Set permissions and access for work tracking

14/03/2019 • 8 minutos para ler • Colaboradores

Neste artigo

- Edit project-level or collection-level/instance-level information
- Create child nodes, modify work items under an area path
- Define and edit queries or query folders
- Edit or manage permissions for Delivery Plans
- Move or permanently delete work items
- Manage test artifacts
- Customize an inherited process
- Related articles

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.

> ⓘ **Observação**
>
> 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	• Manage teams and configure team tools • Define and edit team dashboards • Add and manage team-level work item templates • Add team administrators To add a user to the team administrator role, see Add a team administrator.
Object-level permissions	• 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	• 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	• 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 Project collection-level permissions include all permissions you can set at the project-level.

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.

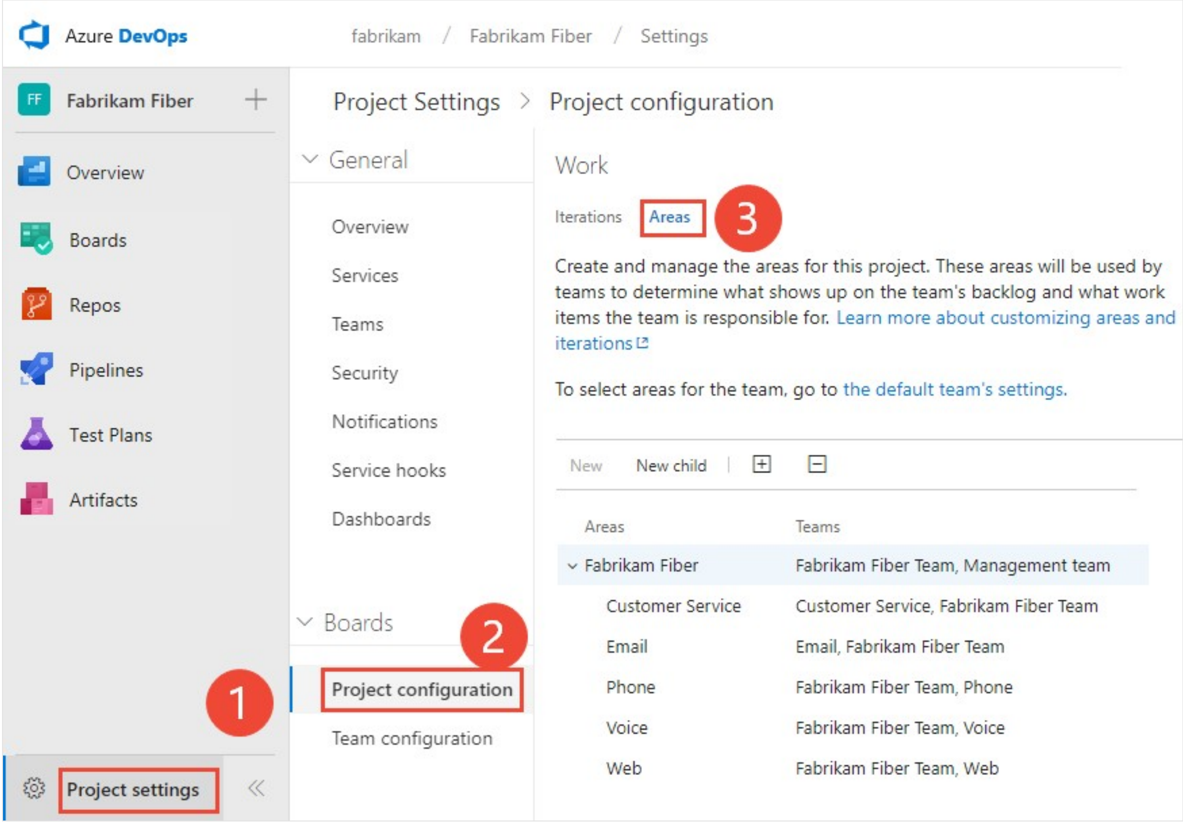
Edit project-level information	Edit instance-level information
• Add and administer teams and all team-related features • Create and modify areas and iterations • Edit shared work item queries • Edit project level permission ACLs • Manage process templates • Customize a project • Create and modify global lists • Edit event subscriptions (email or SOAP) on project level events.	• 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**.

