Manage your organization or collection

Article • 03/25/2024

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

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

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

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

Add users to your organization

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

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

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

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

> **Note**

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

Set up billing

Azure DevOps charges for the following services as described in Pricing for Azure DevOps .

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

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

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

Manage security and permissions

Permissions and security groups control access to specific tasks.

The following table lists the permissions assigned at the organization or collection-level. All of these permissions, except for the **Make requests on behalf of others** permission, are granted to members of the **Project Collection Administrators** group. For a description of each permission, see Permissions and groups reference, Groups.

General

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

Service Account

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

Boards

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

Repos (TFVC)

- Administer shelved changes
- Administer workspaces
- Create a workspace

Pipelines

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

Test Plans

- Manage test controllers

Auditing

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

Policies

- Manage enterprise policies

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

- Get started with permissions, access, and security groups
- Change permissions at the organization or collection-level.

Add members to the Project Collection Administrators group

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

It's always a good idea to have more than one person who has administrative privileges. To add a user to this group, see Change permissions at the organization level,Add members to the Project Collection Administrators group.

Limit user visibility for projects and more

By default, users added to an organization can view all organization and project information and settings.

> **ⓘ Important**
>
> - The limited visibility features described in this section apply only to interactions through the web portal. With the REST APIs or `azure devops` CLI commands, project members can access the restricted data.
> - Guest users who are members in the limited group with default access in Microsoft Entra ID, can't search for users with the people picker. When the preview feature's turned *off* for the *organization*, or when guest users aren't members of the limited group, guest users can search all Microsoft Entra users, as expected.

To restrict select users, such as Stakeholders, Microsoft Entra guest users, or members of a particular security group, you can turn on the **Limit user visibility and collaboration to specific projects** preview feature for the organization. Once turned on, any user or group added to the **Project-Scoped Users** group, are restricted in the following ways:

- Restricted users to only access those projects to which they're added.
- Restricts views that display list of users, list of projects, billing details, usage data, and more that is accessed through **Organization Settings**.
- Limits the set of people or groups that appear through people-picker search selections and the ability to **@mention** people.

> **⚠ Warning**
>
> When the **Limit user visibility and collaboration to specific projects** preview feature is enabled for the organization, project-scoped users are unable to search

for users who were added to the organization through Microsoft Entra group membership, rather than through an explicit user invitation. This is an unexpected behavior and a resolution is being worked on. To self-resolve this issue, disable the **Limit user visibility and collaboration to specific projects** preview feature for the organization.

For more information, see Manage preview features.

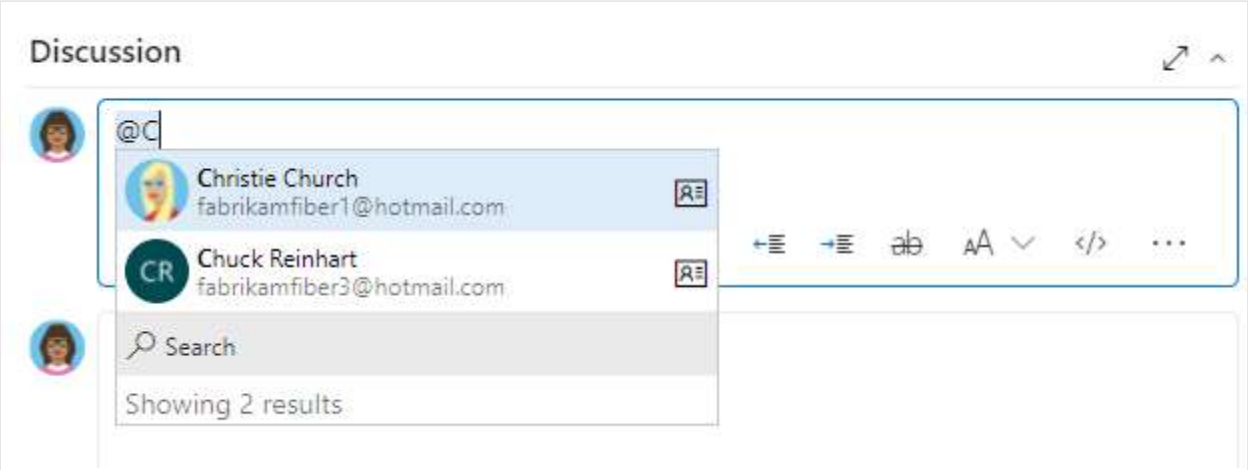
All security groups are organization-level entities, even those groups that only have permissions to a specific project. From the web portal, visibility of some security groups might be limited based on user permissions. However, you can discover the names of all groups in an organization using the **azure devops** CLI tool or our REST APIs. For more information, see Add and manage security groups.

