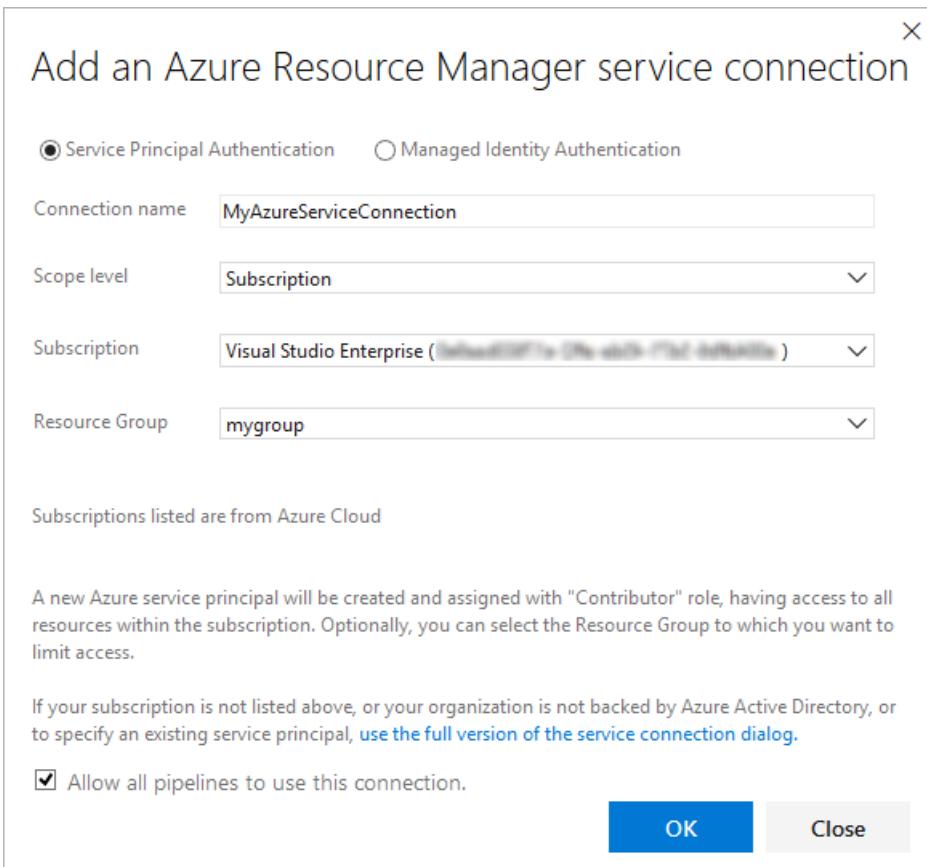
You define and manage service connections from the Admin settings of your project:

- Azure DevOps: https://dev.azure.com/{organization}/{project}/_admin/_services
- TFS: https://tfsserver/{collection}/{project}/_admin/_services

Service connections are created at project scope. A service connection created in one project is not visible in another project.

Create a service connection

1. In Azure DevOps, open the **Service connections** page from the [project settings page](#). In TFS, open the **Services** page from the "settings" icon in the top menu bar.
2. Choose **+ New service connection** and select the type of service connection you need.
3. Fill in the parameters for the service connection. The list of parameters differs for each type of service connection - see the [following list](#). For example, this is the default **Azure Resource Manager** connection dialog:



NOTE

The connection dialog may appear different for the different types of service connections, and have different parameters. See the list of parameters in [Common service connection types](#) for each service connection type.

4. Decide if you want the service connection to be accessible for any pipeline by setting the **Allow all pipelines to use this connection** option. This option allows pipelines defined in YAML, which are not automatically authorized for service connections, to use this service connection. See [Use a service connection](#).
5. Choose **OK** to create the connection.

For more information about Azure Resource Manager service connections, see [Connect to Microsoft Azure](#). You can also create your own [custom service connections](#).

Manage a service connection

1. In Azure DevOps, open the **Service connections** page from the [project settings page](#). Or, in TFS, open the **Services** page from the "settings" icon in the top menu bar.
2. Select the service connection you want to manage.
3. Choose from the list of **Actions** in the **Details** tab in the right pane.

The actions available depend on the chosen type of connection. You can update only some properties of connections; for example, to change the selected subscription you must re-create the connection. Choose **Disconnect** to delete or remove a connection.

Secure a service connection

You can control who can define new service connections in a library, and who can use an existing service

connection. **Roles** are defined for service connections, and **membership** in these roles governs the operations you can perform on those service connections.

ROLE ON A LIBRARY SERVICE CONNECTION	PURPOSE
User	Members of this role can use the service connection when authoring build or release pipelines.
Administrator	In addition to using the service connection, members of this role can manage membership of all other roles for the service connection. The user that created the service connection is automatically added to the Administrator role for that service connection.

Two special groups for service connections, endpoint administrators and creators, are added to every project. Members of the administrators group can manage all service connections. By default, project administrators are added as members of this group. This group is also added as an administrator to every service connection created. Members of the creators group can create new service connections. By default, project contributors are added as members of this group.

To modify the security for a connection:

1. In Azure DevOps, open the **Service connections** page from the [project settings page](#). In TFS, open the **Services** page from the "settings" icon in the top menu bar.
2. Choose the **Roles** link to open the security tab.

The screenshot shows the 'Service connections' page in Azure DevOps. On the left, there's a sidebar with 'New service connection' and a search bar. Below it are sections for 'Azure service' and 'Project2'. The main area is titled 'Service connection: Visual Studio'. It has tabs for 'Details' and 'Roles'. The 'Roles' tab is selected and highlighted with a red box. Below the tabs are buttons for 'Add', 'Edit', and 'Delete'. The table below lists users and their roles and access levels:

User	Role	Access
[Project]\Endpoint Administrators	Administrator	Inherited
SB	Administrator	Assigned

3. Add users or groups, turn on and off inheritance, or change the role for existing users and groups as required.

For more information about securing an Azure Resource Manager service connection, see [Connect to Microsoft Azure](#).

Use a service connection

After the new service connection is created:

- [YAML](#)
- [Classic](#)

Copy the connection name into your code as the **azureSubscription** (or the equivalent connection name) value.

```

25  displayName: dotnet build
26
27 - task: dotNetCoreCLI@1
28   inputs:
29     command: publish
30     arguments: --configuration release --output $(Build.ArtifactStagingDirectory)
31     zipAfterPublish: true
32   displayName: dotnet publish
33
34 - task: publishBuildArtifacts@1
35   inputs:
36     PathToPublish: $(Build.ArtifactStagingDirectory)
37     ArtifactName: drop
38     ArtifactType: Container
39   displayName: Publish the artifacts
40
41 - task: AzureRmWebAppDeployment@3
42   inputs:
43     azureSubscription: 'MyARMConnection'
44     WebAppName: 'MyWebApp'
45

```

Next you must authorize the service connection. To do this, or if you encounter a resource authorization error in your build, use one of the following techniques:

- If you want to authorize any pipeline to use the service connection, go to Azure Pipelines, open the Settings page, select Service connections, and enable the setting **Allow all pipelines to use this connection** option for the connection.
- If you want to authorize a service connection for a specific pipeline, open the pipeline by selecting **Edit** and queue a build manually. You will see a resource authorization error and a "Authorize resources" action on the error. Choose this action to explicitly add the pipeline as an authorized user of the service connection.

You can also create your own [custom service connections](#).

Common service connection types

Azure Pipelines and TFS support a variety of service connection types by default. Some of these are described below:

- [Azure Classic service connection](#)
- [Azure Resource Manager service connection](#)
- [Azure Service Bus service connection](#)
- [Bitbucket Cloud service connection](#)
- [Chef service connection](#)
- [Docker Host service connection](#)
- [Docker Registry service connection](#)
- [External Git service connection](#)
- [Generic service connection](#)
- [GitHub service connection](#)
- [GitHub Enterprise Server service connection](#)
- [Jenkins service connection](#)
- [Kubernetes service connection](#)
- [npm service connection](#)
- [NuGet service connection](#)
- [Python package download service connection](#)
- [Python package upload service connection](#)
- [Service Fabric service connection](#)

- [SSH service connection](#)
- [Subversion service connection](#)
- [Team Foundation Server / Azure Pipelines service connection](#)
- [Visual Studio App Center service connection](#)

After you enter the parameters when creating a service connection, validate the connection. The validation link uses a REST call to the external service with the information you entered, and indicates if the call succeeded.

Azure Classic service connection

Defines and secures a connection to a Microsoft Azure subscription using Azure credentials or an Azure management certificate. [How do I create a new service connection?](#)

PARAMETER	DESCRIPTION
[authentication type]	Required. Select Credentials or Certificate based .
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Environment	Required. Select Azure Cloud , Azure Stack , or one of the pre-defined Azure Government Clouds where your subscription is defined.
Subscription ID	Required. The GUID-like identifier for your Azure subscription (not the subscription name). You can copy this from the Azure portal.
Subscription Name	Required. The name of your Microsoft Azure subscription (account).
User name	Required for Credentials authentication. User name of a work or school account (for example @fabrikam.com). Microsoft accounts (for example @live or @hotmail) are not supported.
Password	Required for Credentials authentication. Password for the user specified above.
Management Certificate	Required for Certificate based authentication. Copy the value of the management certificate key from your publish settings XML file or the Azure portal.

If your subscription is defined in an [Azure Government Cloud](#), ensure your application meets the relevant compliance requirements before you configure a service connection.

Azure Resource Manager service connection

Defines and secures a connection to a Microsoft Azure subscription using Service Principal Authentication (SPA) or an Azure Managed Service Identity. The dialog offers two main modes:

- **Automated subscription detection.** In this mode, Azure Pipelines and TFS will attempt to query Azure for all of the subscriptions and instances to which you have access using the credentials you are currently logged on with in Azure Pipelines or TFS (including Microsoft accounts and School or Work accounts). If no subscriptions are shown, or subscriptions other than the one you want to use, you must sign out of

Azure Pipelines or TFS and sign in again using the appropriate account credentials.

- **Manual subscription pipeline.** In this mode, you must specify the service principal you want to use to connect to Azure. The service principal specifies the resources and the access levels that will be available over the connection. Use this approach when you need to connect to an Azure account using different credentials from those you are currently logged on with in Azure Pipelines or TFS. This is also a useful way to maximize security and limit access.

For more information, see [Connect to Microsoft Azure](#)

NOTE: If you don't see any Azure subscriptions or instances, or you have problems validating the connection, see [Troubleshoot Azure Resource Manager service connections](#).

Azure Service Bus service connection

Defines and secures a connection to a Microsoft Azure Service Bus queue.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Service Bus ConnectionString	The URL of your Azure Service Bus instance. More information .
Service Bus Queue Name	The name of an existing Azure Service Bus queue.

[How do I create a new service connection?](#)

Bitbucket Cloud service connection

Defines a connection to Bitbucket Cloud.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
User name	Required. The username to connect to the service.
Password	Required. The password for the specified username.

[How do I create a new service connection?](#)

Chef service connection

Defines and secures a connection to a [Chef](#) automation server.

PARAMETER	DESCRIPTION
-----------	-------------

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Server URL	Required. The URL of the Chef automation server.
Node Name (Username)	Required. The name of the node to connect to. Typically this is your username.
Client Key	Required. The key specified in the Chef .pem file.

[How do I create a new service connection?](#)

Docker Host service connection

Defines and secures a connection to a Docker host.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Server URL	Required. The URL of the Docker host.
CA Certificate	Required. A trusted certificate authority certificate to use to authenticate with the host.
Certificate	Required. A client certificate to use to authenticate with the host.
Key	Required. The key specified in the Docker key.pem file.

Ensure you protect your connection to the Docker host. [Learn more](#).

[How do I create a new service connection?](#)

Docker Registry service connection

Defines a connection to a container registry.

Azure Container Registry

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task inputs.
Azure subscription	Required. The Azure subscription containing the container registry to be used for service connection creation.

PARAMETER	DESCRIPTION
Azure Container Registry	Required. The Azure Container Registry to be used for creation of service connection.

Docker Hub or Others

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task inputs.
Docker Registry	Required. The URL of the Docker registry.
Docker ID	Required. The identifier of the Docker account user.
Password	Required. The password for the account user identified above.
Email	Optional. An email address to receive notifications.

[How do I create a new service connection?](#)

External Git service connection

Defines and secures a connection to a Git repository server. Note that there is a specific service connection for [GitHub](#) and [GitHub Enterprise Server](#) connections.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Server URL	Required. The URL of the Git repository server.
User name	Required. The username to connect to the Git repository server.
Password/Token Key	Required. The password or access token for the specified username.

Also see [Artifact sources](#).

[How do I create a new service connection?](#)

Generic service connection

Defines and secures a connection to any other type of service or application.

PARAMETER	DESCRIPTION

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Server URL	Required. The URL of the service.
User name	Required. The username to connect to the service.
Password/Token Key	Required. The password or access token for the specified username.

[How do I create a new service connection?](#)

GitHub service connection

Defines a connection to a GitHub repository. Note that there is a specific service connection for [External Git servers](#) and [GitHub Enterprise Server](#) connections.

PARAMETER	DESCRIPTION
Choose authorization	Required. Either Grant authorization or Personal access token . See notes below.
Token	Required for Personal access token authorization. See notes below.
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.

[How do I create a new service connection?](#)

NOTE

If you select **Grant authorization** for the **Choose authorization** option, the dialog shows an **Authorize** button that opens the GitHub login page. If you select **Personal access token** you must obtain a suitable token and paste it into the **Token** textbox. The dialog shows the recommended scopes for the token: **repo, user, admin:repo_hook**. See [this page](#) on GitHub for information about obtaining an access token. Then register your GitHub account in your profile:

- Open your profile from your organization name at the right of the Azure Pipelines page heading.
- At the top of the left column, under **DETAILS**, choose **Security**.
- In the **Security** tab, in the right column, choose **Personal access tokens**.
- Choose the **Add** link and enter the information required to create the token.

Also see [Artifact sources](#).

GitHub Enterprise Server service connection

Defines a connection to a GitHub repository. Note that there is a specific service connection for [External Git servers](#) and [standard GitHub service connections](#).

PARAMETER	DESCRIPTION
Choose authorization	Required. Either Personal access token , Username and Password , or OAuth2 . See notes below.
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Server URL	Required. The URL of the service.
Accept untrusted SSL certificates	Set this option to allow clients to accept a self-signed certificate instead of installing the certificate in the TFS service role or the computers hosting the agent .
Token	Required for Personal access token authorization. See notes below.
User name	Required for Username and Password authentication. The username to connect to the service.
Password	Required for Username and Password authentication. The password for the specified username.
OAuth configuration	Required for OAuth2 authorization. The OAuth configuration specified in your account.
GitHub Enterprise Server configuration URL	The URL is fetched from OAuth configuration.

How do I create a new service connection?

NOTE

If you select **Personal access token** you must obtain a suitable token and paste it into the **Token** textbox. The dialog shows the recommended scopes for the token: **repo**, **user**, **admin:repo_hook**. See [this page](#) on GitHub for information about obtaining an access token. Then register your GitHub account in your profile:

- Open your profile from your account name at the right of the Azure Pipelines page heading.
- At the top of the left column, under **DETAILS**, choose **Security**.
- In the **Security** tab, in the right column, choose **Personal access tokens**.
- Choose the **Add** link and enter the information required to create the token.

Jenkins service connection

Defines a connection to the Jenkins service.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.

PARAMETER	DESCRIPTION
Server URL	Required. The URL of the service.
Accept untrusted SSL certificates	Set this option to allow clients to accept a self-signed certificate instead of installing the certificate in the TFS service role or the computers hosting the agent .
User name	Required. The username to connect to the service.
Password	Required. The password for the specified username.

[How do I create a new service connection?](#)

Also see [Azure Pipelines Integration with Jenkins](#) and [Artifact sources](#).

Kubernetes service connection

Defines a connection to a Kubernetes cluster.

Azure subscription option

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task inputs.
Azure subscription	Required. The Azure subscription containing the cluster to be used for service connection creation.
Cluster	Name of the Azure Kubernetes Service cluster.
Namespace	Namespace within the cluster.

For an RBAC enabled cluster, a ServiceAccount is created in the chosen namespace along with RoleBinding object so that the created ServiceAccount is able to perform actions only on the chosen namespace.

For an RBAC disabled cluster, a ServiceAccount is created in the chosen namespace. But the created ServiceAccount has cluster-wide privileges (across namespaces).

Service account option

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task inputs.
Server URL	Required. Cluster's API server URL.
Token	Token used for authentication.
Certificate	Used for verifying the serving certificate of the API server.

The following command can be used to fetch Server URL -

```
kubectl config view --minify -o jsonpath='{.clusters[0].cluster.server}'
```

Use the following sequence of commands (substituting the appropriate values in <>) to locate token and certificate -

Fetch the name of the secret associated with the service

```
kubectl get serviceaccounts <service-account-name> -n <namespace> -o jsonpath='{.secrets[0].name}'
```

Use the output value of the above command, the secret-name, in these commands -

For token:

```
kubectl get secret <secret-name> -n <namespace> -o jsonpath='{.data.token}'
```

For certificate:

```
kubectl get secret <secret-name> -n <namespace> -o jsonpath='{.data.ca\.crt}'
```

Kubeconfig option

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task inputs.
Kubeconfig	Required. Contents of the kubeconfig file
Context	Context within the kubeconfig file that is to be used for identifying the cluster

[How do I create a new service connection?](#)

npm service connection

Defines and secures a connection to an npm server.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Registry URL	Required. The URL of the npm server.
Username	Required when connection type is Username and Password . The username for authentication.
Password	Required when connection type is Username and Password . The password for the username.

PARAMETER	DESCRIPTION
Personal Access Token	Required when connection type is External Azure Pipelines . The token to use to authenticate with the service. Learn more .

[How do I create a new service connection?](#)

NuGet service connection

Defines and secures a connection to a NuGet server.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Feed URL	Required. The URL of the NuGet server.
ApiKey	Required when connection type is ApiKey . The authentication key.
Personal Access Token	Required when connection type is External Azure Pipelines . The token to use to authenticate with the service. Learn more .
Username	Required when connection type is Basic authentication . The username for authentication.
Password	Required when connection type is Basic authentication . The password for the username.

[How do I create a new service connection?](#)

Python package download service connection

Defines and secures a connection to a Python repository for downloading Python packages.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Python repository url for download	Required. The URL of the Python repository.
Personal Access Token	Required when connection type is Authentication Token . The token to use to authenticate with the service. Learn more .
Username	Required when connection type is Username and Password . The username for authentication.

PARAMETER	DESCRIPTION
Password	Required when connection type is Username and Password . The password for the username.

[How do I create a new service connection?](#)

Python package upload service connection

Defines and secures a connection to a Python repository for uploading Python packages.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Python repository url for upload	Required. The URL of the Python repository.
EndpointName	Required. Unique repository name used for twine upload. Spaces and special characters are not allowed.
Personal Access Token	Required when connection type is Authentication Token . The token to use to authenticate with the service. Learn more .
Username	Required when connection type is Username and Password . The username for authentication.
Password	Required when connection type is Username and Password . The password for the username.

[How do I create a new service connection?](#)

Service Fabric service connection

Defines and secures a connection to a Service Fabric cluster.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Cluster Endpoint	Required. The TCP endpoint of the cluster.
Server Certificate Thumbprint	Required when connection type is Certificate based or Azure Active Directory .
Client Certificate	Required when connection type is Certificate based .
Password	Required when connection type is Certificate based . The certificate password.

PARAMETER	DESCRIPTION
Username	Required when connection type is Azure Active Directory . The username for authentication.
Password	Required when connection type is Azure Active Directory . The password for the username.
Use Windows security	Required when connection type is Others .
Cluster SPN	Required when connection type is Others and using Windows security.