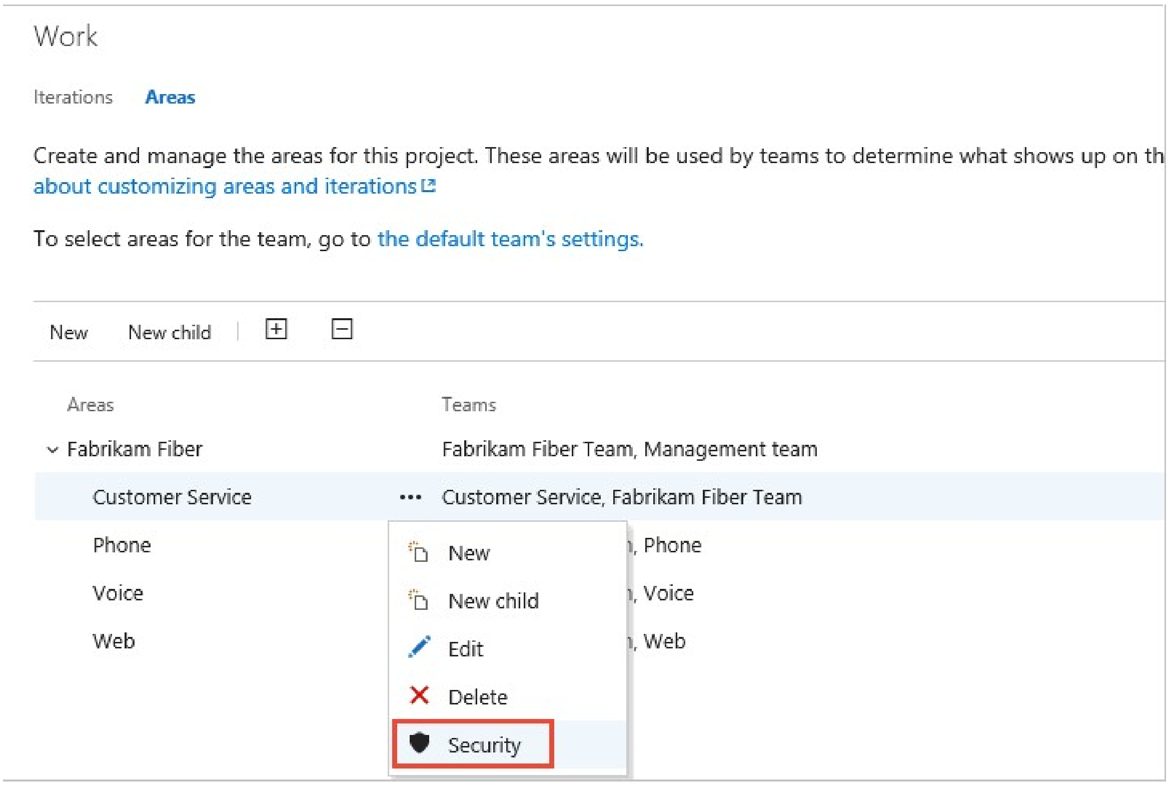


Create and manage the areas for this project. These areas will be used by teams to determine what shows up on the team's backlog and what work items the team is responsible for. Learn more about customizing areas and iterations

