

Permissions, users, and groups in Azure DevOps

06/05/2020 • 63 minutes to read •  +9

In this article

[User accounts](#)

[Groups](#)

[Collection-level groups](#)

[Project-level groups](#)

[Team administrator role](#)[Permissions](#)[Collection-level permissions](#)[Project-level permissions](#)[Analytics views \(object-level\)](#)[Dashboards \(object-level\)](#)[Build \(object-level\)](#)[Git repository \(object-level\)](#)[TFVC \(object-level\)](#)[Area path \(object-level\)](#)[Iteration Path \(object-level\)](#)[Work item query and folder \(object-level\)](#)[Delivery Plans \(object-level\)](#)[Process \(object-level\)](#)[Work item tags](#)[Release \(object-level\)](#)[Task group \(Build and Release\) permissions](#)[Notifications or alerts](#)[Related articles](#)

Azure DevOps Services | Azure DevOps Server 2020 | Azure DevOps Server 2019 | TFS 2018 - TFS 2013

This article provides a comprehensive reference for each built-in user, group, and permission. It's a lot of information describing each built-in security user and 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:

Users and groups

- [Add users to an administrator role](#)
- [Add users to an organization](#)

DevOps permissions

- [Git branch](#)
- [Git repositories](#)
- [TFVC](#)
- [Build and release](#)

Work tracking

- [Area and iteration paths](#)
- [Work item queries and folders](#)
- [Plan permissions](#)

- [Add users to a project or a team](#)
- [Make a user a team admin](#)

- [Approvals and approvers](#)
- [Task groups](#)
- [Variable groups](#)
- [Role-based resources](#)

- [Customize process](#)

Wiki

- [README & Wiki](#)

Reporting permissions

- [Dashboard permissions](#)
- [Analytics](#)
- [Analytics views](#)

7 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.

User accounts

There are a few user accounts that are generated by the system to support specific operations. These include those described in the following table. These user accounts are added at the organization or collection level.

User name	Description
Agent Pool Service	Has 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.
PipelinesSDK	Added as needed to support the Pipelines policy service scope tokens. This user account is similar to the build service identities but supports locking down permissions separately. In practice, the tokens that involve this identity are granted read-only permissions to pipeline resources and the one-time ability to approve policy requests. This account should be treated in the same way that the build service identities are treated.

<i>ProjectName</i>	Has permissions to run build services for the project. This is a legacy user used for XAML builds. It is added to the Security Service Group, which is used to store users who have been granted permissions, but not added to any other security group.
Build Service	
Project	Has permissions to run build services for the collection. It is added to the Security Service Group, which is used to store users who have been granted permissions, but not added to any other security group.
Collection	
Build Service	

Groups







Permissions can be granted directly to an individual, or to a group. Using groups makes 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.



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 not remove or delete the built-in collection-level groups.

7 Note

To enable the new user interface for the Organizations Permissions Settings Page v2, see [Enable preview features](#). The preview page provides a group settings page that the current page does not.

Permissions		+ New Group
<div>GroupsUsers</div>		<input type="text" value="Search groups or users"/>
Name	Description	
 [fabrikam]\Project Collection Administrators	Members of this application group can perform all privileged operations on the Team Project Collection.	
 [fabrikam]\Project Collection Build Administrators	Members of this group should include accounts for people who should be able to administer the build resources.	
 [fabrikam]\Project Collection Build Service Accounts	Members of this group should include the service accounts used by the build services set up for this project collection.	
 [fabrikam]\Project Collection Proxy Service Accounts	This group should only include service accounts used by proxies set up for this team project collection.	
 [fabrikam]\Project Collection Service Accounts	This application group contains Team Project Collection service accounts.	
 [fabrikam]\Project Collection Test Service Accounts	Members of this group should include the service accounts used by the test controllers set up for this project collection.	

	[fabrikam]\Project Collection Valid Users	This application group contains all users and groups that have access to the Team Project Collection.
	[fabrikam]\Security Service Group	Identities which are granted explicit permission to a resource will be automatically added to this group if they were not previ...

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 <i>CollectionName</i>\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> <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. This is a legacy group used for XAML builds. Use the Project Collection Build Service ({your organization}) user for managing permissions for current builds
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	Has service level permissions for the collection and for Azure	Contains the service account that was supplied during installation. This group should contain only service accounts and

Accounts	DevOps Server.	groups that contain only service accounts. By default, this group is a member of the Administrators group.
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.
Security Service Group	Used to store users who have been granted permissions, but not added to any other security group.	Don't assign users to this group. If you are removing users from all security groups, check if you need to remove them from 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**.

7 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.