[How do I create a new service connection?](#)

SSH service connection

Defines and secures a connection to a remote host using Secure Shell (SSH).

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Host name	Required. The name of the remote host machine or the IP address.
Port number	Required. The port number of the remote host machine to which you want to connect. The default is port 22.
User name	Required. The username to use when connecting to the remote host machine.
Password or passphrase	The password or passphrase for the specified username if using a keypair as credentials.
Private key	The entire contents of the private key file if using this type of authentication.

[How do I create a new service connection?](#)

Also see [SSH task](#) and [Copy Files Over SSH](#).

Subversion service connection

Defines and secures a connection to the Subversion repository.

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.

PARAMETER	DESCRIPTION
Server repository URL	Required. The URL of the repository.
Accept untrusted SSL certificates	Set this option to allow the client to accept self-signed certificates installed on the agent computer(s).
Realm name	Optional. If you use multiple credentials in a build or release pipeline, use this parameter to specify the realm containing the credentials specified for this service connection.
User name	Required. The username to connect to the service.
Password	Required. The password for the specified username.

[How do I create a new service connection?](#)

Team Foundation Server / Azure Pipelines service connection

Defines and secures a connection to another TFS or Azure DevOps organization.

PARAMETER	DESCRIPTION
(authentication)	Select Basic or Token Based authentication.
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
Connection URL	Required. The URL of the TFS or Azure Pipelines instance.
User name	Required for Basic authentication. The username to connect to the service.
Password	Required for Basic authentication. The password for the specified username.
Personal Access Token	Required for Token Based authentication (TFS 2017 and newer and Azure Pipelines only). The token to use to authenticate with the service. Learn more .

[How do I create a new service connection?](#)

Use the **Verify connection** link to validate your connection information.

See also [Authenticate access with personal access tokens for Azure DevOps and TFS](#).

Visual Studio App Center service connection

Defines and secures a connection to Visual Studio App Center.

PARAMETER	DESCRIPTION

PARAMETER	DESCRIPTION
Connection Name	Required. The name you will use to refer to this service connection in task properties. This is not the name of your Azure account or subscription. If you are using YAML, use this name as the azureSubscription or the equivalent subscription name value in the script.
API Token	Required. The token to use to authenticate with the service. Learn more .

[How do I create a new service connection?](#)

Extensions for other service connections

Other service connection types and tasks can be installed in Azure Pipelines and Team Foundation Server as extensions. Some examples of service connections currently available through extensions are:

- [TFS artifacts for Azure Pipelines](#). Deploy on-premises TFS builds with Azure Pipelines through a TFS service connection connection and the **Team Build (external)** artifact, even when the TFS machine is not reachable directly from Azure Pipelines. For more information, see [External TFS](#) and [this blog post](#).
- [TeamCity artifacts for Azure Pipelines](#). This extension provides integration with TeamCity through a TeamCity service connection, enabling artifacts produced in TeamCity to be deployed by using Azure Pipelines. See [TeamCity](#) for more details.
- [SCVMM Integration](#). Connect to a System Center Virtual Machine Manager (SCVMM) server to easily provision virtual machines and perform actions on them such as managing checkpoints, starting and stopping VMs, and running PowerShell scripts.
- [VMware Resource Deployment](#). Connect to a VMware vCenter Server from Visual Studio Team Services or Team Foundation Server to provision, start, stop, or snapshot VMware virtual machines.

You can also create your own [custom service connections](#).

Help and support

- See our [troubleshooting](#) page.
- Report any problems on [Developer Community](#), get advice on [Stack Overflow](#), and get support via our [Support](#) page.

Build and release retention policies

5/31/2019 • 8 minutes to read • [Edit Online](#)

[Azure Pipelines](#) | [TFS 2018](#) | [TFS 2017](#) | [TFS 2015](#) | [Previous versions \(XAML builds\)](#)

NOTE

In Microsoft Team Foundation Server (TFS) 2018 and previous versions, build and release *pipelines* are called *definitions*, *service connections* are called *service endpoints*, *stages* are called *environments*, and *jobs* are called *phases*.

Retention policies are used to configure how long builds and releases are to be retained by the system. The primary reasons to delete older builds and releases are to conserve storage and to reduce clutter. The main reasons to keep builds and releases are for audit and tracking.

Build retention

In most cases you don't need to retain completed builds longer than a certain number of days. Using build retention policies, you can control **how many days** you want to keep each build before deleting it and the **minimum number of builds** that should be retained for each pipeline.

As an author of a build pipeline, you can customize retention policies for builds of your pipeline on the **Retention** tab. You can also customize these policies on a branch-by-branch basis if you are building from [Git repositories](#).

Global build retention policy

If you are using an on-premises Team Foundation Server, you can specify build retention policy defaults and maximums for a project collection. You can also specify when builds are permanently destroyed (removed from the **Deleted** tab in the build explorer).

If you are using Azure Pipelines, you can view but not change these settings for your organization.

Global build retention policy settings can be managed from the **Pipelines** settings of your organization or project collection:

- Azure Pipelines: https://dev.azure.com/{your_organization}/_admin/_buildQueue
- TFS 2017 and newer: https://{your_server}/tfs/DefaultCollection/_admin/_buildQueue
- TFS 2015.3: http://{your_server}:8080/tfs/DefaultCollection/_admin/_buildQueue
- TFS 2015 RTM: http://{your_server}:8080/tfs/DefaultCollection/_admin/_buildQueue#a=settings

The **maximum retention policy** sets the upper limit for how long builds can be retained for all build pipelines. Authors of build pipelines cannot configure settings for their definitions beyond the values specified here.

The **default retention policy** sets the default retention values for all the build pipelines. Authors of build pipelines can override these values.

The **build destruction policy** helps you keep the builds for a certain period of time after they are deleted. This policy cannot be overridden in individual build pipelines.

Git repositories

If your [repository type](#) is one of the following, you can define multiple retention policies with branch filters:

- Azure Repos Git or TFS Git
- GitHub
- Other/external Git

For example, your team may want to keep:

- User branch builds for five days, with a minimum of a single successful or partially successful build for each branch.
- Master and feature branch builds for 10 days, with a minimum of three successful or partially successful builds for each of these branches. You exclude a special feature branch that you want to keep for a longer period of time.
- Builds from the special feature branch and all other branches for 15 days, with a minimum of a single successful or partially successful build for each branch.

The following example retention policy for a build pipeline meets the above requirements:

The screenshot shows the 'Retention' tab in the 'Builds' section of the Azure DevOps interface. There are three defined rules:

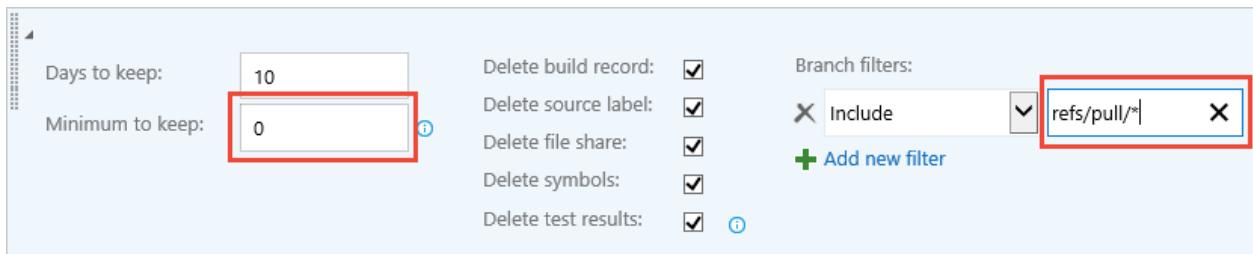
- Rule 1 (Top):** Days to keep: 5, Minimum to keep: 1. Delete build record: checked. Delete source label: checked. Delete test results: checked. Branch filters: Include users/*.
- Rule 2 (Middle):** Days to keep: 10, Minimum to keep: 3. Delete build record: checked. Delete source label: checked. Delete test results: checked. Branch filters: Include master, Include features/*, Exclude features/special.
- Rule 3 (Bottom):** Days to keep: 15, Minimum to keep: 1. Delete build record: checked. Delete source label: checked. Delete test results: checked. Branch filters: Include *.

When specifying custom policies for each pipeline, you cannot exceed the maximum limits set by administrator.

Clean up pull request builds

If you [protect your Git branches with pull request builds](#), then you can use retention policies to automatically delete the completed builds. To do it, add a policy that keeps a minimum of builds with the following branch filter:

```
refs/pull/*
```



TFVC and Subversion repositories

For TFVC and Subversion [repository types](#) you can modify a single policy with the same options shown above.

Policy order

When the system is purging old builds, it evaluates each build against the policies in the order you have specified. You can drag and drop a policy lower or higher in the list to change this order.

The "All" branches policy is automatically added as the last policy in the evaluation order to enforce the maximum limits for all other branches.

<input checked="" type="checkbox"/> Days to keep: 30 Minimum to keep: 10	Delete build record: true Delete source label: true Delete test results: true	Branch filters: All
---	---	---------------------

What parts of the build get deleted

When the retention policies mark a build for deletion, you can control which information related to the build is deleted:

- Build record: You can choose to delete the entire build record or keep basic information about the build even after the build is deleted.
- Source label: If you label sources as part of the build, then you can choose to delete the tag (for Git) or the label (for TFVC) created by a build.
- Automated test results: You can choose to delete the automated test results associated with the build (for example, results published by the Publish Test Results build task).

The following information is deleted when a build is deleted:

- Logs
- [Published artifacts](#)
- [Published symbols](#)

When are builds deleted

Azure Pipelines

Your retention policies are processed once per day. The timing of this process varies because we spread the work throughout the day for load balancing purposes. There is no option to change this process.

TFS

Your retention policies run every day at 3:00 A.M. UTC. There is no option to change this process.

Release retention

The release retention policies for a release pipeline determine how long a release and the build linked to it are retained. Using these policies, you can control **how many days** you want to keep each release after it has been last modified or deployed and the **minimum number of releases** that should be retained for each pipeline. The retention timer on a release is reset every time a release is modified or deployed to a stage. The minimum number of releases to retain setting takes precedence over the number of days. For example, if you specify to retain a minimum of three releases, the most recent three will be retained indefinitely - irrespective of the number of days specified. However, you can manually delete these releases when you no longer require them.

As an author of a release pipeline, you can customize retention policies for releases of your pipeline on the **Retention** tab. You can also customize these policies on a [stage-by-stage basis](#).

Global release retention policy

If you are using an on-premises Team Foundation Server, you can specify release retention policy defaults and maximums for a project. You can also specify when releases are permanently destroyed (removed from the **Deleted** tab in the build explorer).

If you are using Azure Pipelines, you can view but not change these settings for your project.

Global release retention policy settings can be managed from the **Release** settings of your project:

- Azure Pipelines:

```
https://dev.azure.com/{your_organization}/{project}/_admin/_apps/hub/ms.vss-releaseManagement-web.release-project-admin-hub
```

- On-premises:

```
https://{your_server}/tfs/{collection_name}/{project}/_admin/_apps/hub/ms.vss-releaseManagement-web.release-project-admin-hub
```

The **maximum retention policy** sets the upper limit for how long releases can be retained for all release pipelines. Authors of release pipelines cannot configure settings for their definitions beyond the values specified here.

The **default retention policy** sets the default retention values for all the release pipelines. Authors of build pipelines can override these values.

The **destruction policy** helps you keep the releases for a certain period of time after they are deleted. This policy cannot be overridden in individual release pipelines.

In TFS, release retention management is restricted to specifying the number of days, and this is available only in TFS 2015.3 and newer.

Stage-specific retention

You may want to retain more releases that have been deployed to specific stages. For example, your team may want to keep:

- Releases deployed to Production stage for 60 days, with a minimum of three last deployed releases.
- Releases deployed to Pre-production stage for 15 days, with a minimum of one last deployed release.
- Releases deployed to QA stage for 30 days, with a minimum of two last deployed releases.
- Releases deployed to Dev stage for 10 days, with a minimum of one last deployed release.

The following example retention policy for a release pipeline meets the above requirements:

The screenshot shows the 'Retention' tab selected in the top navigation bar of the TFS interface. On the left, there are three stages: 'Dev', 'Production', and 'QA', each with its own retention policy. The 'Dev' stage is highlighted with a blue background and contains the text 'Keep for 30 days, 3 good releases and keep artifacts.' To the right, under 'Settings for Dev', there are configuration options: 'Days to retain a release *' set to 30, 'Minimum releases to keep *' set to 3, and a checked checkbox for 'Retain associated artifacts'. A link 'View or manage retention policy defaults.' is also present.

In this example, if a release that is deployed to Dev is not promoted to QA for 10 days, it is a potential candidate for deletion. However, if that same release is deployed to QA eight days after being deployed to Dev, its retention timer is reset, and it is retained in the system for another 30 days.

When specifying custom policies per pipeline, you cannot exceed the maximum limits set by administrator.

Interaction between build and release retention

The build linked to a release has its own retention policy, which may be shorter than that of the release. If you want to retain the build for the same period as the release, set the **Retain build** checkbox for the appropriate stages. This overrides the retention policy for the build, and ensures that the artifacts are available if you need to redeploy that release.

When you delete a release pipeline, delete a release, or when the retention policy deletes a release automatically, the retention policy for the associated build will determine when that build is deleted.

In TFS, interaction between build and release retention is available in TFS 2017 and newer.

Q&A

Are manual test results deleted?

No

If I mark a build or a release to be retained indefinitely, does the retention policy still apply?

No. Neither the pipeline's retention policy nor the maximum limits set by the administrator are applied when you mark an individual build or release to be retained indefinitely. It will remain until you stop retaining it indefinitely.

How do I specify that builds deployed to production will be retained longer?

Customize the retention policy on the release pipeline. Specify the number of days that releases deployed to production must be retained. In addition, indicate that builds associated with that release are to be retained. This will override the build retention policy.

I did not mark builds to be retained indefinitely. However, I see a large number of builds being retained. How can I prevent this?

Builds that are deployed as part of releases are also governed by the release retention policy. Customize the release retention policy as explained above.

Are automated test results that are published as part of a release retained until the release is deleted?

Test results published within a stage of a release are associated with both the release and the build. These test results are retained as specified by the retention policy configured for the build and for the test results. If you are

not deploying Team Foundation or Azure Pipelines Build, and are still publishing test results, the retention of these results is governed by the retention settings of the release they belong to.

Deployment groups

4/27/2019 • 4 minutes to read • [Edit Online](#)

[Azure Pipelines](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#)

NOTE

In Microsoft Team Foundation Server (TFS) 2018 and previous versions, build and release *pipelines* are called *definitions*, *service connections* are called *service endpoints*, *stages* are called *environments*, and *jobs* are called *phases*.

A deployment group is a logical set of deployment target machines that have agents installed on each one. Deployment groups represent the physical environments; for example, "Dev", "Test", "UAT", and "Production". In effect, a deployment group is just another grouping of agents, much like an [agent pool](#).

When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a [job](#) using a deployment group. This makes it easy to define [parallel execution](#) of deployment tasks.

Deployment groups:

- Specify the security context and runtime targets for the agents. As you create a deployment group, you add users and give them appropriate permissions to administer, manage, view, and use the group.
- Let you view live logs for each server as a deployment takes place, and download logs for all servers to track your deployments down to individual machines.
- Enable you to use machine tags to limit deployment to specific sets of target servers.

Create a deployment group

You define groups on the **Deployment Groups** tab of the **Azure Pipelines** section, and install the agent on each server in the group. After you prepare your target servers, they appear in the **Deployment Groups** tab. The list indicates if a server is available, the tags you assigned to each server, and the latest deployment to each server.

The tags you assign allow you to limit deployment to specific servers when the deployment group is used in a [Deployment group job](#). Tags are each limited to 256 characters, but there is no limit to the number of tags you can use. You manage the security for a deployment group by [assigning security roles](#).

Deploy agents to a deployment group

Every target machine in the deployment group requires the build and release agent to be installed. You can do this using the script that is generated in the **Deployment Groups** tab of **Azure Pipelines**. You can choose the type of agent to suit the target operating system and platform; such as Windows and Linux.

If the target machines are Azure VMs, you can quickly and easily prepare them by installing the **Azure Pipelines Agent** Azure VM extension on each of the VMs, or by using the **Azure Resource Group Deployment** task in your release pipeline to create a deployment group dynamically.

You can force the agents on the target machines to be upgraded to the latest version without needing to redeploy them by choosing the **Upgrade targets** command on the shortcut menu for a deployment group.

For more information, see [Provision agents for deployment groups](#).

Monitor releases for deployment groups

When release is executing, you see an entry in the live logs page for each server in the deployment group. After a release has completed, you can download the log files for every server to examine the deployments and resolve issues. To navigate quickly to a release pipeline or a release, use the links in the **Releases** tab.

Share a deployment group

Each deployment group is a member of a **deployment pool**, and you can share the deployment pool and groups across projects provided that:

- The user sharing the deployment pool has [User permission](#) for the pool containing the group.
- The user sharing the deployment pool has permission to create a deployment group in the project where it is being shared.
- The project does not already contain a deployment group that is a member of the same deployment pool.

The tags you assign to each machine in the pool are scoped at project level, so you can specify a different tag for the same machine in each deployment group.

Add a deployment pool and group to another project

To manage a deployment pool, or to add an existing deployment pool and the groups it contains to another project, choose the **Manage** link in the **Agent Pool** section of the **Deployment Group** page. In the **Deployment Pools** page, select the projects for which you want the deployment group to be available, then save the changes.

When you navigate to the **Deployment Groups** page in the target project(s), you will see the deployment group you added and you can assign project-specific machine tags as required.

Create a new deployment pool

You can add a new deployment pool, share it amongst your projects, and then add deployment groups to it. In the **Deployment Pools** page, choose **+ New**. In the **New deployment pool** panel, enter a name for the pool and then select the projects for which you want it to be available.

When you navigate to the **Deployment Groups** page in the target project(s), you will see the deployment group you added and you can assign project-specific machine tags as required.

Related topics

- [Run on machine group job](#)
- [Deploy an agent on Windows](#)
- [Deploy an agent on macOS](#)
- [Deploy an agent on Linux](#)

Help and support

- See our [troubleshooting](#) page.
- Report any problems on [Developer Community](#), get advice on [Stack Overflow](#), and get support via our [Support](#) page.

2 minutes to read

2 minutes to read

Set repository permissions for Git or TFVC

6/26/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

By default, members of the project Contributors group have permissions to contribute to a repository. However, to create and manage permissions for a repository, you must be a member of the Project Administrators group. You can grant or restrict access to a repository by setting the permission state to **Allow** or **Deny** for a single user or a security group.

Prerequisites

- You must have a project. If you don't have a project yet, create one in [Azure DevOps](#) or set one up in an [on-premises TFS](#).
- You must be a member of the [Project Administrators Group](#) or have your **Manage permissions** set to **Allow** for Git repositories or the TFVC repository.

Default repository permissions

To contribute to the source code, you must be granted **Basic** access level or greater. Users granted **Stakeholder** access for private projects have no access to source code. Users granted **Stakeholder** access for public projects have the same access as Contributors and those granted **Basic** access. To learn more, see [About access levels](#).

To contribute to the source code, you must be granted **Basic** access level or greater. Users granted **Stakeholder** access have no access to source code. To learn more, see [About access levels](#).

For a description of each security group and permission level, see [Permissions and group reference](#).

Git

You can use Git repositories to host and collaborate on your source code. For an overview of code features and functions, see [Git](#).