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

2. Choose the ... context menu for the node you want to manage and select **Security**.



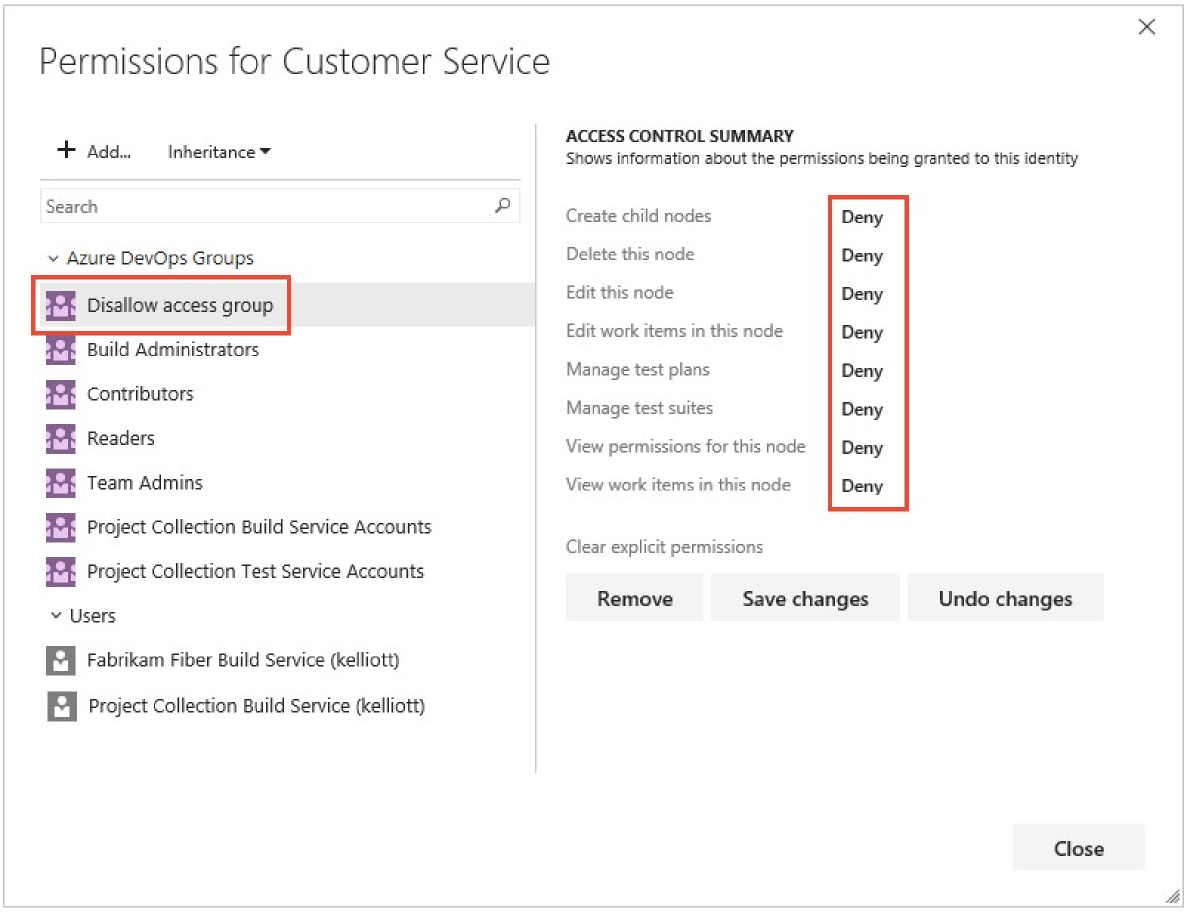
Create and manage the areas for this project. These areas will be used by teams to determine what shows up on th
about customizing areas and iterations

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
Phone	, Phone
Voice	, Voice
Web	, Web