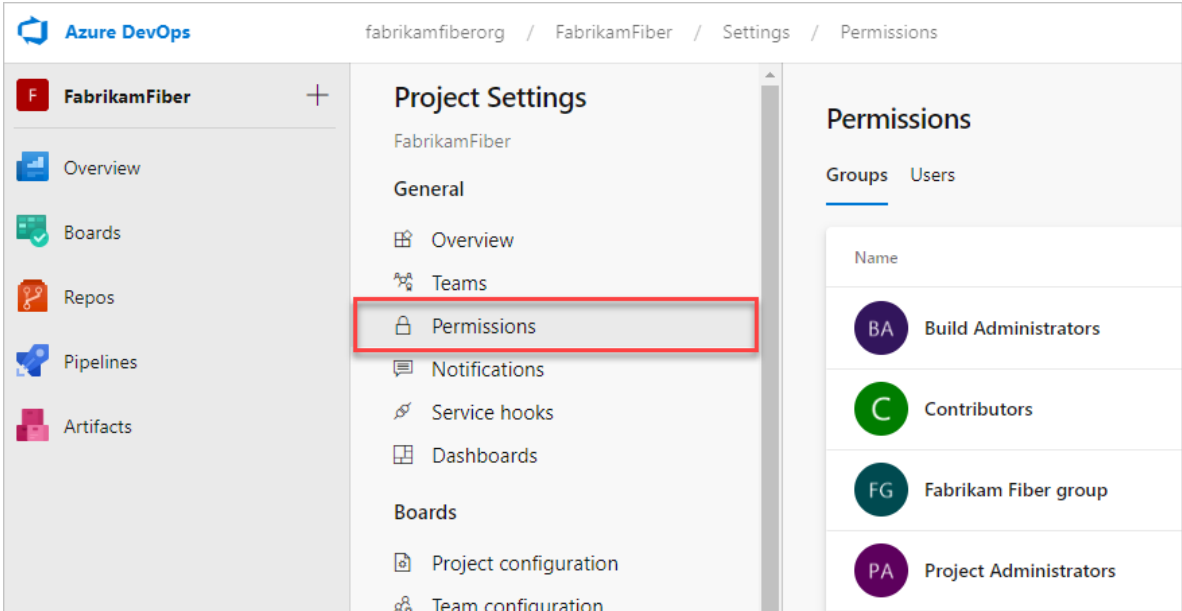
7 Note

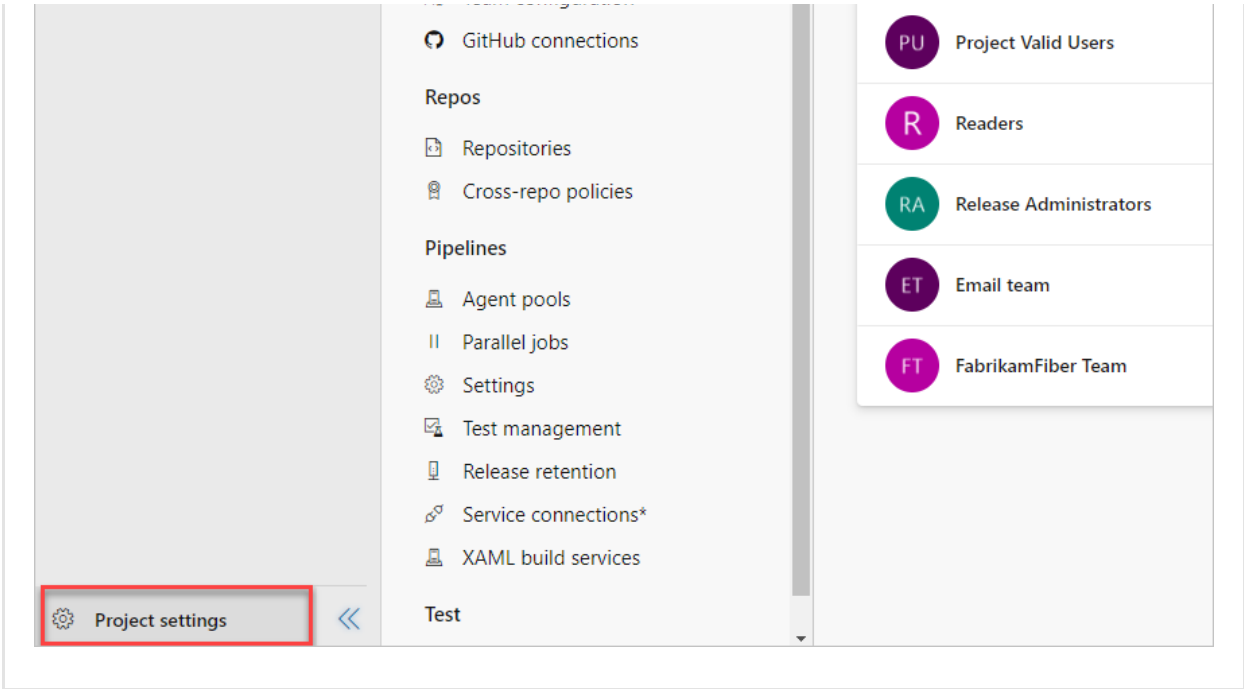
To enable the new user interface for the Project Permissions Settings Page, see

to enable the new user interface for the Project Permissions settings page, see [Enable preview features](#).

Preview page

Current page





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.	Assign to users who define and manage build pipelines.
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