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

Task	Readers	Contributors	Build Admins	Project Admins
Clone, fetch, contribute to pull requests, and explore the contents of a repository	✓	✓	✓	✓
Contribute to a repository, create branches, create tags, manage notes		✓	✓	✓
Create, delete, and rename repositories				✓
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) (<i>not set for any security group</i>)				
---	--	--	--	--

Set permissions across all Git repositories by making changes to the top-level **Git repositories** entry. Individual repositories inherit permissions from the top-level **Git Repositories** entry. Branches inherit a subset of permissions from assignments made at the repository level. For branch permissions and policies, see [Set branch permissions](#) and [Improve code quality with branch policies](#).

By default, the project-level Readers groups have read-only permissions.

TASK	CONTRIBUTOR S	BUILD ADMINS	PROJECT ADMINS
Branch Creation: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓
Contribute: At the repository level, can push their changes to branches in the repository. Does not override restrictions in place from branch policies . At the branch level, can push their changes to the branch and lock the branch.	✓	✓	✓
Note Management: Can push and edit Git notes to the repository. They can also remove notes from items if they have the Force permission.	✓	✓	✓
Tag Creation: Can push tags to the repository, and can also edit or remove tags if they have the Force permission.	✓	✓	✓
Administer: Delete and rename repositories If assigned to the top-level Git repositories entry, can add additional repositories. At the branch level, users can set permissions for the branch and unlock the branch. The Administer permission set on an individual Git repository does not grant the ability to rename or delete the repository. These tasks require Administer permissions at the top-level Git repositories entry.			✓
Rewrite and destroy history (force push): Can force an update to a branch and delete a branch. A force update can overwrite commits added from any user. Users with this permission can modify the commit history of a branch.			✓

The Project Collection Build Service can read from all repositories by default. Any pipeline which runs with project collection scope can potentially read any repository in the organization/collection. You can remove this permission for a repository: set "Read" to "Deny" for the Project Collection Build Service.

TFVC

[Team Foundation Version Control \(TFVC\)](#) provides a centralized version control system to manage your source control.

TASK	READERS	CONTRIBUTOR S	BUILD ADMINS	PROJECT ADMINS

Contribute to a centralized version control, including Code Review (Check in, label, lock, merge, pend a change)	Read only	✓	✓	✓
Check in, revise, undo, or unlock other users' changes				✓
Manage branches, manage permissions				✓

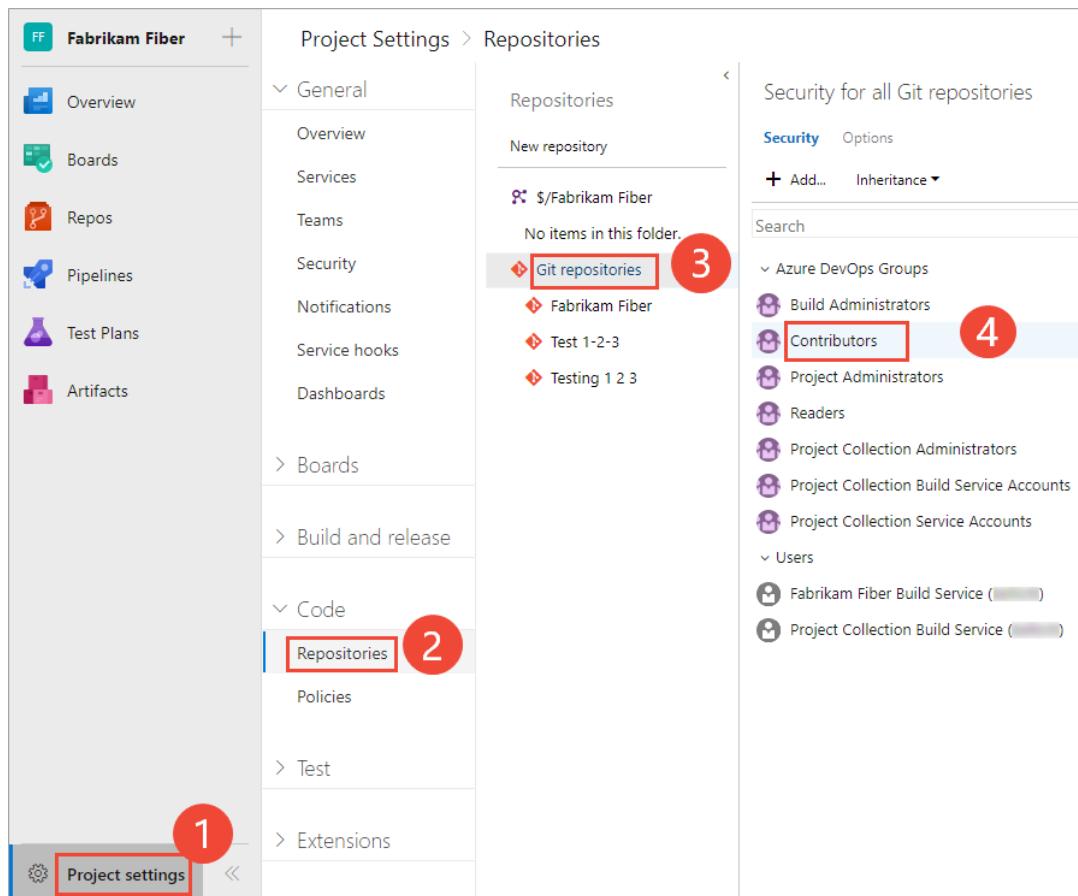
Set Git repository permissions

You can set the permissions for all Git repositories for a project, or for a single repository.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. To set the permissions for all Git repositories for a project, choose **Git Repositories** and then choose the security group whose permissions you want to manage.

For example, here we choose (1) **Project Settings**, (2) **Repositories**, (3) **Git repositories**, (4) the **Contributors** group, and then (5) the permission for **Create repository**.

To see the full image, click to expand.



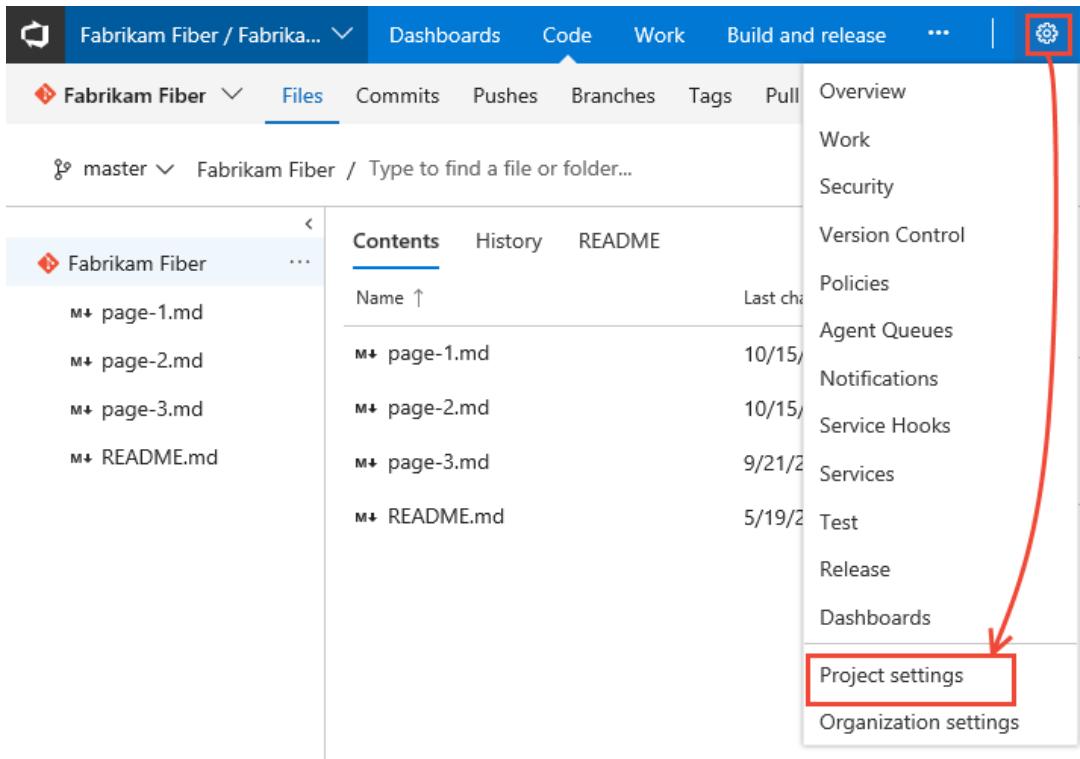
Otherwise, choose a specific repository and choose the security group whose permissions you want to manage.

NOTE

If you add a user or group, and don't change any permissions for that user or group, then upon refresh of the permissions page, the user or group you added no longer appears.

3. When done, choose **Save changes**.

1. Open the web portal and choose the project where you want to add users or groups. To choose another project, see [Switch project, repository, team](#).
2. Choose the gear icon to open the administrative context.



3. Choose **Version Control**.

4. To set the set the permissions for all Git repositories for a project, (1) choose **Git Repositories** and then (2) choose the security group whose permissions you want to manage.

Otherwise, choose a specific repository and choose the security group whose permissions you want to manage.

5. Choose the setting for the permission you want to change.

Here we grant permissions to the Contributors group to (3) create repositories.

The screenshot shows the 'Version Control' tab selected in the top navigation bar. On the left, under 'Repositories', the 'Git repositories' section is highlighted with a red box and labeled '1'. Inside this section, the 'Contributors' group is highlighted with a red box and labeled '2'. In the 'ACCESS CONTROL SUMMARY' table, the 'Create branch' permission is shown with a red box around the 'Allow' button, labeled '3'.

ACCESS CONTROL SUMMARY	
Shows information about the permissions being granted to this identity	
Contribute	Allow
Create branch	Allow
Create repository	Allow
Create tag	Not set
Delete repository	Not set
Edit policies	Not set
Exempt from policy enforcement	Not set
Force push (rewrite history and delete branches)	Not set
Manage notes	Allow
Manage permissions	Not set
Read	Allow
Remove others' locks	Not set
Rename repository	Not set

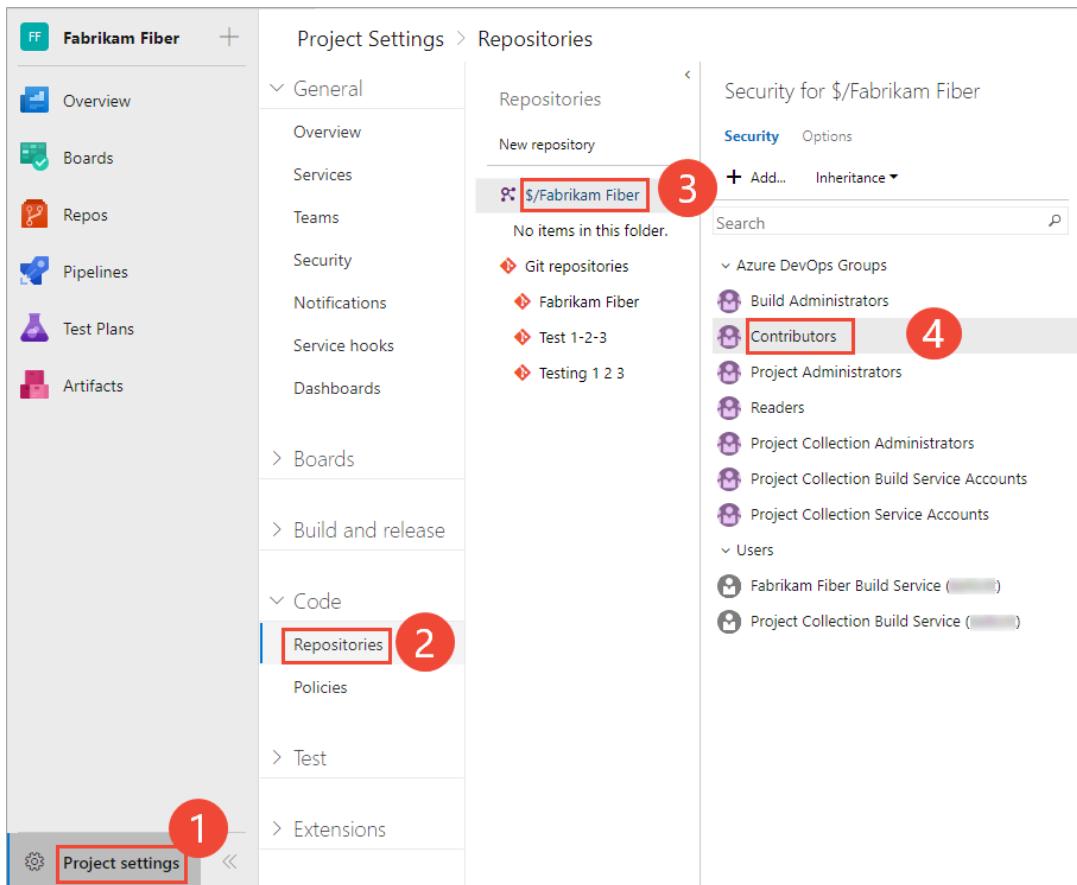
6. When done, choose **Save changes**.

Set TFVC repository permissions

1. To set the permissions for the TFVC repository for a project, choose **TFVC Repository** and then choose the security group whose permissions you want to manage.

For example, here we choose (1) **Project Settings**, (2) **Repositories**, (3) the **TFVC repository**, (4) the **Contributors** group, and then (5) the permission for **Manage branch**.

To see the full image, click to expand.



NOTE

If you add a user or group, and don't change any permissions for that user or group, then upon refresh of the permissions page, the user or group you added no longer appears.

2. Save your changes.
1. From the web portal, open the admin context by choosing the gear Settings icon and choose **Version Control**.
2. Choose the TFVC repository for the project and then choose the security group whose permissions you want to manage.
3. Change the permission setting to **Allow** or **Deny**.

For example, here we change the **Manage branch** permission to Allow for all members of the Contributors group.

The screenshot shows the Microsoft DevOps interface for a project named "Fabrikam Fiber". The top navigation bar includes links for Overview, Work, Security, Version Control (which is selected), Agent Queues, Notifications, Service Hooks, Services, and Test. On the left, there's a sidebar for "Repositories" with options for "New repository" and two listed items: "Git repositories" and "Fabrikam Fiber". The main content area is titled "Security for \$/Fabrikam Fiber". It features a search bar and dropdown menus for "Add..." and "Inheritance". A list of security groups and users is shown, with "Contributors" being highlighted (circled with number 2). To the right is a "ACCESS CONTROL SUMMARY" table with columns for permission names and their current status (e.g., Not set, Allow, Not set). The "Manage permissions" row for the "Contributors" group has its "Allow" button circled with number 3. At the bottom are buttons for "Clear explicit permissions", "Remove", "Save changes", and "Undo changes".

4. Save your changes.

Related articles

- [Default Git permissions](#)
- [Default TFVC permissions](#)
- [Default permissions and access](#)
- [Permissions and groups reference](#)

2 minutes to read

Control how long to keep test results

7/3/2019 • 2 minutes to read • [Edit Online](#)

Azure Test Plans | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015

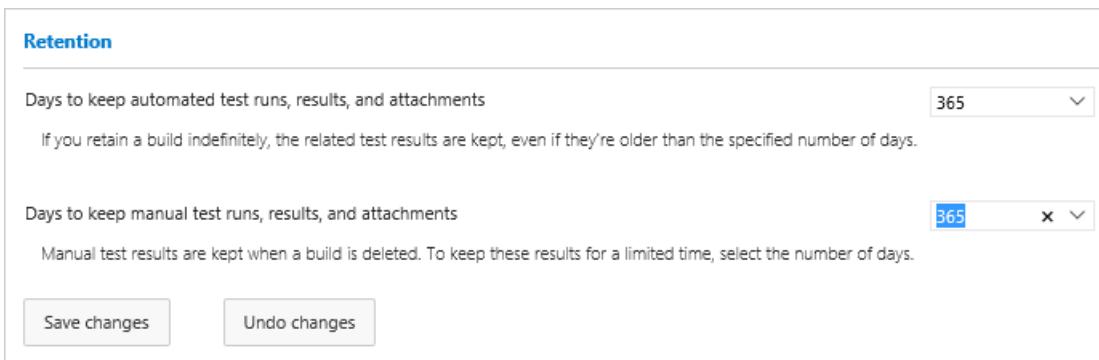
Running tests, especially automated ones, generates lots of data. To keep your test system responsive and performing well, have a policy to clear test results that you don't need anymore. Delete automated test results when you delete your builds. You can keep manual test results while you're still reviewing them, for example, up to a year.

To use all the features described in this topic you must have either an [Enterprise](#), [Test Professional](#), or [MSDN Platforms](#) subscription; or have installed the [Test Manager extension for Azure Test Plans](#) available from Visual Studio Marketplace. See [Manual testing permissions and access](#).

Manual test results

To delete manual test results after a specific number of days, set the retention limit at the project level. Azure DevOps keeps manual test results related to builds, even after you delete those builds. That way, build policies don't delete your test results before you can analyze the data.

1. Sign into Azure DevOps. You'll need at least project administrator permissions.
2. Go to your project and then open the [project settings page](#).
3. In the **Test | Retention** page, select a limit for how long you want to keep manual test data.



Automated test results

Automated test results associated with builds

By default, Azure DevOps keeps automated test results related to builds only as long as you keep those builds. To keep test results after you delete your builds, edit the build retention policy. If you use Git for version control, you can specify how long to keep automated test results based on the branch.

1. Sign into Azure DevOps. You'll need at least build level permissions to edit build pipelines.
2. Go to your project. Find and edit your build pipeline.

The screenshot shows the Azure Pipelines dashboard. On the left, there's a search bar for 'Search all pipelines' and a 'New' button. Below that, a list of pipelines includes 'DotNetSample-ASP.NET Co...' which is checked and has a commit history from 'master' 3 days ago. On the right, the pipeline details for 'DotNetSample-ASP.NET Core-CI' are shown, with the 'Edit' button highlighted by a red box.

3. Open the **Retention** page. Modify the default policies as required, or add new policies.

The screenshot shows the 'Retention' page for the 'DotNetSample-ASP.NET Core-CI' pipeline. The 'Retention' tab is selected and highlighted with a red box. The page is divided into two main sections: 'Policies' and 'Settings'. In the 'Policies' section, there are two items: 'Keep for 10 days, 1 good build' (with a '+refs/heads/*' filter) and 'Keep for 30 days, 10 good builds' (marked as 'Maximum'). In the 'Settings' section, under 'Branch filters', there's an 'Include' type set to '*'. Under 'Days to keep', the value is '10' and 'Minimum to keep' is '1'. Under 'When cleaning up builds, delete the following:', several options are checked: 'Build record', 'File share', 'Symbols', and 'Automated test results'.

If you use Git, and have more than one branch, set the branch filter to delete test results and builds in specific branches as required. You can keep test results in other branches, even though you delete the builds in these branches.

Automated test results not associated with builds or orphaned from deleted builds

To clean up automated test results that are left over from deleted builds or test results that aren't related to builds, for example, results published from external test systems, set the retention limits at the project level as shown [here](#).

See also

- [FAQs for manual testing](#)

Help and support

Report any problems on [Developer Community](#), get advice on [Stack Overflow](#), and get support via our [Support](#) page.

Quickstart: Access, export, and filter audit logs

6/21/2019 • 6 minutes to read • [Edit Online](#)

Azure DevOps Services

NOTE

Auditing is currently in a Public Preview.

In this quickstart, you learn how to access, export, and filter audit logs. Auditing contains numerous changes that occur throughout an Azure DevOps organization. Changes occur when a user or service identity within the organization edits the state of an artifact. In some limited cases, it can also include accessing an artifact. Think permissions changes, resource deletion, code download, accessing the auditing feature, and much more.

When an audit-able event occurs, a log entry is recorded as an audit event. Events contain information such as IP, user who caused the event, what happened, and other useful pieces of data that help you answer the who, what, when, and where.