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

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

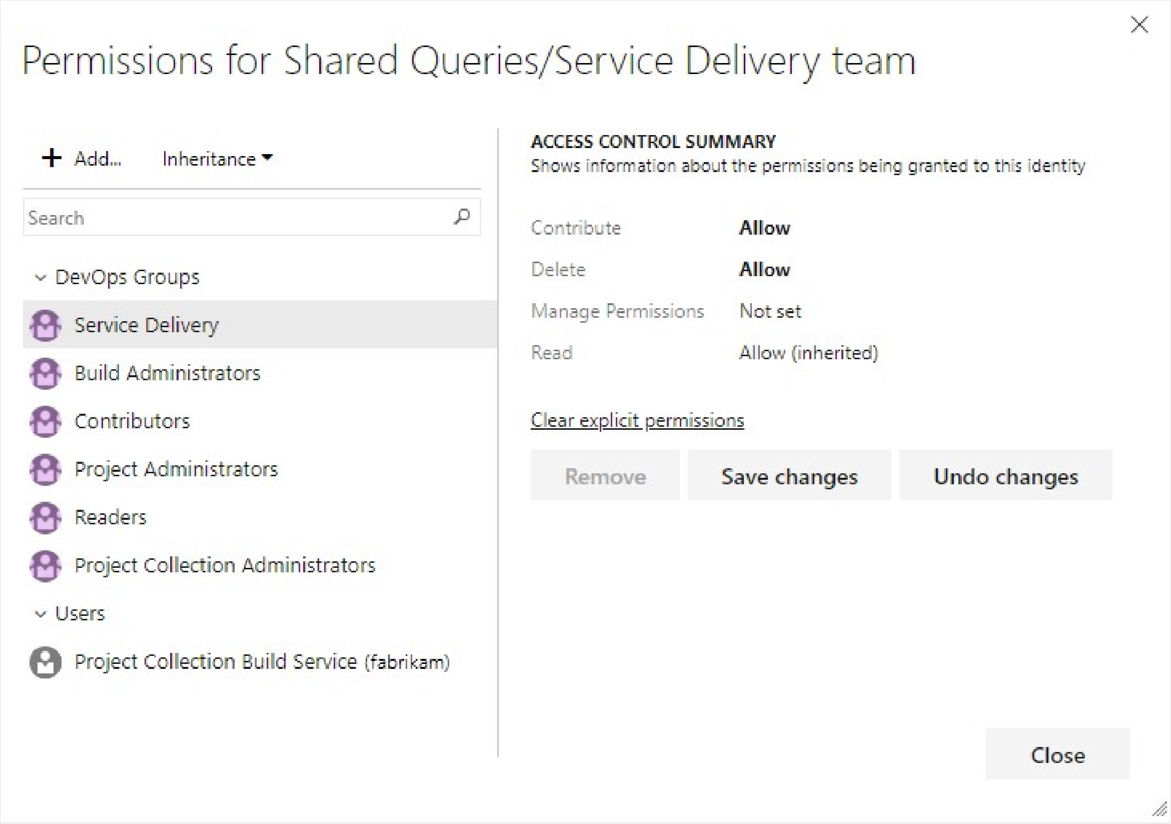
Create child nodes	Deny
Delete this node	Deny
Edit this node	Deny
Edit work items in this node	Deny
Manage test plans	Deny
Manage test suites	Deny
View permissions for this node	Deny
View work items in this node	Deny

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

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

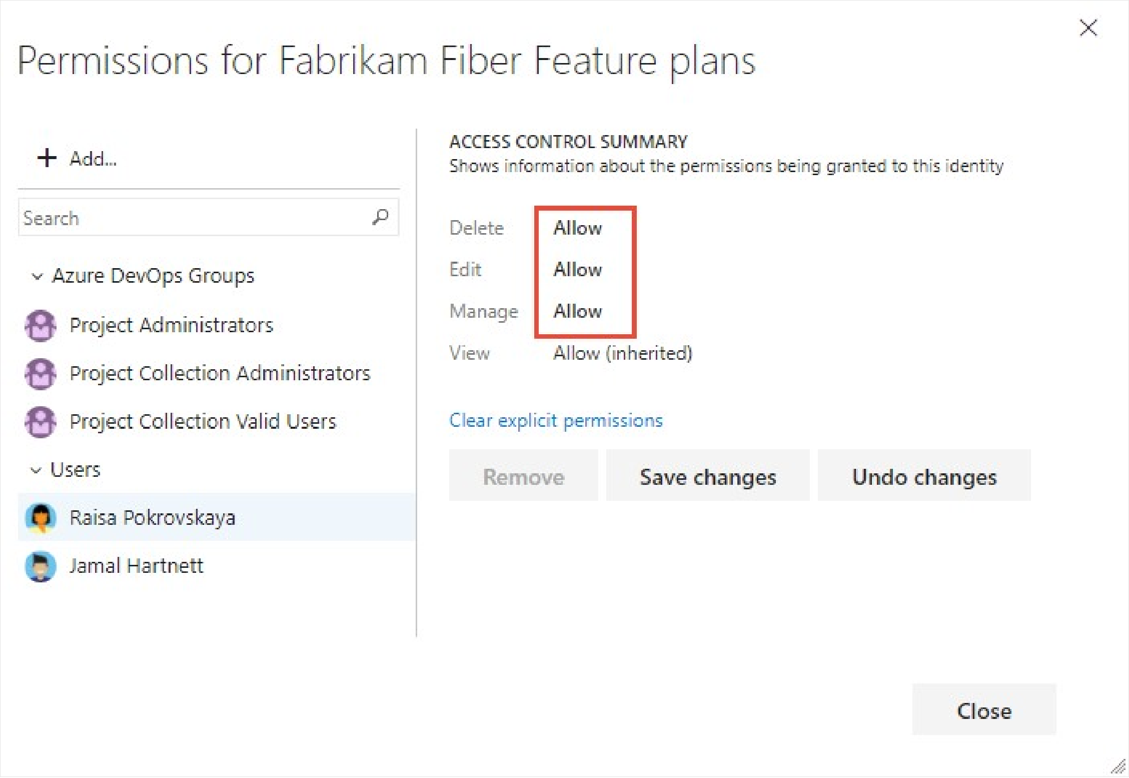
Contribute	**Allow**
Delete	**Allow**
Manage Permissions	Not set
Read	Allow (inherited)