Auditing is turned on by default for all Azure DevOps organizations. You can't turn auditing off, ensuring that you never miss an actionable audit event. Events are stored for 90 days and then they're deleted. However, you can back up audit events to an external location to keep the data for longer than the 90-day period.

Prerequisites

By default, Project Collection Administrators are the only group that can access the auditing feature.

Access auditing

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

The screenshot shows the Azure DevOps portal interface. On the left, there's a sidebar titled 'My organizations' with a list of projects: 'FabrikamFiber' (selected), 'P [redacted]', 'fabrikamfib', and 'fabrikamfiber4'. Below this is a 'New organization' button and an 'Organization settings' button, which is highlighted with a red box. The main content area is titled 'FabrikamFiber' and shows three projects: 'Fabrikam Fiber' (blue icon), 'Fabrikam' (teal icon), and 'FabrikamFiber4.0' (purple icon). At the bottom of the sidebar, there are links for 'All projects', 'New organization', and 'Organization settings'.

3. Select **Auditing**.

The screenshot shows the 'Organization Settings' page for 'FabrikamFiber'. The left sidebar has a 'General' section with 'Overview', 'Users', 'Billing', 'Auditing' (which is selected and highlighted with a red box), 'Global notifications', 'Usage', 'Extensions', and 'Azure Active Directory'. Below that is a 'Security' section with 'Policies' and 'Permissions'. The right side shows the 'Auditing' section, which includes a table of audit logs. The table has columns: Actor, Timestamp, Area, Category, and Details. The details column contains links to view specific audit events. The table shows several entries from 'Josh Hartn...' on different dates, mostly related to security and access modifications.

Actor	Timestamp	Area	Category	Details
JH	6/10/2019, 3:58:56 PM	Auditing	Access	Accessed the audit log 2 times
JH	6/10/2019, 3:55:54 PM	Security	Modify	Permission "AuditLog\View audit log" was set to allow for [FabrikamFiber]\Auditing Access
Azure Dev...	6/10/2019, 3:55:54 PM	Security	Modify	Permission "AuditLog\View audit log" was set to allow for [FabrikamFiber]\Auditing Access
JH	6/10/2019, 3:55:53 PM	Security	Modify	Permission "AuditLog\View audit log" was set to allow for [FabrikamFiber]\Auditing Access
Azure Dev...	6/10/2019, 3:54:07 PM	Project	Create	Foobar project was created successfully
Azure Dev...	6/10/2019, 3:54:07 PM	Security	Modify	3 permissions were modified for [Foobar]\Project Administrators
JH	6/10/2019, 3:54:06 PM	Security	Modify	2 permissions were modified for [FabrikamFiber]\Project Collection Test Service Accounts
JH	6/10/2019, 3:54:06 PM	Security	Modify	3 permissions were modified for [FabrikamFiber]\Project Collection Test Service Accounts

If you don't see Auditing in organization settings, then you don't have access to view audit events. Outside

of the Project Collection Administrators group, you can give permissions to other users and groups, so they can view auditing.

4. Select **Security**, and then find the group or users to provide auditing access to.
5. Set **View audit log** to **allow**, and then select **Save changes**.

[FabrikamFiber]\Auditing Access

Permissions Members Member of

General

Alter trace settings	Not set
Create new projects	Not set
Delete team project	Not set
Edit instance-level information	Not set
View audit log	Allow
View instance-level information	Allow (inherited)

Service Account

Make requests on behalf of others	Not set
Trigger events	Not set
View system synchronization information	Not set

Boards

Create process	Not set
Delete field from organization	Not set
Delete process	Not set
Edit process	Not set

Repos

Administer workspaces	Not set
-----------------------	---------

Saved

The user or group members have access to view your organization audit events.

Review audit log

The auditing page provides a simple view into the audit events that are recorded for your organization. For now, you can only search by a time range to find audit events that occurred within the last 90 days.

See the following description of the information that's visible on the auditing page.

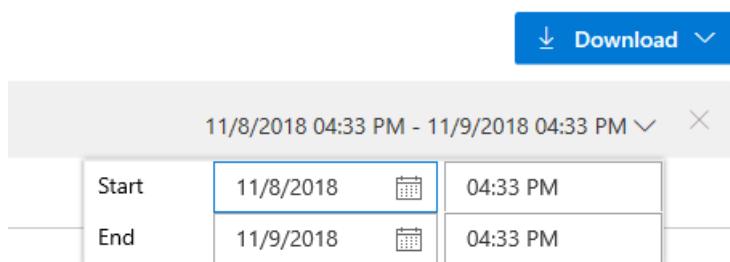
Information and details

INFORMATION	DETAILS
Actor	Display name of the individual that triggered the audit event to be recorded
IP	IP address of the individual that triggered the audit event to be recorded

INFORMATION	DETAILS
Timestamp	Time that the triggered event happened. Time is localized to your time zone
Area	Location in Azure DevOps where the event took place
Category	Description of the type of action that occurred For example, Modify, Rename, Create, Delete, Remove, Access
Details	Brief description of what happened during the event

Each audit event records additional pieces of information to what is viewable on the auditing page. This information includes the authentication mechanism, a correlation ID to link similar events together, user agent, and additional information that's dependent on the type of audit event. This information can only be viewed by downloading auditing events.

To scope down the viewable audit events, select the time filter on the top-right-hand side of the page.



You can select any time range over the last 90 days and scope it down to the minute. Once you've selected your wanted time range, select anywhere off the time range selector to start the search. By default, the top 200 results are returned for that time selection. If there are more results, then you can scroll down to load them onto the page. If you wish to further scope down the set of results returned, then you need to download the auditing data.

Some audit events can contain multiple actions that took place at once, known as bulk audit events. You can distinguish these events from others with the information icon on the far right of the event.

Clicking on the information icon will display a flyout that contains additional information about what happened in this audit event.

Export auditing events

To do a more detailed search of the auditing data, or store more than 90 days of data, you need to export existing audit events. The exported data can then be stored in another location or service.

Exporting can be done via the download button in the top-right-hand side of the auditing page. From that button, you can select to download to CSV or JSON.

Selecting either option starts the download. Events are downloaded based on the time range you've selected in the filter. If you had one day selected, then you get that one day's worth of data. Transversely, if you wanted all 90 days, select 90 days from the time range filter and then start the download.

Filter audit log

The auditing page in Azure DevOps currently supports searching for audit events only by setting a time range. Other, more detailed types of searches will need to be done using other tools after exporting your audit event data.

For quick investigations, we recommend that you download the logs as CSV files. You can then use Microsoft Excel or other CSV parsers to quickly filter on the area and category columns. For longer term, we recommend that you place your exported audit events in a Security Incident and Event Management (SIEM) tool. The tool allows you to keep greater than 90 days of events, search, generate reports, and configure alerts based on audit events.

When you're filtering through audit events, it's best to leverage the "area" and "category" columns. These columns allow you to quickly filter down to just the type of events that you're interested in. The following tables have a list of current areas and categories.

Categories

CATEGORY	DESCRIPTION
Modify	Modify implies that an artifact in an organization was changed. This could be a state or property change
Rename	Rename is a special type of modify event, which occurs when an artifact in an organization has its name changed
Create	Create refers to artifacts that are newly made in an organization
Delete	Delete refers to when an artifact is deleted or removed from an organization
Access	Access refers to when an artifact is viewed or opened in an organization

Areas

AREA	DESCRIPTION
Project	Create, delete, change in visibility, and rename a project in an organization
Security	Modify security permissions, create group, delete group, update group, add member to group, and remove member from group
Audit	View or download audit events
Agile	Process, create, delete, and modify
Notification	Create, remove, and modify a subscription
Pipelines	Create, delete, and modify build definition
Extensions	Install, delete, or update an extension

Filtering tips

After you download a copy of your auditing events, you can view additional pieces of information collected with

each event. See the following useful tips for how to filter through events beyond using only the categories and areas fields.

ID & correlation ID

Each audit event has a unique identifier called the "ID" and a correlation ID called the "CorrelationID". The correlation ID is helpful to find related audit events. For example, a project creation can generate several dozen audit events. You can link these events together because they all have the same correlation ID.

When an audit event ID matches its correlation ID, that's an indication that the audit event is the parent or original event. So, the initial event, showing that a user created a project, will have the same ID as the correlation ID. If you want to view only the set of events that were originators and not post action events, you can set a filter for where "ID" equals the "Correlation ID". Then, if you find an event that you're interested in investigating, you can search for just events with that correlation ID. Note that not all events have other related events.

Limitations

The following limitations exist for what can be audited.

- Azure Active Directory (Azure AD) group membership changes – In the future, auditing will include changes to Azure DevOps groups, such as adding or removing a group or user. However, if you manage membership via Azure AD groups, additions and removals of users from those Azure AD groups are not audited by Azure DevOps. Review the Azure AD audit logs to see when a user or group was added or removed from an Azure AD group.
- Signing in – Sign-in events to Azure DevOps aren't tracked. View the Azure AD audit logs to review sign-in events to your Azure AD.

What are the features in Azure DevOps?

7/10/2019 • 54 minutes to read • [Edit Online](#)

Azure DevOps Services | Azure DevOps Server 2019 | TFS 2018 | TFS 2017 | TFS 2015 | TFS 2013

Learn about all the features available to help you plan and track your projects and code, build, test, and release your software applications in Azure DevOps.

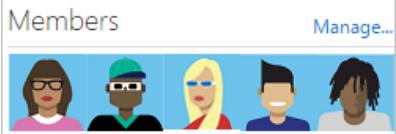
If you're new to Azure DevOps, see our overview articles that are designed to give beginners an understanding of the server-client structure and tools supported. For a description of the core services supported through the web portal, see [Essential services](#).

NOTE

Some features are platform-dependent, based on the following two platforms:

- **Azure DevOps Services** - cloud service
- **Azure DevOps Server** - on-premises

Access and supported clients

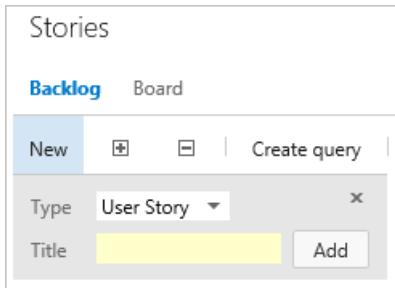
Browsers	Manage users and groups	Access levels
<p>Browsers</p> <p>Connect to the web portal from the latest versions of these supported browsers:</p> <ul style="list-style-type: none">- Chrome- Microsoft Edge- Firefox- Internet Explorer- Safari (Mac)	<p>Manage users and groups</p> <p>Add members to your project adds them to the Contributor group. When managing a large group of users, use built-in groups to manage users and their permissions.</p> <p>Add team members</p> <p>To share and contribute to your project, add users to Azure DevOps Services or your TFS.</p>  <p>Azure Active Directory (Azure AD) (Azure DevOps Services)</p> <p>Control who can access your team's critical resources and key business assets by managing access with Azure Active Directory groups.</p>	<p>All users that you add to your Azure DevOps organization or to your TFS project have access to Basic features by default, except Stakeholders who have access to a limited set of features, or those added to the Advanced access level in TFS.</p> <ul style="list-style-type: none">- Manage users (Azure DevOps Services) - Change access levels (TFS)
<p>Integrated Development Environments (IDE)</p> <p>Track work and integrate with your code, build, and test environments from the following clients:</p> <ul style="list-style-type: none">- Eclipse (Team Explorer Everywhere)- Visual Studio- Android Studio- IntelliJ- Visual Studio Code <p>To learn how to connect, see Connect to a project.</p>		<p>Permissions</p> <p>Control access to specific features by setting permissions for a user or group.</p> <ul style="list-style-type: none">- Area and iteration paths- Build & Release- Git- TFVC- Dashboards- Queries- Manage teams and configure team tools- Test- Work item tags
<p>Office integration clients</p> <p>Use features supported by these familiar clients to manage your project and illustrate your requirements.</p> <ul style="list-style-type: none">- Excel- Project- PowerPoint - Storyboarding		

Agile tools to plan and track work

Backlogs

Create your backlog

Plan your project by [adding a work item for each user story or requirement](#) you plan to develop.



Organize your backlog

Group items into a hierarchical list using [portfolio backlogs](#) and quickly reorder and re-parent items to effectively manage your deliverables.

Forecast

Use the [forecast](#) tool to estimate work to be completed in future sprints.

Storyboard

Visualize your ideas and user stories and support greater understanding of them by [storyboarding them with PowerPoint](#), also link your storyboards to your backlog work items.

Move work item to a different project (Azure DevOps Services)

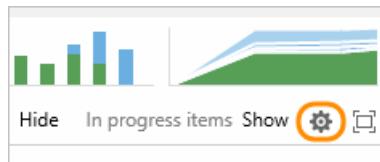
Choose the Change project menu option, Actions menu in a work item form to [move the work item to a different project](#).

Full screen mode

Choose or to enter or exit full screen mode.

Backlog and board settings

Choose to configure team backlogs and boards, including [show bugs on backlogs and boards](#) and [set team backlog levels](#).



View portfolio backlog hierarchy

Use [Parents Show/Hide](#) to drill down into the backlog hierarchy.

Multi-team backlog ownership

Easily view and track items [owned by other teams](#) and quickly reorder and re-parent items to effectively manage your backlog.

Change work item type (Azure DevOps Services)

If you added a task instead of a bug and want to change the work item type to bug, you can.

Choose the Change type option from the Actions menu in a work item form to [change the work item type](#).

Filter your backlog

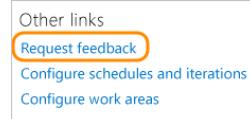
Use **Show/Hide in progress** to only show or hide items which have moved from the new or proposed state to active or in progress state.

Additionally, you can list a subset of items based on keywords [keywords](#) or [tags](#).



Request feedback

Request feedback on [working software](#) and easily track responses that capture interaction with video, verbal, or type-written comments.



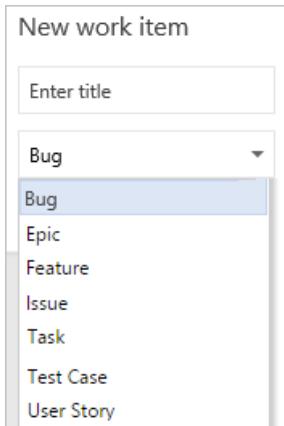
Feedback client

Provide the free [Microsoft feedback client](#) to capture their responses to your feedback requests.

Bug, task, and issue tracking

Track issues and other types of work

Different types of work items track [different types of work](#) - such as bugs, test cases, risks, issues, and more.

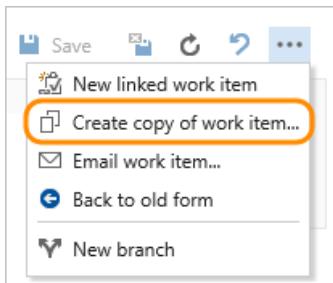


Bulk modify

Quickly change one or more fields in several work items using [bulk modify in the web portal](#) or [bulk modify using Excel](#).

Copy or clone a work item

[Copy an existing work item](#) or bulk copy several using [Excel](#).



Follow a work item

Choose the Follow / Following icons to quickly start or stop tracking changes made to a work item.



Rich text comments

Describe and comment on work using [formatted text](#), [hyperlinks](#), and [inline images](#). Choose or to expand or contract the viewing area.

Clear HTML formatting

Use the icon or [CTRL+Spacebar](#) to remove formatting from

Estimates and time tracking

Track [estimated](#), [completed](#), and [remaining work](#) for tasks and other work items. Several reports and dashboards provide charts that display data based on team capacity and remaining work.

New work item experience

The [new work item experience](#) provides access to a more modern form, additional features, and the ability to add fields and apply other customizations to the work item type.

Manage bugs

[Capture and triage bugs](#) using different kinds of tools.

Choose how you want to track bugs

Each team can [choose to manage bugs on their backlog](#) or along with tasks.

Share plans and information

Share information using work items and [generate summary lists with links to backlogs or queries](#).

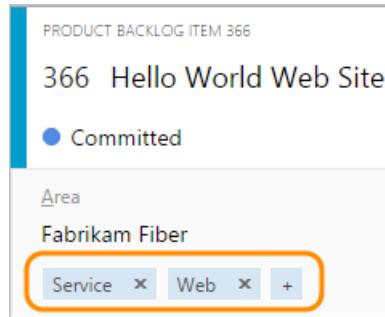
Remove or delete a work item

Remove work items from the backlog by changing their State to Removed. Or, [move them to the recycle bin](#) or permanently delete them.



Tags

Add [tags to work items](#) to filter backlogs and queries. [Bulk update work items](#) or [use work item templates](#) to add or remove tags.



Work item templates

Quickly add new work items based on templates [with pre-populate values for your team's commonly](#)

Discussion

[Add or review comments](#) added to a work item. Start by choosing the discussion icon.

Integrate Git development with work tracking

Drive Git development and stay in sync as a team to complete backlog items and tasks using the [Git Development section](#). Add branches, create pull requests, and view all development done to support the specific work item.

Development

		Added file
		Created 33 minutes ago, Completed
		features/cancel-order-form
		Updated 35 minutes ago Create a pull request
		Added file
		Created 35 minutes ago, 4ba415

Verify a bug, rerun test case

Choose the **Verify** option from the bug work item form context menu to launch the relevant test case in the web runner. For more information, see [Run tests for web apps](#).

Link work items

Track related work, dependencies, and changes made over time by [linking work items](#).

Links

ID	Title
Child (3)	
346	Add animated emoticons
347	Implement a service that receiv
348	As a <user>, I can select an em

Add or modify a field

Add a custom field ([Azure DevOps Services](#) | [TFS](#)) to support tracking additional data requirements or modify an existing field to apply optional rules.

Restrict access

Limit who can create or modify work items or a work item field based on area path, work item type, or based on your specific

highlighted text.

Attachments

To support collaboration of work in progress, [add emails, documents, images, log files, or other file types](#) to work items.

[used fields](#).

History & auditing

Review and query [work item change history](#) to learn of past decisions and support future ones.

conditions.

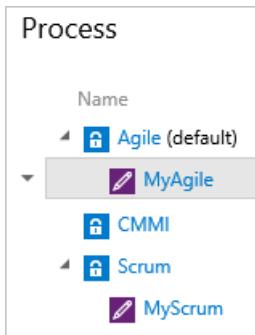
Field index

Find descriptions and usage information for each field from the [work item field index](#).

Customize (Azure DevOps Services)

Create an inherited process

The first step in customizing a project is to [create an inherited process](#). You can only customize inherited processes.



New work item experience

The [new work item experience](#) provides access to a more modern form, additional features, and the ability to add fields and apply other customizations to the work item type.

Customize a process

Customizations you make to an inherited process automatically update all team projects that reference that process. You can customize your project as follows:

- [Add and modify fields](#)
- [Modify the web form layout](#)
- [Modify the workflow states](#)
- [Add a custom work item type](#)
- [Add a custom control](#)

Change the process used by a project

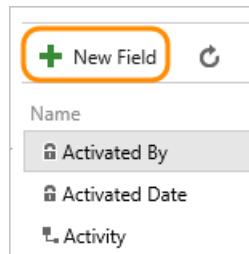
To apply customizations to one or more team projects, you [change the process they reference to a customized inherited process](#).

Enable/disable a process

To make sure no one creates a project from a process that you don't want used, [you can disable it](#).

Add or modify a field

Add a custom field to support tracking additional data requirements or modify an existing field to apply optional rules.

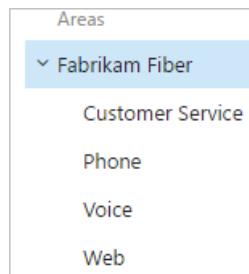


Remove a field from a form

You can [remove a custom field](#) and [select inherited fields](#) from a work item form. You can also [relabel the fields](#) that appear on the form.

Area path pick lists

Change the [pick list of area paths](#) to support grouping work items by team, product, or feature area.



Sprint/iteration pick lists

Change the [pick list of iteration paths](#) to support grouping work into sprints, milestones, or other event-specific or time-related period. Activate sprints for each team.



Review fields

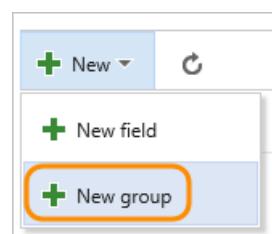
You can [review the list of fields](#) defined for a process, their data type, and the WITs which reference them. For descriptions and usage of each field, see [Work item field index](#).

Delete a field from the collection

You can [delete a custom field](#) if you find it's no longer required.

Customize the web form

For each work item type, you can [add custom pages to group](#) [additional custom fields](#) and you can organize your forms by placing logically related groups and HTML fields on separate pages within a form.



Add a custom work item type

You can [add and modify a custom work item type](#).

Customize the workflow

For each work item type, you can [add custom workflow states to support your business tracking needs](#).

Delete a process

Delete those inherited processes that you no longer want used. Simply choose the Delete option from its context menu.

Set process permissions

To customize a process, add custom fields, or change the layout of a work item form, you must be a member of the Project Collection Administrators group or be [granted explicit permissions to edit a specific process](#).

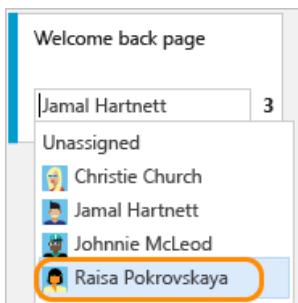
Customize (TFS)

<p>Add or modify a field</p> <p>Add or modify a field to support work tracking and reporting by editing the WIT definition.</p> <p>Add rules to a field</p> <p>Apply various rules to custom fields to qualify the value it can have, to copy a value, to specify a default, to restrict who can modify it, to enforce pattern matching, or to enforce conditional values.</p> <p>Remove a field</p> <p>Stop tracking a field by removing the field from the work item form of select work item types.</p>	<p>Area path pick lists</p> <p>Change the pick list of area paths to support grouping work items by team, product, or feature area.</p> <p>Sprint/iteration pick lists</p> <p>Change the pick list of iteration paths to support grouping work into sprints, milestones, or other event-specific or time-related period.</p> <p>Custom pick lists</p> <p>Define or modify pick list values by editing the work item type definition.</p>	<p>Modify the workflow</p> <p>Design your custom workflow by adding states, transitions, reasons, and optional actions.</p> <p>Change the work item form</p> <p>Change the layout of your work item form by adding fields, custom controls, or tabs.</p> <p>Add a custom work item type</p> <p>Add a custom work item type to track different data requirements.</p>
---	---	---

Kanban

Kanban basics

Use your Kanban board to [visualize and track the flow of work](#) from idea to completion as well as quickly update work item fields

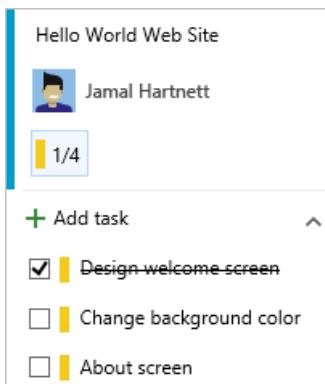


Drag-n-drop

[Drag and drop items](#) on the Kanban board to update status and to reorder and reparent items.

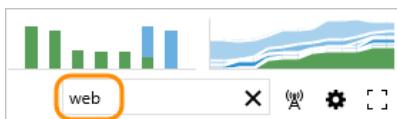
Add task checklists

Add and mark tasks as done with [lightweight tasks checklists](#).



Filter

Use key words to filter and find items on the Kanban board.



Set WIP limits

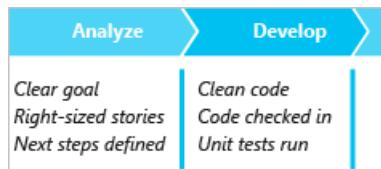
Set constraints on the amount of work your team undertakes at each [work stage](#) to gain access to sprint backlogs and task boards.

Split columns

Turn on split columns to [track the lag between when items are done in one state and work actually starts in a new state](#).

Map your workflow

Customize columns to support your team's [workflow](#) and track work from start to finish.



Expedite work with swimlanes

Use [swimlanes](#) to track work at different service-level classes.

Definition of done

Support your team to be in sync by specifying [requirements to fulfill](#) prior to handoff of items to a downstream work stage.

Filter by field values or parent work items

Choose the  field filter icon to [filter the board based on](#) assignment, iteration, work item type, or tags.



Cumulative Flow Diagram

With the CFD, you can [monitor the count of work items as they progressively move through various states which you define](#).

Customize cards

Add [fields to cards](#) that you can edit directly on your Kanban and task boards.

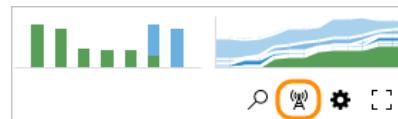
5 Slow response on form

	Jamal Hartnett	8
State	Committed	
Changed...	Christie Church	
Changed...	7/29/2015	

Performance Web

Live updates

Enable [live updates](#) to automatically refresh your Kanban board when changes are made by others or to the board settings.



Add inline tests

Add, run, and update tests with inline test on your Kanban board.

Add checklists to features and epics

Add and mark user stories and other work items as done from your [Kanban features or epics boards](#).

Set team's card reorder preference

You can preserve the backlog priority when you move a card to a new column by setting your team's [Kanban board card reordering setting](#).

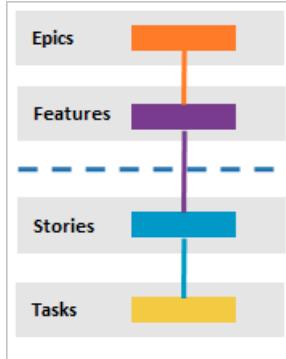
Enable/disable card annotations

Turn on or off [task checklists](#) or [inline tests](#) for your Kanban board.

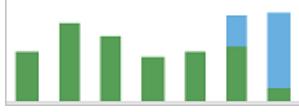
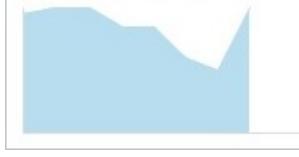
Configure inline tests

Configure how new inline tests are added to the Kanban board: [create a new test plan/test suite](#) or [choose an existing test plan](#).

Scale

<h3>Add another team</h3> <p>Add and structure teams and organize work to support team autonomy and organizational alignment. Teams can manage their work independently of one another while the organization gains visibility across all teams.</p> <div data-bbox="155 399 414 714" style="border: 1px solid #ccc; padding: 10px;"> <p>Teams</p> <p>New team </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Team Name</th> </tr> </thead> <tbody> <tr> <td> Email</td> </tr> <tr> <td> Fabrikam Fiber Team</td> </tr> <tr> <td> Voice</td> </tr> </tbody> </table> </div> <p>Set team defaults</p> <p>Several Agile tools reference the team's default area path, iteration path, and activated sprints to automatically filter the set of work items they display. Understand how defaults are used.</p>	Team Name	 Email	 Fabrikam Fiber Team	 Voice	<h3>Set up a team hierarchy</h3> <p>By configuring your teams and backlogs into an hierarchical structure, program owners can more easily track progress across teams, manage portfolios, and generate rollup data.</p> <p>Autonomy and alignment</p> <p>As your organization grows, your tools can grow to support a culture of team autonomy and organizational alignment.</p> <p>Scale your tools and practices</p> <p>Incrementally adopt practices that scale to create greater rhythm and flow within your organization, engage customers, improve project visibility, and develop a productive workforce.</p>	<h3>Portfolio management</h3> <p>Manage a portfolio of backlogs and gain insight into each team's progress as well as the progress of all programs.</p> <div data-bbox="1028 303 1314 662" style="border: 1px solid #ccc; padding: 10px; text-align: center;">  <pre> graph TD Epics[Epics] --> Features[Features] Features --> Stories[Stories] Stories --> Tasks[Tasks] </pre> </div> <p>Scaled Agile Framework</p> <p>Structure team projects to support epics, release trains, and multiple backlogs to support the Scaled Agile Framework.</p>
Team Name						
 Email						
 Fabrikam Fiber Team						
 Voice						

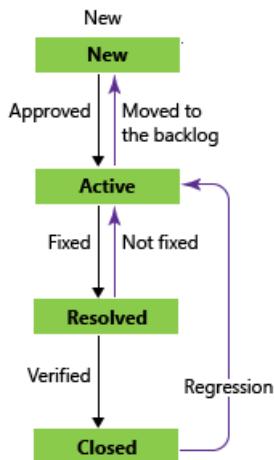
Scrum

<p>Define sprints</p> <p>Schedule and activate your team's sprints to gain access to sprint backlogs and task boards.</p> <p>Select team sprints, set team defaults</p> <p>Several tools reference the team's default and active iteration paths or sprints. For the Agile tools to work best, each team needs to set their team area path(s) and iteration paths to support their work tracking activities.</p> <p>Plan sprints</p> <p>Build your sprint backlog, add tasks, and load balance work across your team as you plan your sprint.</p> <p>Track work on your task board</p> <p>Use your task board during your daily Scrum meetings to view and update progress.</p>	<p>Velocity & forecasting</p> <p>Use velocity charts and forecast tools to estimate work that can be completed in future sprints.</p> <div data-bbox="591 1336 890 1448" style="border: 1px solid #ccc; padding: 10px; text-align: center;">  </div> <p>Sprint burndown charts</p> <p>Monitor progress and review team patterns from sprint burndown charts.</p> <div data-bbox="591 1650 890 1897" style="border: 1px solid #ccc; padding: 10px; text-align: center;"> <p>Sprint 91 October 19 - November 6</p>  </div>	<p>Manage resources</p> <p>Use capacity planning tools to track individual, team, and activity over and under capacity for a sprint.</p> <div data-bbox="1028 1336 1345 1987" style="border: 1px solid #ccc; padding: 10px;"> <p>Work</p> <p>Team  (51 of 61 h)</p> <p>Work By: Activity</p> <p>Work By: Assigned To</p> <ul style="list-style-type: none">  Christie Church  (15 of 6 h)  Jamal Hartnett  (11 of 24 h)  Johnnie McLeod  (10 of 16 h)  Raisa Pokrovskaya  (15 of 15 h) </div>
---	--	--

Workflow

What is workflow?

You use workflow to track the progress of work as it moves from new, active, to complete or closed. Each workflow consists of a set of states, the valid transitions between the states, and the reasons for transitioning the work item to the selected state.

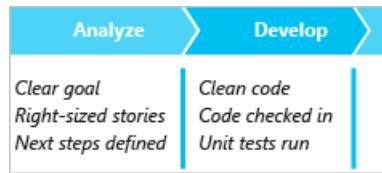


Default workflows

Each process [defines the workflow](#) for each work item type to track progress from newly defined, to in progress, to completed or closed.

Kanban workflow

You can fully customize your Kanban board to map the workflow your team uses by [adding and renaming columns](#)



Customize the workflow

For Azure DevOps Services: [add custom workflow states to support your business tracking needs](#). For TFS: [Design your custom workflow](#) by adding states, transitions, reasons, and optional actions.

States

States allow you to [track the status of work](#). For example, a bug moves from **Active**, **Resolved**, and **Closed** to correspond to when it's defined, fixed, and verified as fixed.

Transitions

Transitions specify the [valid progressions and regressions from state to state](#) for a work item type.

Reasons

Each transition [specifies a default reason as well as optional reasons](#) for tracking the change in state.

Update fields during workflow changes (TFS)

You can [define rules that change a field value](#) whenever you change the state, perform a transition, or select a reason.

Apply workflow conditional field rules (TFS)

You can define rules that [change a field value based on the contents of other fields](#) during workflow changes.

Restrict who can make changes during workflow transitions (TFS)

Set a condition field rule that applies to a group to [restrict who can make changes to a workflow or a field](#).

Event-generated workflow changes or field assignments (TFS)

Add an action to a custom workflow definition to automatically transition work items or specify a field value based on an internal TFS event or external event.

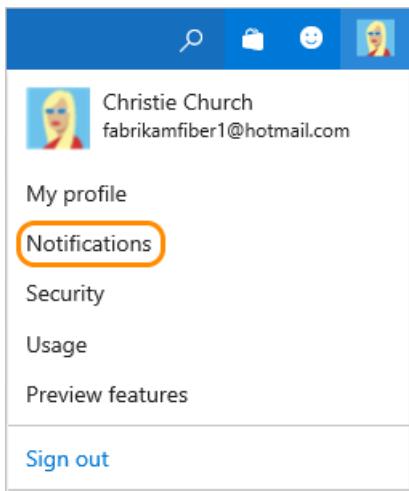
Visual workflow design tool (TFS)

You can change the workflow or view the workflow state diagram by using the [Process Editor](#), a power tool for Visual Studio.

Alerts and notifications

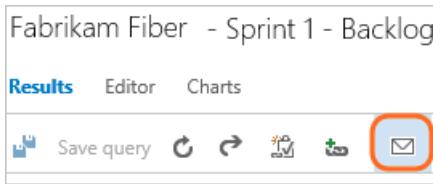
Personal and team notifications or alerts

Get notified as changes occur to work items, code reviews, source control files, and builds by setting [personal notifications](#) or [team notifications](#).



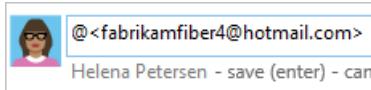
Share queries and sprint plans

Email a query or [sprint plan](#).



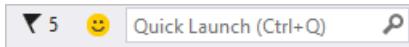
Quick alerts to team members

Use the **@mention** control to send email to team members to bring them into a discussion around work changes, pull requests, or other items.



Client feature flag updates

Alert flag within the IDE automatically notifies you of the latest client changes.



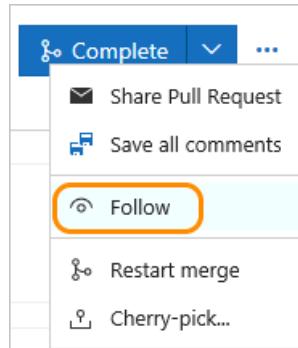
Follow a work item

Choose the Follow / Following icons to quickly start or stop tracking changes made to a work item.



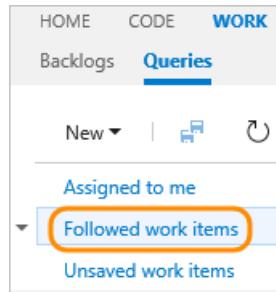
Follow a pull request

To track the progress of a single pull request, choose the Follow option from the context menu.



Manage work items you follow

From the **Work > Queries** page you can view the list of work items that you're following.



Frequent on-line feature updates

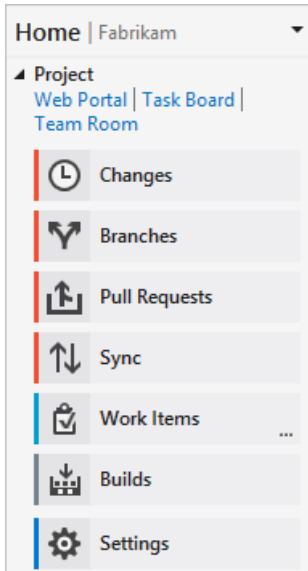
Check the [News](#) for product updates, or read about them by accessing the News link in your web portal.

Code

Code: Git

Get started with Git in Visual Studio

To get started working with Git, [clone a repository](#), [add code](#), and [create branches](#) in Azure DevOps Services or Visual Studio. Learn how to commit, publish, and conduct a pull request of your changes.

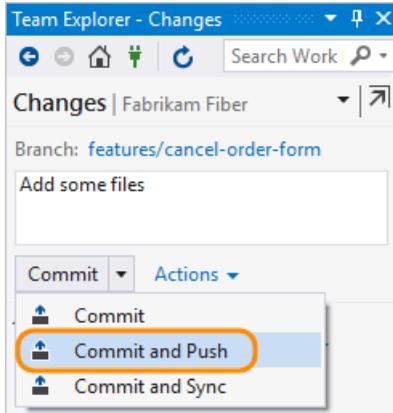


Clone repositories

To work locally, you [clone a repository](#).

Commit changes

Enter commit messages and [quickly push](#) your local changes to the shared repo.



Pull requests

Use [pull requests](#) to review and merge branch code to a master branch.

Sync

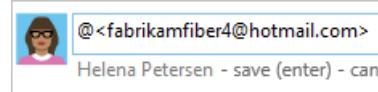
Quickly [sync](#) your local branch with a shared repo.

Get started using Eclipse

[Work with Git repositories](#) using the Team Explorer Everywhere IDE for Eclipse.

Add reviewers to get feedback

Use the [@mention](#) control to add [reviewers](#) to your pull request to get their feedback about your changes.



Resolve Git merge conflicts

Merge conflicts occur when commits have changes to the same files as other newer commits in the branch history. Learn how to [prevent and resolve merge conflicts](#).

Code search

Maximize cross-team collaboration and code sharing by finding code across all the projects to which you have access. Narrow down your results and focus in on code by using [filters](#), [preview code](#), [view history](#), [compare versions](#), and more



Get notified about pull requests

Subscribe to email alerts to get notified about [new pull requests](#), [changes](#), [approvals](#), and [rejections](#).

Set branch policies

To improve code quality, [set branch policies](#) to require code reviews or automatically add reviewers.

Automatically build pull requests

Set a branch policy to [automatically generate a build](#) for a pull request to selected branches.

Create Git repositories

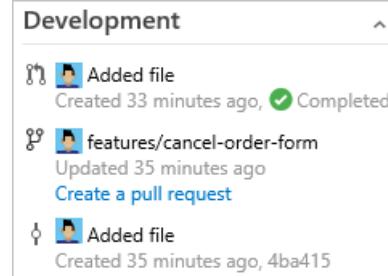
When you create a project with Git as your version control system, you automatically create a Git repo. You can [Create additional Git repos](#) from the admin context.

Rename a Git repository

[Rename Git repos](#) from the admin context.

Integrate Git development with work tracking

Drive Git development and stay in sync as a team to complete backlog items and tasks using the [Git Development section](#). Add branches, create pull requests, and view all development performed to support the specific work item.



Quickly link work items to pull requests

Use the [#ID](#) control to link work items to your pull request to support tracking work.

Get started using Xcode

[Work with Git repositories](#) using the Xcode IDE.

Git commands

Use [Git command line tools](#) when you need to perform select manual tasks or to automate work using a script.

Bypass a branch policy

Grant an [Exempt from policy enforcement](#) permission to a user or group.

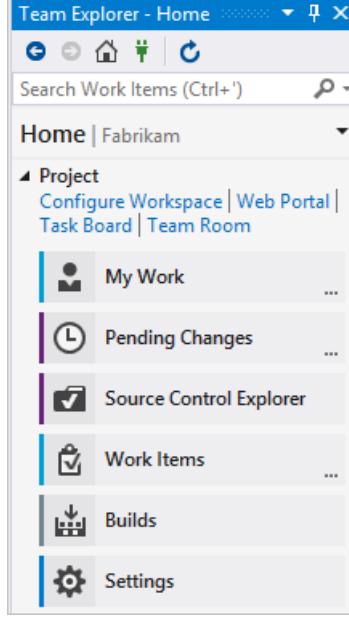
Rebase a branch

Before merging a branch into master, you may choose to first [rebase your branch onto the latest commit in master](#).

Git permissions

Set permissions on a [Git project](#), [repository](#), or [branch](#) from the context menu or from the web portal administration page.