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



Permissions for Fabrikam Fiber Feature plans

ACCESS CONTROL SUMMARY
Shows information about the permissions being granted to this identity

Delete	Allow
Edit	Allow
Manage	Allow
View	Allow (inherited)

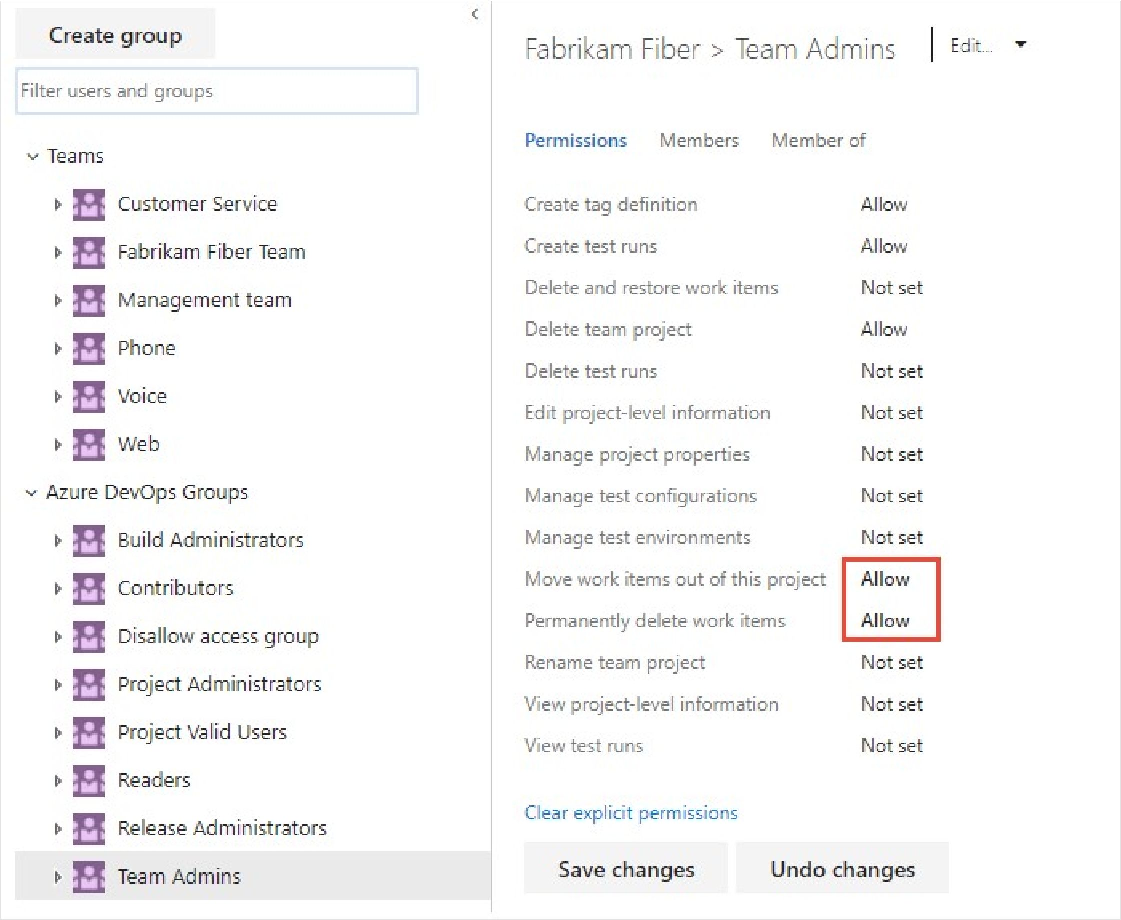
To learn more, see Edit or manage Delivery Plan permissions. To learn more about Delivery Plans, see Review team plans.