Code: TFVC

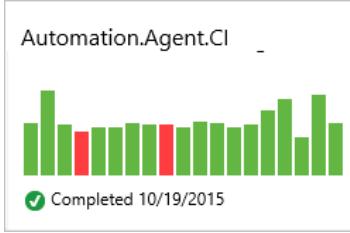
<p>Get started with TFVC in Visual Studio</p> <p>Develop and share your code. Learn how to configure your workspace, check-in your code, compare file changes, and view file history.</p>  <p>Set up local or server workspaces</p> <p>Create a local workspace that maps to the code base of interest.</p> <p>Resolve conflicts</p> <p>Support for Resolve conflicts that arise when several people work concurrently on a file.</p> <p>Compare files and folders</p> <p>Compare server folders and local folders to each other, and view the differences between the contents of each folder.</p>	<p>Track changesets</p> <p>Find information about which branches have received a particular set of changes and when those changes were merged.</p> <p>Request code review</p> <p>Increase overall code quality and reduce the risk of creating bugs by requesting a code review when you check-in code.</p> <p>Review history of a file</p> <p>Get detailed information about what changes have been made to your files.</p> <p>Suspend work</p> <p>Use shelvesets when you need to set aside some or all of your work in progress.</p> <p>Manage branches, isolate risk</p> <p>Use branches and locks to isolate risk introduced by work done by different teams.</p> <p>Merge branches</p> <p>Integrate work completed in different branches during certain phases of your project.</p> <p>Set check-in and check-out policies</p> <p>Enforce practices that lead to better code and more efficient group development by setting check-in/check-out rules.</p>	<p>Code search</p> <p>Find code across all the projects to which you have access. Narrow down your results and focus in on code by using filters, preview code, view history, compare versions, and more</p> <div data-bbox="1023 415 1396 482"><input type="text" value="Search code"/> </div> <p>Subscribe to alerts when check-ins occur</p> <p>Get notified when someone checks in code to your TFVC project by subscribing to receive email alerts.</p> <p>Version control locks</p> <p>Lock files or folders when you need to prevent them from being checked out or modified.</p> <p>Download files from the server</p> <p>Get the latest files from the server on a regular basis so that the code you develop is compatible with the code developed by others on your team.</p> <p>TFVC permissions</p> <p>Set permissions on select code management tasks from the context menu for TFVC files or folders or the admin context for the project.</p>
---	---	---

Azure Artifacts (Azure DevOps Services)

<p>What is Azure Artifacts?</p> <p>Azure Artifacts is the new name for what was previously Package Management. Azure Artifacts helps you manage code sharing by automating common tasks for discovering, consuming, and sharing components.</p> <p>Create feeds</p> <p>Create feeds to share code through packages.</p> <p>Move existing file shares to the cloud</p> <p>Eliminate dependencies on on-premises file shares and hosted instances of NuGet.Server by moving your packages to Azure DevOps Services.</p>	<p>Discover and consume packages</p> <p>Consume packages by connecting to a feed.</p> <p>Publish packages to feeds</p> <p>Publish packages to share code with your team and your organization.</p> <p>Add identities to your feeds</p> <p>Give teams and service identities access to your feeds.</p>	<p>Bootstrap the developer environment</p> <p>Increase your team's velocity and decrease the amount of code duplication across your organization. Access a set of tools and conventions for integrating Azure DevOps Services NuGet into your workflow by getting the NuGet VSS.PackageManagement.Bootstrap package.</p> <p>Remove a NuGet package from a feed</p> <p>[Unlist or remove a package]Delete packages and recover deleted packages from the recycle bin in Azure Artifacts you no longer want users to discover.</p> <p>Secure feeds</p> <p>Control who can contribute to or consume from a feed.</p>
--	--	--

Continuous delivery

Build

<p>Define builds</p> <p>Start from a build template and customize your build from there. Build for Windows, iOS, Android, Java (Ant, Maven, or Gradle), or Linux using the same domain-specific languages you use every day on your dev machine. Build Xamarin apps for both iOS and Android and run tests on the Xamarin Test Cloud as part of the build.</p> <p>Customize build process using scripts</p> <p>Use a script to add your team's business logic to your build process.</p> <p>Build agents and agent pools</p> <p>At least one agent is required to build your code. As you scale your system with more code, people, and builds, you'll need more build agents organized within agent pools. You can use both on-premises or Microsoft-hosted agent pools.</p> <p>Gated check-in (TFVC, Azure DevOps Services)</p> <p>Use gated check-in to protect against breaking changes when checking code into TFVC.</p> <p>Branch policies (Git)</p> <p>Improve code quality by setting branch policies to ensure build are never broken or getting the right people to review changes.</p>	<p>Specify your build steps</p> <p>Add steps to specify what you want to build, the tests to run, and all the other steps needed to complete the process.</p> <p>pipelines\tasks\build_img</p> <ul style="list-style-type: none">  Build an Android app using Gradle  Sign and align Android APK files  Build with Apache Ant  Build using a Gradle wrapper script  Grunt: The JavaScript Task Runner  Gulp: Node.js task-based build system  Index source code and publish symbols  Build with Apache Maven  Build with MSbuild  SonarQube for MSbuild  Visual Studio and MSbuild  Build an Android app with Xamarin  Build an iOS app with Xamarin on macOS <p>Build variables</p> <p>Use predefined variables or add your custom variables when configuring your build definition or your build scripts.</p>	<p>Continuous integration builds</p> <p>Define a CI build that compiles and tests your solutions whenever your team checks in code.</p> <p>Build summary charts</p> <p>View real-time build status and add build summary charts to your dashboards.</p> <div data-bbox="1075 503 1425 736">  </div> <p>Code coverage charts</p> <p>From the Code Coverage tab on a Build summary page, you can view percentage of code coverage as well as upload code coverage data in Jacoco or Cobertura formats.</p> <p>Audit changes</p> <p>Determine who changed what in the build definition and when they did it.</p> <p>Build retention policies</p> <p>Define policies to automatically delete old completed builds to minimize clutter.</p> <p>Build permissions</p> <p>Determine who can define, delete, and manage builds.</p>
--	---	--

Release

<p>Automate deployments</p> <p>Reduce time-to-market and respond to customer feedback with greater agility by automating your release process. Deploy applications across platforms to all environments of the pipeline with just one selection.</p>	<p>Works for any app</p> <p>Deploy any type of application across multiple platforms including Windows and Linux, whether on-premises or in the cloud.</p> <p>Approval workflows</p> <p>Streamline your application release workflow by routing pre- and post-deployment approvals to multiple approvers or teams.</p> <p>Release notifications</p> <p>Receive email messages as releases occur. Approvers receive</p>	<p>Release names</p> <p>Specify the naming and numbering scheme you want used when adding releases.</p> <p>Global configuration properties</p> <p>Simplify management of custom values that you use to configure multiple releases by specifying custom values for any of the tasks in any of the environments of a release definition.</p> <p>View test results</p> <p>Open the Tests tab to view a</p>
---	---	--

The screenshot shows the Azure Pipelines Overview page. At the top, there's a toolbar with icons for Refresh, Cancel, Restart, and Delete. Below the toolbar, a table lists four releases under the heading "Release Definition". Each row contains a status icon (blue play button for Release-7, green checkmark for Release-6, red X for Release-5, green checkmark for Release-4), the title, the environment name "Fabrikam", and a small gear icon.

When to use Azure Pipelines or Build & Release in TFS?

Evaluate how Azure Pipelines and Build & Release in TFS can help you in [your development and deployment efforts](#).

Release definitions

Add a release definition by [choosing the build version, target release environments, and tasks](#).

Release environments

[Define and clone release environments](#), logical entities that represent where you want to deploy a release, such as a collection of servers, a cloud, multiple clouds, or an app store.

Artifacts

A release is fundamentally defined by [versioned artifacts that make up the release](#). As you deploy the release to various environments, you deploy and validate the same artifacts on all environments.

Tasks

Automate release deployment by [defining the events that trigger a release](#).

Agents and agent pools

Agent pools are the execution containers that specify the security context and runtime environment for the [agents that run when you deploy a release](#).

notifications automatically when a release is waiting for approval.

Full traceability

Monitor the status of your release pipelines and track every deployment in each of the environments. Retain full audit history of all activities performed on a release with detailed release logs and approval tracking.

Release logs

View or download log files as zip files. Log files contain the status for each step or task of a release, for each of the environments in the release definition. Each completed release--succeeded, failed, or abandoned--[includes a live log file, details, and history for each step or task](#).

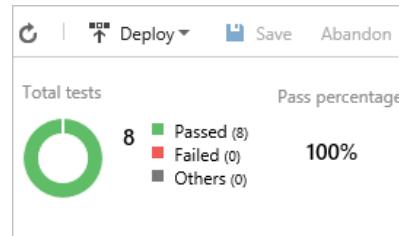
Triggers

Automate release deployment by [defining the events that trigger a release](#).

Variables

Lookup the description for all [release system, global, and agent variables](#).

summary of the test results, including pass/fail percentages and run duration. Sort the test results into groups or filter the results to show just passed, failed, or other results.



Add release summary to dashboard (Azure DevOps Services)

[Add a release summary chart](#) to a team dashboard.

Extend and customize

[Create workflows tailored to your process](#) by customizing our tasks, or extend with your own custom tasks.

The screenshot shows a list of deployment tasks. Each task has an icon and a brief description:

- Azure SQL Database Deployment: Deploy Azure SQL DB using DACPAC
- Azure Web App Deployment: Publish a Visual Studio Web project to Azure Web App using Web Deploy
- Chef: Deploy to Chef environments by editing environment attributes
- Chef Knife: Run Scripts with knife commands on your workstation
- Docker: Deploy a docker image to a remote machine

Manage permissions

Grant or deny permissions to [manage release definitions, environments approvers, or release permissions](#). Set permissions for users, groups, or per release definition.

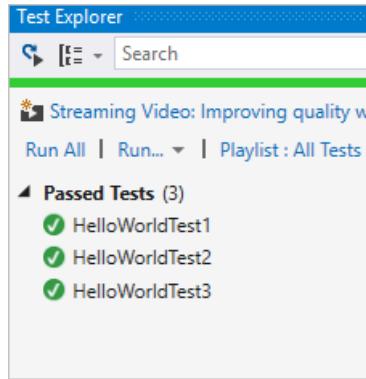
Test

Comprehensive testing

Perform exploratory, manual, system, and user acceptance tests for any app, in any language. Using Visual Studio or 3rd-party test frameworks, you can include automated tests with builds and releases for continuous integration and deployment.

Unit testing with Git

Create unit tests and run them frequently to make sure your code is working properly.



Manual test plans and test cases

Get started by creating test plans and test cases to track manual testing for sprints or milestones.

Shared steps and shared parameters

Create shared steps to include often repeated sequence of steps in your manual test cases, such as logging in. Repeat manual tests with different data using shared parameters.

Coded UI testing

Use Visual Studio to create coded UI tests to test your application's user interface.

Run test with your builds for continuous integration

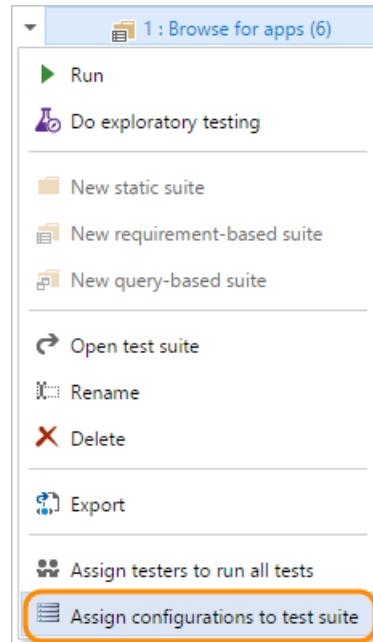
Use continuous integration builds to run tests automatically.

Review automated test results after a build

Review your test results to analyze any problems that were found.

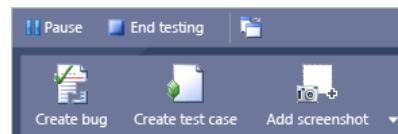
Quickly assign configurations to test plan, test suite, or test case

From the context menu of a test plan, test suite, or test case, you can assign a configuration.



Exploratory testing

Explore user stories without test cases or test steps using Azure Test Plans and exploratory testing.



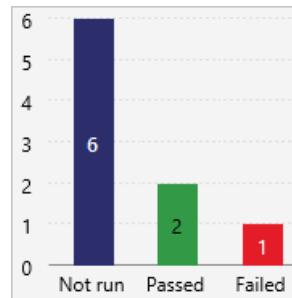
Or, download and install the Test & Feedback extension. Capture screenshots, annotate them, and submit bugs while you explore your web app - all directly from your Chrome browser.

Record and play back manual tests

With Azure Test Plans, you can record your keystrokes and gestures while you test an application. The next time you run the test, you can play back your actions quickly and accurately.

Track test status and test results

Quickly view the status of your testing using lightweight charts.



Test environments

Specify a combination of hardware and software that represents a user or machine environment in which your app runs.

Test permissions

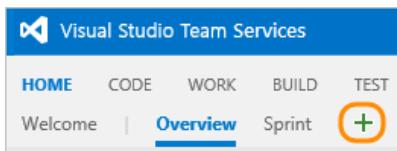
Set permissions on who can manage test configurations, test environments, and publish and delete test results.

Dashboards and reports

Charts and dashboards

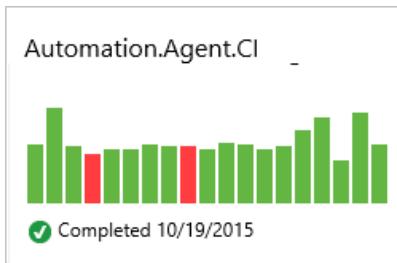
Multiple team dashboards

Each team can create several [team dashboards](#) to help keep both the team and Stakeholders in sync. Each dashboard tile provides quick access to the progress of builds, status of work items, or latest code changes.



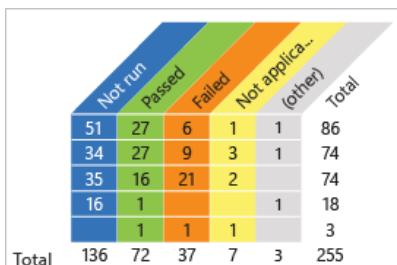
Build history charts

Add [build history charts](#) to your dashboards.



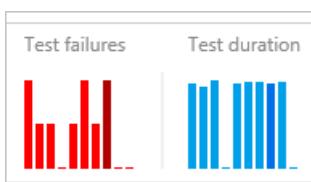
Test charts

Track the status of your [test progress](#) and [test runs](#). Optionally add these charts to a dashboard.



Test quality trend charts

Add [failure](#) and [duration](#) charts for tests run as part of your build to your team dashboard.



Restrict or allow team members to manage dashboards (Azure DevOps Services)

Set permissions to restrict or allow team members to manage dashboards.

Capacity planning and tracking

Easily track how much work your team has completed and has left to do in a sprint by adding the [sprint capacity chart widget](#) to your dashboard.



Share dashboards with Stakeholders

Grant non-licensed users access as Stakeholders ([Azure DevOps Services | TFS](#)) so they can view progress, run queries, and contribute ideas.

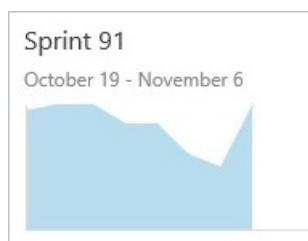
Velocity charts

[Team velocity](#) tracks the total estimated effort (story points or size) of backlog items (user stories or requirements) completed or still in progress within each sprint.



Sprint burndown charts

Monitor progress and review team patterns from [sprint burndown charts](#)



Add release summary to dashboard (Azure DevOps Services)

Add a [release summary chart](#) to a team dashboard.

Edit dashboard mode

Add, remove, move, and configure widgets by [choosing the Edit dashboard icon](#). Choose the checkmark icon to exit.



Auto-refresh dashboards

You can [enable auto-refresh](#) for any [team dashboard](#), and it automatically updates every five minutes. This is a useful feature for when your dashboard serves as a team wallboard.

Widget catalog

Add [widgets](#) to your dashboard to provide information and monitor the data your team needs.



Work item query charts

View the status of work in progress by [charting the results of a flat-list query](#). You can create several types of charts—such as pie, column, or trend—for the same query. Optionally add these charts to a dashboard.

Drag-n-drop layout

Configure the layout to your specifications by [dragging tiles into the sequence you want](#).

Cumulative flow diagrams

Track the progress of work on your backlog [through the CFD charts](#).

Power BI dashboards (Azure DevOps Services)

You can create dashboards, individual reports, or explore data collected for your Visual Studio Online account once you [connect to Power BI](#).

Power BI dashboards and reports (Azure DevOps Services)

<p>Basic Power BI concepts</p> <p>The 3 major building blocks of Power BI are dashboards, reports, and datasets.</p> <p>Get started</p> <p>You can create dashboards, individual reports, or explore data collected for your organization once you connect to Power BI.</p>	<p>Connect to Power BI</p> <p>Steps required to authorize Power BI to access your organization.</p> <p>Available data</p> <p>The Power BI Data Connector supports building reports to track status and trend work items.</p>
---	--

SQL Server Reports (TFS)

<p>Reporting Services reports</p> <p>You can analyze the progress and quality of your project by using the out-of-the-box reports in SQL Server Reporting Services. These reports aggregate metrics from work items, version control, test results, and builds. They are uploaded when you create a project based on the process - Agile, Scrum, or CMMI - that you choose.</p> <p>Add Reporting Services reports</p> <p>If you need to add reporting services to a project or on-premises TFS after you've created your team projects, you can by adding a report server and uploading reports.</p> <p>Manage the data warehouse</p> <p>The reporting warehouse is a traditional data warehouse that consists of a relational database and an Analysis Services database. You manage it through the following activities:</p> <ul style="list-style-type: none">- Manually process the data warehouse- Rebuild the data warehouse- Resolve schema conflicts- Change a process control setting	<p>Build reports</p> <p>Build reports track the quality of software under development. By defining tests to run automatically as part of each build definition and instrumenting tests to gather code coverage data, you can gain insight about the quality of the builds, tests, and code.</p> <ul style="list-style-type: none">- Build Quality Indicators (Agile & CMMI)- Build Success Over Time- Build Summary <p>Test and bug reports</p> <p>Test planning reports support monitoring the test progress and coverage of backlog items or user stories. Bug tracking reports illustrate the team's capacity to find and resolve bugs.</p> <ul style="list-style-type: none">- Test Case Readiness- Test Plan Progress- Bug Status (Agile & CMMI)- Bug Trends (Agile & CMMI)- Reactivations (Agile & CMMI) <p>Required team activities to generate useful reports</p> <p>To gain useful, actionable information from your reports, team members must perform certain activities.</p>	<p>Project management</p> <p>Project management reports provide insight into how much work the team is tackling within a sprint or release, and the rate of their progress. By linking work items and updating specific fields as work is performed, you can track the progress of individual stories and be able to more accurately estimate future activities.</p> <p><i>Scrum reports</i></p> <ul style="list-style-type: none">- Backlog Overview- Release Burndown- Sprint Burndown- Velocity <p><i>Agile and CMMI</i></p> <ul style="list-style-type: none">- Burndown and Burn Rate- Remaining Work- Requirements Overview (CMMI)- Requirements Progress (CMMI)- Status of All Iterations (similar to Velocity)- Stories Overview (Agile)- Stories Progress (Agile)- Unplanned Work <p>Set permissions to view or create reports</p> <p>Enable members of your team to view or manage Reporting Services reports. To create or modify reports, you need to grant them access to read databases.</p>
--	---	--

Widgets

<p>What is a widget?</p> <p>You build your dashboards by adding information tiles or widgets. The widget catalog provides a</p>	<p>Plan and track work</p> <p>Assigned to me widget</p> <p>Provides quick access to work items assigned to the logged in user.</p>	<p>Plan and track work (continued)</p> <p>Sprint burndown</p> <p>Adds a burndown chart for tracking a team's Scrum progress for the</p>
--	--	---

number of predefined widgets.

Drag-and-drop widgets

Drag widgets, tiles, or charts anywhere on a dashboard to [configure the layout you want](#).

Informational content and other links

Markdown widget

Adds a configurable tile to your dashboard to [display any type of information, guidance, or links](#) that you want using markdown syntax.

Team Updates

- New - User Story 2830 created
- New - Bug 9530 created
- Update - Today's design meeting has been *canceled*
- Update - Spec is ready for [User Story 4295](#)
- Reminder - Work on PO bugs before features

Team member

Opens the team's quick dialog to [add or remove team members](#).

Members



Team rooms

Provides [status and access to a team room](#), an archived space to discuss work in progress, ask questions, share status, and clarify issues that arise.

Visual Studio widget

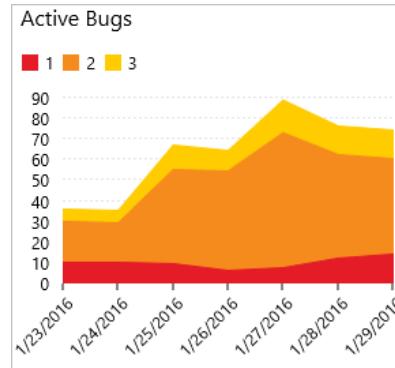
Provides [links to open or download Visual Studio](#). The Visual Studio IDE client comes with the Team Explorer plug-in which provides quick access to several features (some of which aren't available through the web portal).

Welcome widget

Provides quick access to [getting started info on how to track work, code, build, and test](#).

Chart for work items

Adds a configurable tile to display the [chart for a shared query](#).



current sprint.

Sprint capacity

Adds a [chart for tracking remaining capacity](#) when tracking a team's Scrum progress for the current sprint.



New work item

Add [work items](#) pre-scooped to your team's default area and iteration paths.

New work item

Enter title

Bug

Bug

Epic

Feature

Issue

Task

Test Case

User Story

Other links widget

Provides quick access links from a team dashboard to [request feedback, define sprints, and modify your team's area paths](#).

Other links

[Request feedback](#)

[Configure schedules and iterations](#)

[Configure work areas](#)

Query tile

Configurable tile to display the [results and link to a shared query](#).



Query results

sprint.

Sprint overview

Displays a visual overview of the [current sprint progress](#) for tracking a team's Scrum progress for the current sprint, indicating the number of backlog items in progress, completed, or not started.

Work links

Provides quick access links from a team dashboard to open the [team backlog, Kanban board, task board, and queries](#).

Build and test widgets

Chart for build history

Configurable tile to display the [histogram for a specific build definition](#).

Deployment status (Azure DevOps Services)

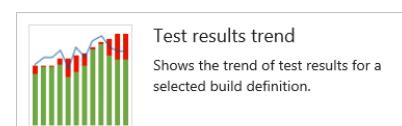
Configurable tile that shows you a consolidated view of the [deployment status and test pass rate across multiple environments](#) for a recent set of builds.

Release definition overview

Configurable tile to view and track the status of a release definition. The widget [shows the release as a series of environments, with the name of the release and the date or time it was started](#).

Test trend results

Provides [trend of test results](#), such as passed or failed tests, for a selected build definition.



Extensibility

Marketplace widgets



Manage Work
[Add work to your board](#)



Collaborate on code
[Add code to your repository](#)



Continuously integrate
[Automate your builds](#)



Visualize progress
[Learn how to add charts](#)

Adds a configurable [query results list](#) to a team dashboard.

Requirements quality

Displays a configurable widget that you can use to [track quality continuously from a build or release definition](#).

You can find additional widgets by browsing the [Marketplace](#)

Dashboard widget SDK

[Create a dashboard widget](#) using the REST API service.

Code widgets

Code tile

Configurable tile to display [status](#) and [links](#) to a Git or TFVC code repository, branch, or folder.

Pull request

Adds a configurable tile to display active pull requests requested by the team, or assigned to or requested by the person logged in. You select the Git repository for the pull requests of interest.

Pull Request in Fabrikam (2)



Updated ProjectController.cs
Dan Paul into [`master`](#) features/VirutalParameters, creat



Fixed layout issues, bug #8730
John Smith into [`master`](#), created 13 minutes ago

Extensibility

Marketplace

Feature availability: You can add Marketplace extensions from the web portal for Azure DevOps Services or TFS 2015.2 or later version or for Visual Studio or Visual Studio Code.

What is the Marketplace?

From the [Marketplace](#), you can extend the functionality available to you by installing free extensions or purchasing a subscription or paid extension. Extensions support adding new capabilities to Visual Studio, Visual Studio Code, Azure DevOps Services, or TFS.

Featured



Exploratory Testing

Microsoft

Explore your app, find and submit bugs directly from your browser

[PREVIEW](#)



Test Manager

Microsoft

Integrated test management system for all your manual, exploratory and user

[PAID](#)

Subscriptions

[Visual Studio subscriptions](#) are a way for you to get the Visual Studio IDE, team collaboration benefits like Azure DevOps Services and TFS, and subscriber benefits like dev/test use of Windows, Windows Server, and SQL Server.

Extensions

You can [get and quickly install extensions](#) to add functionality to Visual Studio, Visual Studio Code, or Azure DevOps Services.

Try Azure Test Plans for free

You can [start a trial for Azure Test Plans for free](#).

Get extensions for...

- [Azure DevOps Services](#)
- [Visual Studio](#)
- [Visual Studio Code](#)

Get cloud subscriptions

Buy [cloud subscriptions](#) in the Marketplace.

REST APIs

Get started with REST APIs

Learn the basic patterns for [using the REST APIs](#) for Azure DevOps Services and TFS.

Authorization

Get authorization from your customers to access Azure DevOps Services resources using [OAuth 2.0](#).

REST API reference

Use the [REST APIs](#) to work with Azure DevOps Services and TFS resources.

.NET client libraries

For .NET developers building Windows apps and services that integrate with Visual Studio Online, [client libraries](#) are available for integrating with work item tracking, version control, build, and other services are now available. These packages replace the traditional TFS Client OM installer and make it easy to acquire and redistribute the libraries needed by your app or service.

REST API samples

Here are a number of [samples](#) that work with the REST APIs directly.

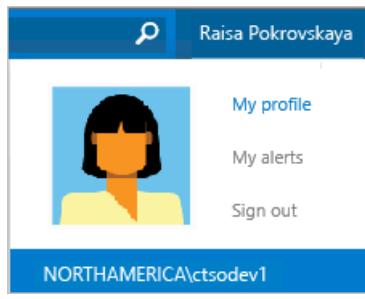
C# client library samples

Here are a few quick [samples](#) to help you get started with the client libraries.

Service hooks

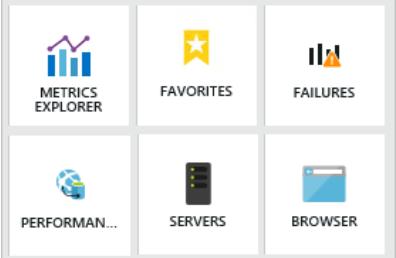
<p>Integrate with service hooks</p> <p>Service hooks enable you to perform tasks on other services when events happen in your Visual Studio Online projects</p> <p>Create integrations</p> <p>Integrate other services like HipChat, Slack, and UserVoice with Azure DevOps using service hooks.</p>		<p>Authorize</p> <p>Authorize other services to access your organization using the industry standard OAuth 2.0. OAuth 2.0 provides safe, secure access to your resources like work items, source code and build results by those other services.</p>
--	--	---

Global

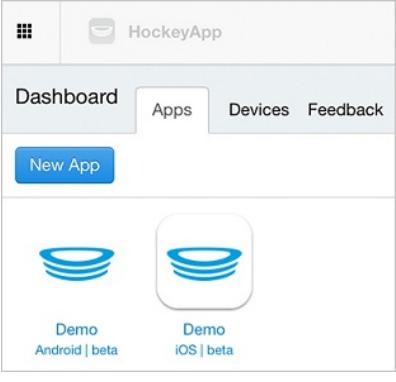
<p>Web portal preferences</p> <p>Choose your name to access your profile settings and set your web portal preferences which include language (currently only English is supported for Azure DevOps), date and time pattern, and time zone.</p>  <p>Language Interface Packs (LIPs)</p> <p>By using a Windows Language Interface Pack (LIP), you can install a language version of Windows, and then install various User Interface Language Packs. Language packs switch your English Visual Studio Professional user interface into any of these languages and have a majority of the user interface localized.</p>	<p>Localized content</p> <p>Most content that supports Azure DevOps Services and TFS is localized into the following 14 languages.</p> <ul style="list-style-type: none"> • English • Brazilian Portuguese • Chinese Simplified • Chinese Traditional • Czech • German • French • Italian • Japanese • Korean • Polish • Russian • Spanish • Turkish <p>Currently, the visualstudio.com content is only available in English.</p>	<p>Visual Studio language pack</p> <p>Install the language pack to switch the UI display to different languages. Visual Studio provides localized UI support for these 14 languages.</p> <ul style="list-style-type: none"> • English • Brazilian Portuguese • Chinese Simplified • Chinese Traditional • Czech • German • French • Italian • Japanese • Korean • Polish • Russian • Spanish • Turkish <p>Eclipse plug-in language support</p> <p>Install Team Explorer Everywhere, which includes language support for English, French, German, Japanese, and Simplified Chinese.</p>
--	--	--

Monitor

Application Insights (Preview)

<p>What is Application Insights</p> <p>Application Insights, an extensible analytics service that monitors your live web application, supports developers to continuously improve the performance and usability of apps. With it you can detect and diagnose performance issues, and understand what users actually do with your app.</p> <p>Web site availability monitoring</p> <p>Know when your site or service goes down by setting up tests and performance thresholds to monitor both uptime and responsiveness.</p> <p>Web site performance & usage</p> <p>Open the Performance blade to see request, response time, dependency and other data.</p> <p>Power BI integration</p> <p>Get even more flexible views of your telemetry, and present your web app telemetry alongside data from devices and other business sources.</p>	<p>Dashboard</p> <p>Get the full picture with customizable dashboards that track application health alongside usage metrics and app crashes. Within the dashboard, you can filter, search, and drill down to an event instance for more detail or to segment data.</p>  <p>Diagnose failures and exceptions</p> <p>Quickly diagnose causes and correlate failed requests with exceptions and other events at both the client and server.</p>	<p>Usage analysis</p> <p>Gain a clear view of where your users are coming from and how they use your app. Add custom instrumentation to determine usage patterns and next version investment areas.</p> <p>Diagnose dependency issues</p> <p>See how long your application waits for dependencies and how often a dependency call fails. Dependencies are external components that your app calls such as an HTTP service, database, or file system.</p> <p>Custom data collectors</p> <p>Add custom data collectors to your app using the Application Insights API to customize your telemetry data.</p> <p>Continuous data export</p> <p>Perform custom analysis on your telemetry through continuous export of your data.</p>
---	---	--

HockeyApp

<p>Get HockeyApp for mobile app development</p> <p>Distribute mobile apps for testing, collect user metrics and feedback, and respond to crashes more easily by adding HockeyApp to your Agile, continuous integration, and continuous delivery workflows.</p> <p>Simplified distribution</p> <p>Manage distribution of development and production versions of your apps and use independent bundle identifiers that can run in parallel on the same device.</p> <p>Integrate with Azure DevOps Services and TFS</p> <p>Integrate HockeyApp directly in Azure DevOps Services or TFS to upload your Android, iOS, or Windows builds.</p>	<p>Comprehensive dashboard</p> <p>Manage all your apps, users, and devices from a single dashboard. Monitor crashes and feedback as well. As an admin, you'll have full control over which user can see and install which app.</p> 	<p>Invite or recruit testers</p> <p>Invite beta testers and distribute your beta versions through the dashboard.</p> <p>Usage</p> <p>Get advanced metrics to understand the testing performed on your app. See which devices were tested, which testers used the app for how long, and which language was tested.</p> <p>Crash reports</p> <p>Get the information you need to analyze and respond to crashes by getting symbolicated stack traces and environment details.</p> <p>Webhooks</p> <p>Use webhooks to receive notifications about new versions, crash groups, and feedback.</p>
---	---	---

Navigation

Web portal

Operational hubs

Each hub—[Home](#), [Code](#), [Work](#), [build](#), and [Test](#)—supports specialized functions to share information, view and create dashboards, collaborate on code, plan and track work, build and test your applications, plus much, much more.

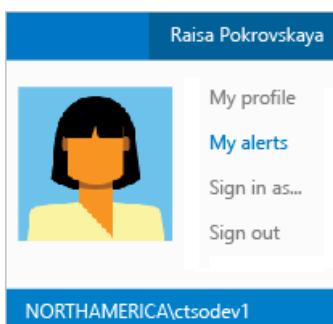
Home Code Work Build & Release Test

Project page

To view and quickly navigate to teams, team projects, branches, work items, pull requests and other objects that are relevant to you, use your [Project page](#).

Your profile and preferences

Choose your name to access [your profile settings](#), set preferences, [create personal access tokens](#) ([Azure DevOps Services](#)), set alerts, and log-in or out.



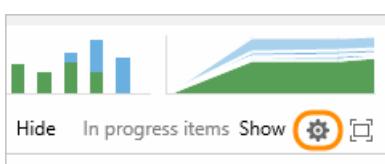
Switch team context

Navigate to a different team or project from the top row.



Change team settings

Customize features to meet your team needs by [configuring your team assets](#).



Home

Provide team guidance through [Welcome](#) (Markdown format) pages and add team [dashboards](#) to monitor progress and trends.

Code

Manage source code using distributed [Git repositories](#) or [Team Foundation version control](#), to

Work

Plan and track work by [creating a product backlog](#), and managing work using [Kanban](#) or [Scrum](#) processes. Find work items you want to review or update by [creating queries](#), or visualize progress by [creating query-based charts](#)

Build

Define and monitor [builds](#) and set up continuous builds to improve the quality of your app.

Test

Create and run [manual tests](#) for your app.

Package (Azure DevOps Services, Preview)

Share code as binary assets and control dependencies by [subscribing to and working with Azure Artifacts feeds](#).

Release (Azure DevOps Services, Preview)

Manage the release of your app by [deploying it to a specific environment for each separate release step](#), and by controlling the process through approvals for each step.

Code search

Search within your code branches ([TFVC](#)) and repositories ([Git](#)) to find files, commits, and more using powerful filters to obtain rich results.

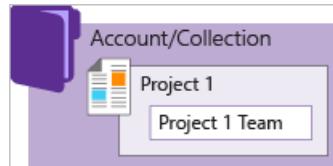


Find work items

When in the Work hub, [enter IDs or keywords to start a query](#) to find work items that you want to review, triage, or update.

Collection-project-team structure

The [collection-project-team structure](#) provides teams a high-level of autonomy to configure their tools in ways that work for them. It also supports administrative tasks to occur at the appropriate level.

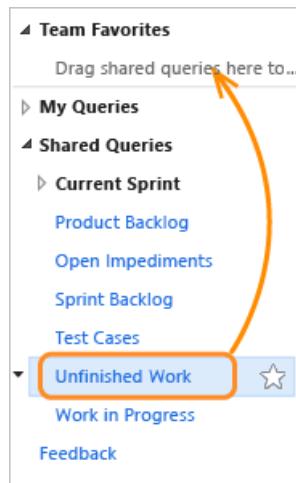


My favorites

From any context, you can drag folders, queries, or builds to My favorites when working in the Code, Work, or Build hubs to provide quick access to those items.

Team favorites

From your team context, drag shared queries, builds, and folders to Team favorites to provide quick access to those items.



Project admin context

Open the admin context to [add teams](#) and [manage permissions](#). From any project hub, choose the gear icon to open the admin context.



Project collection admin context

From the collection admin context, you can [manage collection-level permissions](#), and set build policies, and [manage extensions](#). Choose the gear icon to open the admin context, and then choose

Keyboard shortcuts

Increase your productivity by working with [hot keys and shortcuts](#).

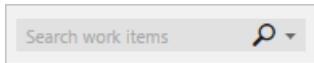
Search work items

DefaultCollection.

Search, queries, and filters

Quick work item search

Find work items based on [ID](#), [assignment](#), [changed date](#), or [keyword](#).



Code search

Find code based on [keywords](#) and [semantic search filters](#) across your Git repositories.



CodeLens search

Find references and changes to your code, linked bugs, work items, code reviews, and unit tests.

Work item queries

Open shared queries or create your own query using the query editor to [list work items or show hierarchical or dependent items](#).

> Manage risks and dependencies

Link work items to [track related work, dependencies, and changes made over time](#).

History & auditing

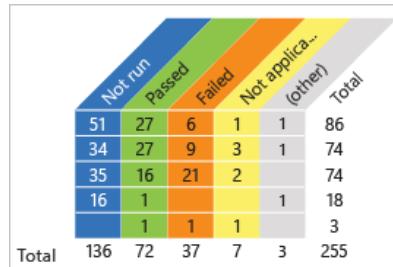
Review and query [work item change history](#) to learn of past decisions and support future ones.

Bulk add or modify using Excel

Bulk add items to [track or modify multiple field values](#) using Excel.

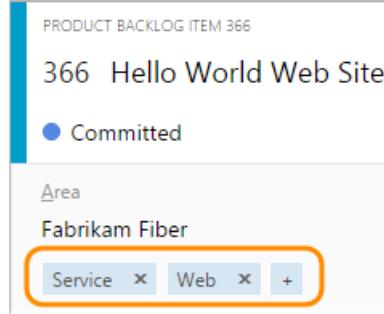
Charts

Turn your [queries into a status or trend chart](#) and share them with your team, organization, and Stakeholders.



Tags

Add [tags to work items](#) to filter backlogs and queries. Bulk update work items to add or remove tags: [Azure DevOps Services | TFS](#).



<p>

Bulk modify

Edit or update [multiple work items](#) from any backlog or query result. Supported tasks include:

- Modify field values
- Add or remove tags
- Reassign
- Move to an iteration
- Delete
- Link to a new or existing work item
- Change work item type
- Move to another project
- Create a new Git branch

Query by date or current iteration

List work items based on [when changes occurred or if they belong to the team's current sprint](#).

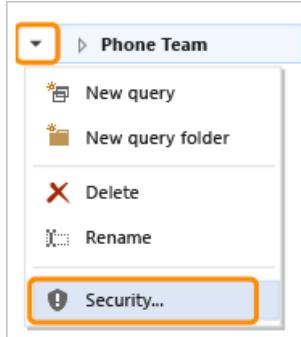
Query by workflow

Find and list work items based on [their current state](#), such as new, in progress, resolved, done, or closed.

Query by Kanban board change

Track status and trends of work items based on [changes made to the Kanban board](#).