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.

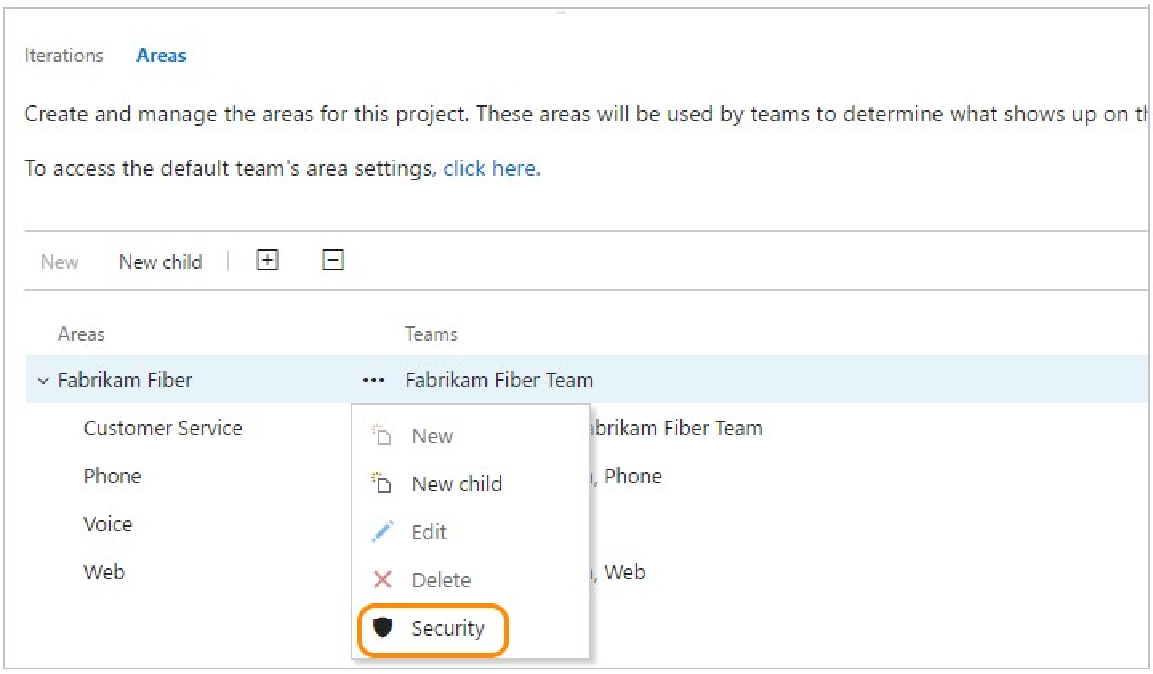


Create tag definition	Allow
Create test runs	Allow
Delete and restore work items	Not set
Delete team project	Allow
Delete test runs	Not set
Edit project-level information	Not set
Manage project properties	Not set
Manage test configurations	Not set
Manage test environments	Not set
Move work items out 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

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.

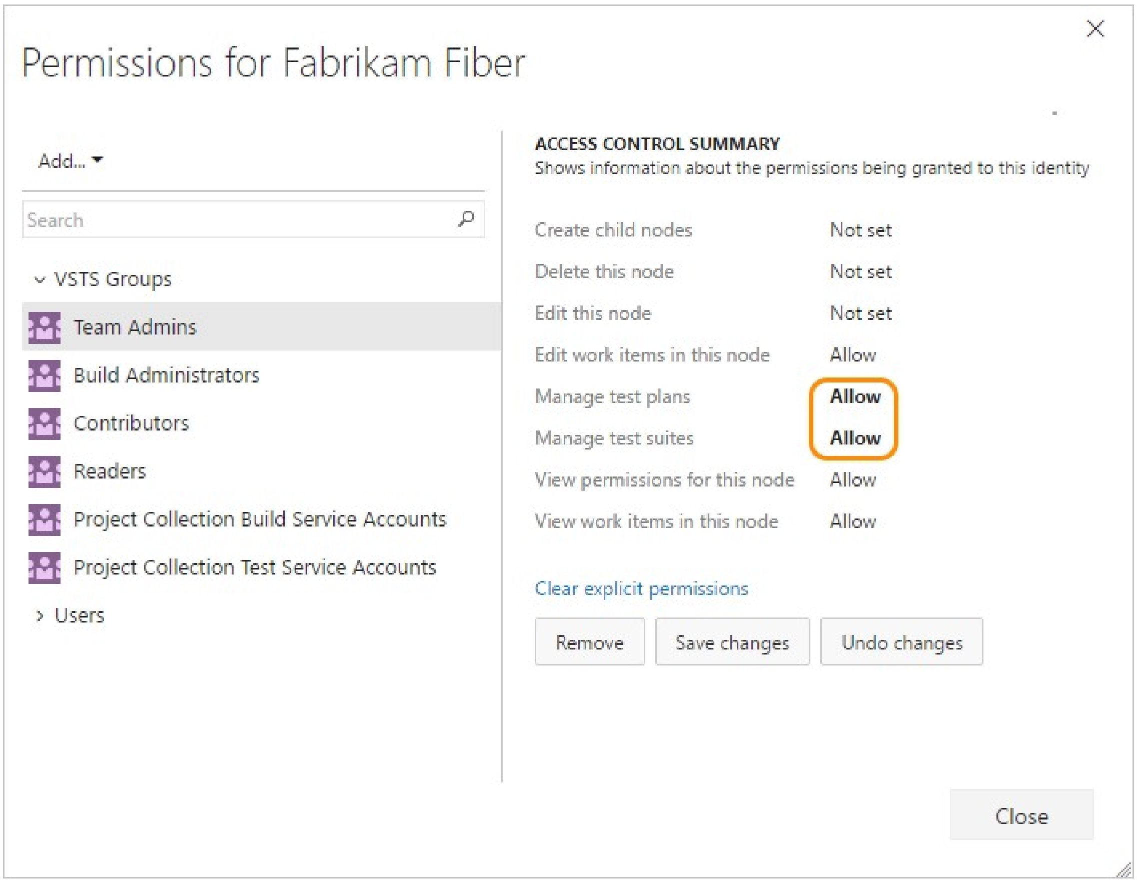


Create and manage the areas for this project. These areas will be used by teams to determine what shows up on tl

To access the default team's area settings, click here.

Areas	Teams
Fabrikam Fiber	Fabrikam Fiber Team
Customer Service	abrikam Fiber Team
Phone	, Phone
Voice	
Web	, Web

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

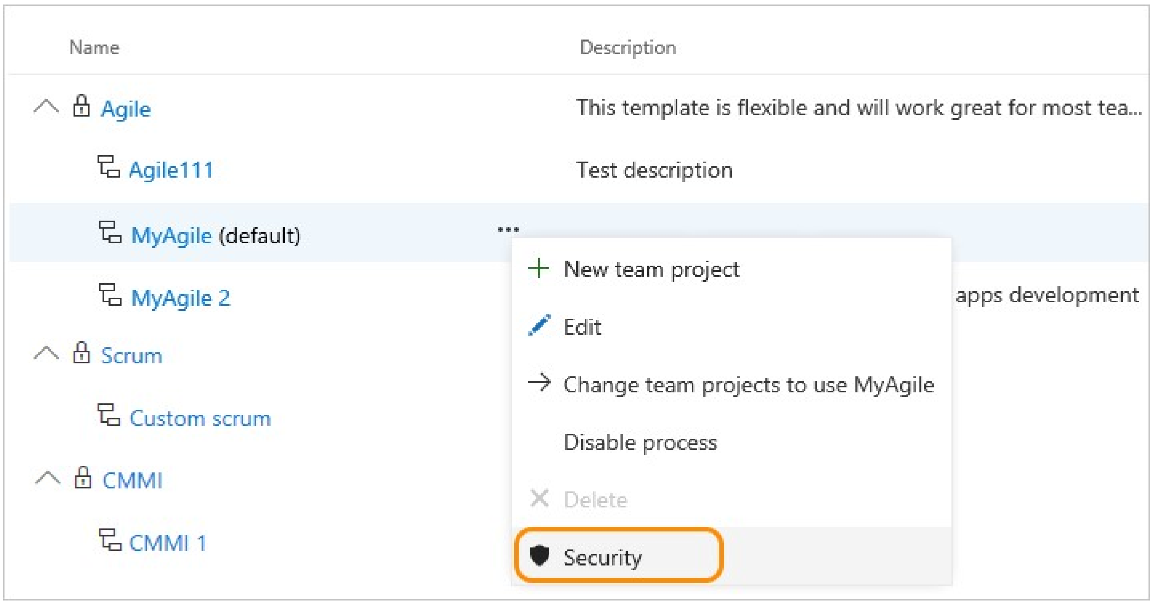
To have full access to the Test feature set, your access level must be set to Basic + Test Plans. Users with Basic access and with permissions to permanently delete work items and manage test artifacts can only delete orphaned test cases.