Security

<p>Manage users and groups</p> <p>Add users to built-in groups to grant them access to your project. Optionally, create groups to customize access based on your business requirements.</p> <p>Permission states</p> <p>Understand how Allow, Deny, Not set and other permissions states control access to features and objects.</p> <table border="1" data-bbox="155 534 552 893"> <thead> <tr> <th>Permissions</th><th>Members</th><th>Member of</th></tr> </thead> <tbody> <tr> <td colspan="3">Members of this group can add, modify, and delete items within the team project.</td></tr> <tr> <td>Create tag definition</td><td>Inherited allow</td><td></td></tr> <tr> <td>Create test runs</td><td>Allow</td><td></td></tr> <tr> <td>Delete team project</td><td>Deny</td><td></td></tr> <tr> <td>Delete test runs</td><td>Allow</td><td></td></tr> <tr> <td>Edit project-level information</td><td>Not set</td><td></td></tr> <tr> <td>Manage test configurations</td><td>Allow</td><td></td></tr> </tbody> </table> <p>Manage work access (Azure DevOps Services)</p> <p>Control user access with a directory to enforce policies about accessing company resources.</p> <p>Azure Active Directory (Azure DevOps Services)</p> <p>Easily control access to your team's critical resources and key business assets with Azure Active Directory groups.</p> <p>Set up groups (TFS)</p> <p>Create Windows or Active Directory groups to manage access to your team projects and collections.</p> <p>Built-in groups</p> <p>Understand the permissions granted to built-in groups and use them to manage access to your team projects and collections.</p>	Permissions	Members	Member of	Members of this group can add, modify, and delete items within the team project.			Create tag definition	Inherited allow		Create test runs	Allow		Delete team project	Deny		Delete test runs	Allow		Edit project-level information	Not set		Manage test configurations	Allow		<p>DevOps permissions</p> <p>Grant or restrict access to:</p> <ul style="list-style-type: none"> • Git repositories • Git branches • TFVC source code and folders • Build • Test) • Release <p>Work item tracking permissions</p> <p>Control access to specific features by setting permissions for a user or group.</p> <ul style="list-style-type: none"> • Area and iteration paths • Query permissions • Work item tags • Move work items to another project • Permanently delete work items • Provide feedback through the Microsoft Feedback client <p>Team admin role and permissions</p> <p>Add users as team administrators to enable them to configure team settings and manage team assets.</p> <p>Manage administrative permissions</p> <p>[Add users to one of the following built-in groups] to provide them permissions assigned to that group:</p> <ul style="list-style-type: none"> • Project Administrators, who manage shared features for a project • Project Collection Administrators, who manage collection-level features • Team Foundation Server Administrators, who manage on-premises application servers <p>Restrict access</p> <p>You can restrict access to several features and tasks by setting the permission state to Deny to individual users or a security group.</p>	<p>Stakeholder access</p> <p>Grant Stakeholders, non-licensed users, limited access to contribute ideas and access team dashboards.</p> <p>Query permissions</p> <p>Grant permissions to create shared queries and query folders.</p>  <p>Process permissions</p> <p>To customize a process, add custom fields, or change the layout of a work item form, you must be a member of the Project Collection Administrators group or be granted explicit permissions to edit a specific process.</p> <p>Valid users</p> <p>Understand how valid user groups are populated and the permissions they're granted.</p> <p>Permission reference</p> <p>Provide or restrict access for practically any feature, function, or object at the collection or project level.</p> <p>SharePoint permissions (TFS)</p> <p>Grant permissions to view and contribute to SharePoint project portals.</p> <p>SQL Server reporting permissions (TFS)</p> <p>Grant permissions to view and author Excel and SQL Server reports.</p>
Permissions	Members	Member of																								
Members of this group can add, modify, and delete items within the team project.																										
Create tag definition	Inherited allow																									
Create test runs	Allow																									
Delete team project	Deny																									
Delete test runs	Allow																									
Edit project-level information	Not set																									
Manage test configurations	Allow																									

Set up and installation

<p>Free developer offers</p> <p>To get started, download and install Visual Studio an integrated development environment (IDE) that works with Azure DevOps Services and TFS.</p> <p>Migrate from on-premises to hosted</p> <p>You can migrate source code and work items from an on-premises TFS to the cloud.</p>	<p>Sign up for Azure DevOps Services</p> <p>Store your code, tests, and test results in the cloud with Azure DevOps Services, as well as plan your project and track progress.</p> <p>Install TFS</p> <p>Download and install the latest version of Team Foundation Server. TFS provides the collaboration hub to support your teams DevOps tasks. at the center of the Microsoft devops solution.</p>	<p>Email configuration (TFS)</p> <p>For feedback requests, alerts, and other special controls to work, you must configure an SMTP server for your on-premises TFS.</p> <p>Automated, scheduled backups (TFS)</p> <p>Reduce the risk of lost data by scheduling automated backups of the data store.</p> <p>Built-in SQL Server database (TFS)</p> <p>For small teams, you can install TFS using SQL Server Express which installs with TFS.</p>
---	--	--

Teams, team projects, and processes

Processes and process guidance

What is a process?

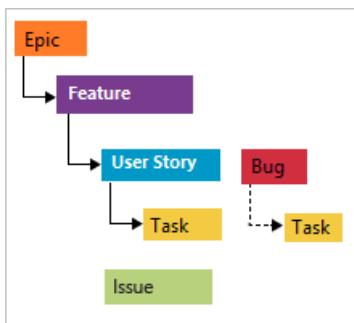
A [process defines the building blocks](#) of the work item tracking system as well as other sub-systems you access through your project.

Compare and choose a process

Compare the three core system processes--[Agile](#), [Scrum](#), [CMMI](#)--before you choose one to create a project.

Agile process

Choose [Agile](#) when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. With Agile, you can track user stories and bugs on the Kanban board, or track bugs and tasks on the task board.



Customize a process (Azure DevOps Services)

Customizations you make to an inherited process automatically update all team projects that reference that process. You can customize your project as follows:

- Add and modify fields
- Modify the web form layout
- Modify the workflow states
- Add a custom work item type

Manage processes (Azure DevOps Services)

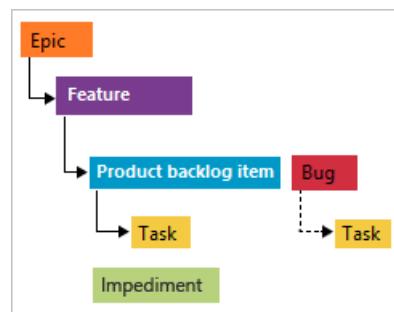
Create [inherited processes](#) and [migrate team projects](#) to use them. Set the default process and enable, disable, or delete processes you no longer want to use.

Kanban process tools

You can use the Kanban board with any process--Agile, Scrum, CMMI--or project that you select or create. Agile Kanban tools support working with the [Kanban board](#), adding [task checklists](#), setting [WIP limits](#), [custom columns](#), [split columns](#), [custom swimlanes](#), and [customizing cards](#).

Scrum process

Choose [Scrum](#) when your team practices Scrum and you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the task board.



Scrum work items and workflow process guidance

Plan and track your work using the [work item types and workflow supported by the Scrum process](#).

Agile work items and workflow process guidance

Plan and track your work using the [work item types and workflow supported by the Agile process](#).

Work item field index

For descriptions and usage of each field used by the core and inherited processes, see [Work item field index](#).

Scrum process tools

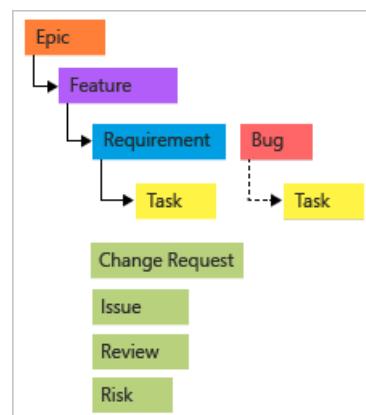
Scrum processes can be used with any process--Agile, Scrum, CMMI--or project that you select or create. Agile Scrum tools support [sprint planning](#), [capacity planning](#), [task boards](#), and [burndown charts](#).

Manage processes (Azure DevOps Services)

Add users to [built-in groups](#) to grant them access to your project. Optionally, create groups to customize access based on your business requirements.

CMMI process

Choose [CMMI](#) when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. CMMI supports tracking requirements, change requests, risks, and reviews.

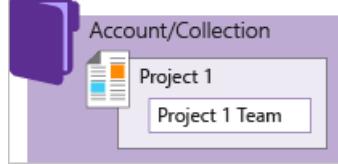


CMMI work items and workflow process guidance

Plan and track your work using the [work item types and workflow supported by the CMMI process](#).

<p>What is a process template?</p> <p>A process template is the forerunner and on-premises version of a process. It provides the building blocks of the work item tracking system as well as other sub-systems you access through your project. Process templates support full customization of all its objects.</p> <p>Manage process templates</p> <p>Download and upload process templates to support customization and upgrade of your work tracking experience and team projects.</p>	<p>Process template files</p> <p>You customize the initial configuration of team projects by customizing one or more process template files. By customizing these files, you can define the initial configuration of all team projects that are created from the process template.</p> <p>Configure Features Wizard</p> <p>Use the Configure Features Wizard to configure team projects after a TFS upgrade to access new features.</p>	<p>Changes made to process templates</p> <p>For a catalog of changes, see Changes made to process templates.</p> <p>Customize the Microsoft Project field mapping file</p> <p>You can customize how work item fields that are defined in Team Foundation map to fields in Microsoft Project. And, you can change how specific fields are published.</p>
--	---	---

Team projects

<p>What is a project?</p> <p>A project provides a repository for source code and a place for a group of developers to plan, track progress, and collaborate on building software solutions. A project lives within a project collection. You can grant permissions to and customize a project to support your business needs.</p> <p>Create a project</p> <p>You can create a project hosted in the cloud (Azure DevOps Services), avoiding maintenance and administrative overhead, or create a project on an on-premises TFS.</p> <p>Rename a project</p> <p>Rename a project as needed to reflect changes that occur within your org.</p> <p>Delete a project</p> <p>Simplify the navigation to team projects that are in use by deleting team projects you no longer use.</p>	<p>Collection-project-team structure</p> <p>The collection-project-team structure provides teams a high-level of autonomy to configure their tools in ways that work for them. It also supports administrative tasks to occur at the appropriate level.</p>  <p>Change the process (Azure DevOps Services)</p> <p>You change the process of a project to apply customizations you've made to an inherited process. You can add and modify fields and modify the layout of each work item type defined for that process.</p>	<p>View your work across teams and team projects</p> <p>From your Project page, you can view and quickly navigate to teams, team projects, branches, work items, pull requests and other objects that are relevant to you and that are stored in different team projects within the organization or collection.</p> <p>Customize a project (TFS)</p> <p>You customize a project defined on an on-premises TFS by modifying definition files for work item types or process configuration, or changing field attributes.</p> <p>Update a project after an upgrade (TFS)</p> <p>Some features added when you upgrade your on-premises application server may require you to configure features to access them.</p> <p>Upload reports (TFS)</p> <p>Upload the latest reports provided for your process or add reports after you've already created a project by adding SQL Server Reporting Services.</p>
---	--	--

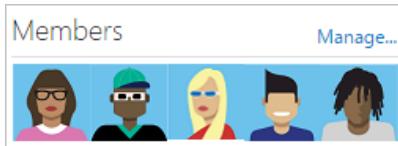
Teams

What is a team?

A team is an organizing unit used to support a number of [team-configurable tools](#) to plan and manage work and facilitate collaboration.

Add team members

Add organizations-[Azure DevOps Services](#) | [TFS](#)--to a team to enable users to share code, plan and track work, and access other team assets and resources.



Add a team

As your organization grows, consider moving from your [default team of one to two or more teams](#) to support feature-focused groups within your org.

Add a team admin

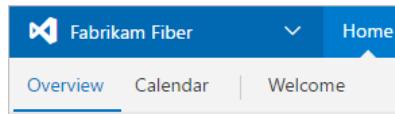
Add users to the team admin role to enable them to [Manage teams and configure team tools](#). Team settings can only be configured by a team or project admin.

Support Stakeholders

Members within your org who don't have a license or contribute to developing the code base [can track project priorities and provide direction, feature ideas, and business alignment to a team](#).

Team dashboards

Share progress, status, and guidance with your team using configurable team dashboards.



Team welcome page

Provide in-project guidance through the [Welcome page and other pages you format using Markdown](#).

Setup a team hierarchy

By [configuring your teams and backlogs into an hierarchical structure](#), program owners can more easily track progress across teams, manage portfolios, and generate rollup data.

Set team defaults

Several Agile tools reference the team's default area path, iteration path, and activated sprints to automatically filter the set of work items they display. Understand how defaults are used] (./organizations/settings/about-teams-and-settings.md).

Select team sprints

[Select your team's sprints](#) to gain access to sprint backlogs and task boards.

+ Select iteration(s) X Remove New New child		
Iteration	Start Date	End Date
Fabrikam Fiber\Iteration 1	10/3/2016	10/21/2016
Fabrikam Fiber\Iteration 2	10/24/2016	11/11/2016
Fabrikam Fiber\Iteration 3	11/14/2016	12/2/2016

Configure team settings

Configure, customize, and manage all [team-related activities](#)

Team alerts

As changes occur to work items, code reviews, source control files, and builds, your team can automatically [receive email notifications for alerts](#) that you define.

Team rooms

Team rooms, like chat rooms, provide teams with a [space to discuss work in progress, ask questions, share status, and clarify issues](#) that arise. Use team rooms to foster and capture communication among team members, both near and far.

Team groups

A [team group is created](#) when you create a team. Use this group in queries or to set permissions for your team.

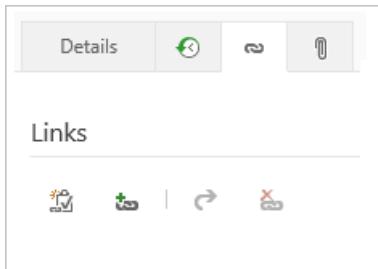
Traceability

Work item history & auditing

Review and query [work item change history](#) to learn of past decisions and support future ones.

Manage risks and dependencies

Link work items to [track related work, dependencies, and changes made over time](#). Create queries based on link type to monitor dependencies.

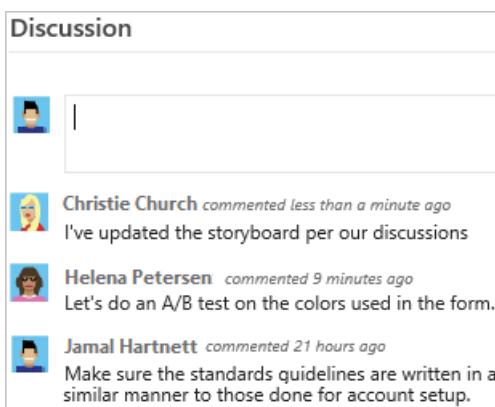


Rich text comments

Describe and comment on work to perform using [formatted text, hyperlinks, and inline images](#).

Discussion (Azure DevOps Services)

Add or review comments added to a work item. Start by choosing the discussion icon.



Storyboard

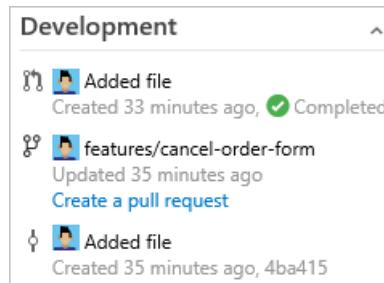
[Link your storyboards to your backlog work items](#).

Git code changes

Get detailed information about what changes have been made to your local and centralized branches and [repositories](#), compare files and folders, review history of commits and file changes.

Integrate Git development with work tracking (Azure DevOps Services)

Drive Git development and stay in sync as a team to complete backlog items and tasks using the [Git Development section](#). Add branches, create pull requests, and view all development performed to support the specific work item.



TFVC code changes

Get detailed information about what changes have been made to your files, compare files and folders, view where and when changesets have been merged, and view file changes using [annotate](#).

Build changes

Determine who [changed what in the build definition and when they did it](#).

Release audit history

Retain full audit history of all activities performed on a release with detailed release logs and approval tracking.

Release logs

View or download log files as zip files. Log files contain the status for each step or task of a release, for each of the environments in the release definition. Each completed release--succeeded, failed, or abandoned--includes a [live log file, details, and history for each step or task](#).

Related articles

We add new features frequently. We'll work to keep this list up-to-date. Other resources you might want to bookmark:

- [Azure DevOps Services - Features update](#)
- [Microsoft devops blog](#)

Get started today using our cloud offering, [Azure DevOps Services](#), or our [on-premises TFS server](#).

Choosing the right authentication mechanism

6/25/2019 • 3 minutes to read • [Edit Online](#)

When writing an application which interfaces with Azure DevOps Services, you will have to authenticate to gain access to resources like REST APIs. We understand that Azure DevOps Services offers many different ways to authenticate your application. This topic provides guidance to help you choose the right authentication for your application. The following table outlines the recommended authentication mechanism for different application types. We have provided basic descriptions, examples, and code samples to get you started.

Type of Application	Description	Example	Authentication Mechanism	Code Samples
Interactive client-side (REST)	Client application, that allows user interaction, calling Azure DevOps Services REST APIs	Console application enumerating projects in an organization	Active Directory authentication library (ADAL)	sample
Interactive client-side (Client library)	Client application, that allows user interaction, calling Azure DevOps Services Client libraries	Console application enumerating bugs assigned to the current user	Client libraries	sample
Interactive Javascript	GUI based Javascript application	AngularJS single page app displaying project information for a user	Active Directory authentication Library for JS (ADAL JS)	sample
Non-interactive client-side	Headless text only client side application	Console app displaying all bugs assigned to a user	Device Profile	sample
Interactive client-side app targeting Azure DevOps Services and TFS	Client application, that allows user interaction, authenticates Azure DevOps Services and TFS users	Console application allowing Azure DevOps Services and TFS users to see assigned bugs	Client Library (Interactive and Windows authentication)	sample
Interactive web	GUI based web application	Custom Web dashboard displaying build summaries	OAuth	sample
TFS application	TFS app using the Client OM library	TFS extension displaying team bug dashboards	Client Libraries	sample
Azure DevOps Services Extension	Azure DevOps Services extension	Agile Cards	VSS Web Extension SDK	sample walkthrough

NOTE

The Azure DevOps API doesn't support non-interactive service access via service principals.

To learn more about how security and identity are managed, see [About security and identity](#).

To learn more about how we store your credentials, see [Credential storage for Azure DevOps](#).

Enabling IIS Basic Authentication invalidates using PATs for TFS

Learn more about [using IIS Basic Authentication with TFS on-premises](#).

Q&A

Q: I am making an interactive client-side application. Should I use Azure DevOps Services Client Libraries or Azure DevOps Services REST APIs?

A: We recommend using Azure DevOps Services Client Libraries over REST APIs when accessing Azure DevOps Services resources. They are simpler and more easily maintained when version changes to our REST endpoints occur. If there is missing functionality from the client libraries [ADAL](#) is the best authentication mechanism to use with our REST APIs.

Q: Can I use ADAL if I log into my organization with a Microsoft account (MSA)?

A: Yes, you can use ADAL to create client side applications for an MSA backed account using ADAL with some limitations. Instead of configuring ADAL with a `Client ID` or `Reply URL` from Azure Portal, MSA users can use the `Client ID: "872cd9fa-d31f-45e0-9eab-6e460a02d1f1"` and `Reply URL: "urn:ietf:wg:oauth:2.0:oob"` as replacement values to get a valid ADAL access token without needing an Azure Active Directory.

Note: This approach will only work for client side applications. For JS web apps, ADAL JS will not work without an Azure AD tenant.

Q: Is this guidance only for Azure DevOps Services or is this also relevant for on-prem TFS users?

A: This guidance is mainly for Azure DevOps Services users. [Client Libraries](#) are a series of packages built specifically for extending TFS functionality. For on-prem users, we recommend using the [Client Libraries](#), Windows Auth, or [Personal Access Tokens \(PATs\)](#) to authenticate on behalf of a user.

Q: What if I want my application to authenticate with both TFS and Azure DevOps Services?

A: The best practice is to have different authentication paths for TFS and Azure DevOps Services. You can use the `requestContext` to find out which you're hitting and then use the best mechanism for each. Alternatively, if you want a unified solution, [PATs](#) will work for both.