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.

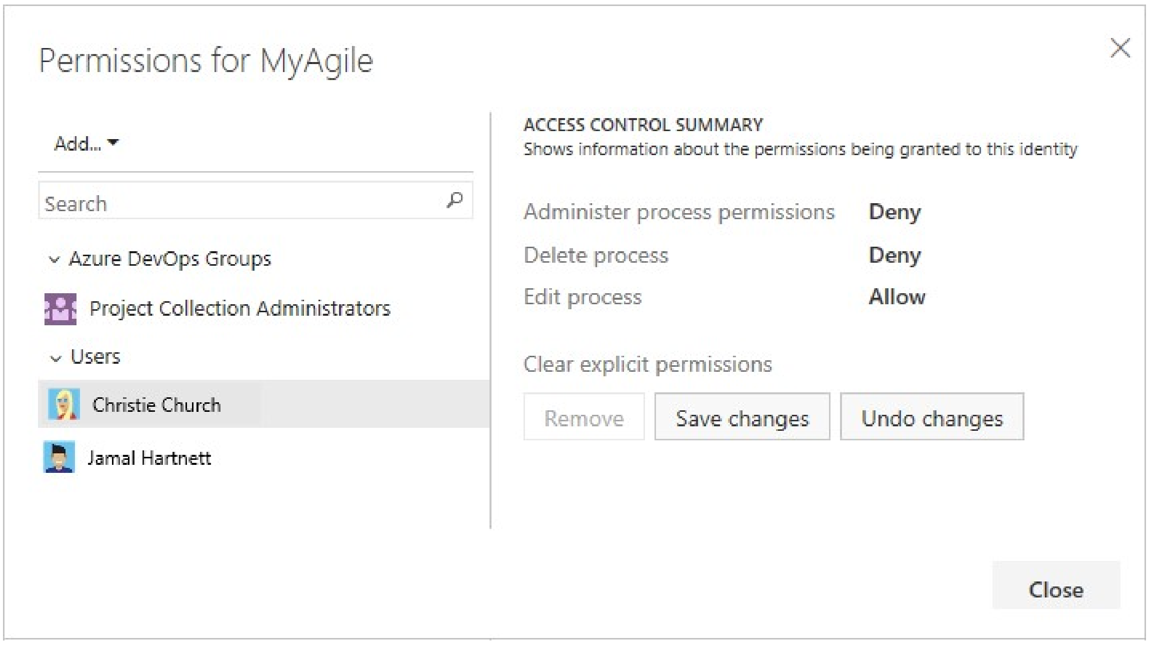
1. Open the ... context menu for the inherited process and choose **Security**. To open this page, see Customize a project using an inherited process.



Name	Description
Agile	This template is flexible and will work great for most tea...
Agile111	Test description
MyAgile (default)	
MyAgile 2	apps development
Scrum	
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.



Permissions for MyAgile

Azure DevOps Groups
- Project Collection Administrators

Users
- Christie Church
- Jamal Hartnett

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

ⓘ Observação

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.

Related articles

- Set permissions on queries and query folders
- Permissions and access for work tracking

- Permissions and groups reference