Limit identity search and selection

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

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

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



Users and groups who are added to the **Project-Scoped Users** group can only see and select users and groups in the project they're connected to from a people picker. To

scope people pickers for all project members, see Limit user visibility for projects and more earlier in this article.

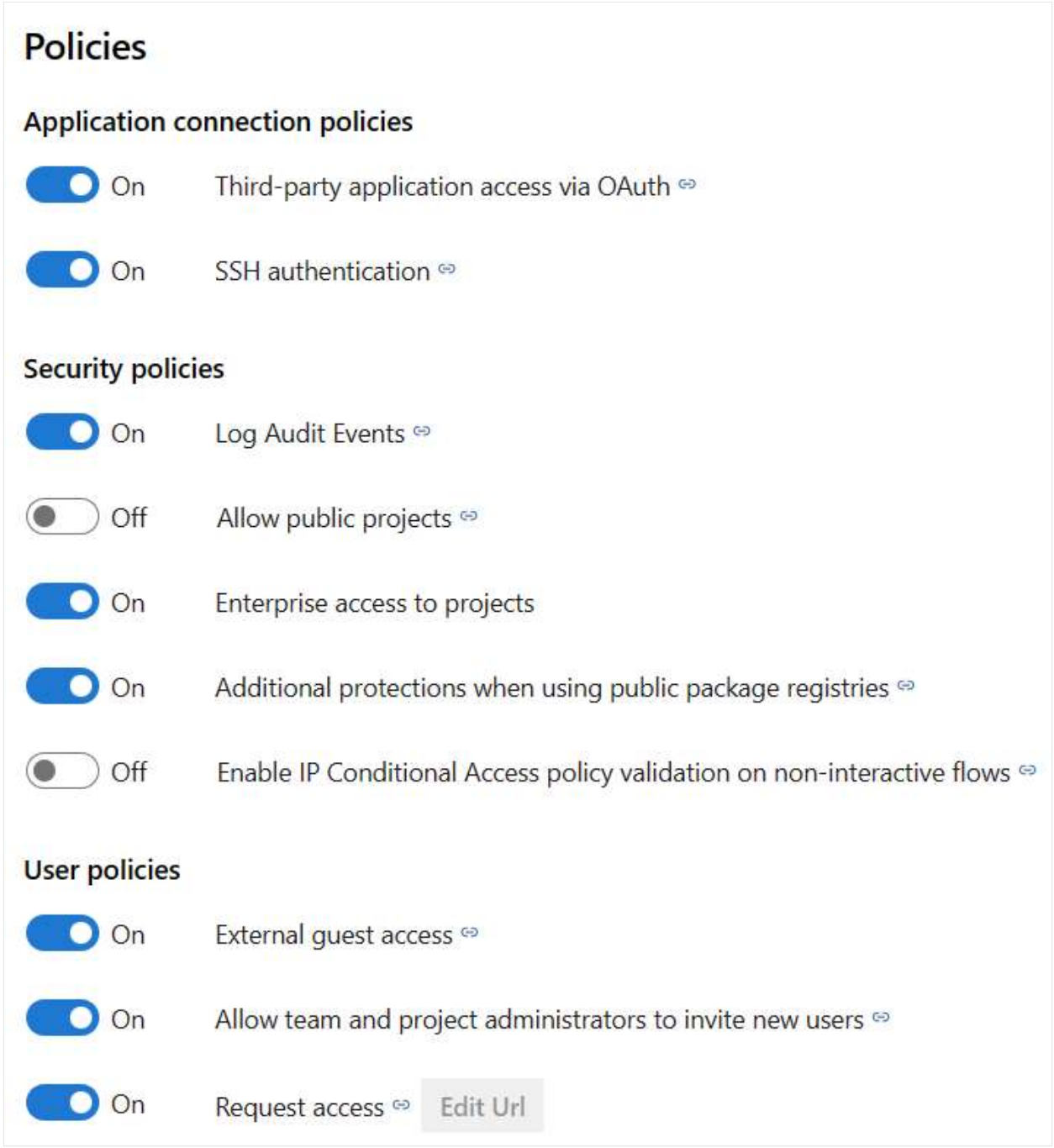
To limit the identity selection to only users and groups added to a project, perform the following procedure for your organization and projects.

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

Set security policies

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

- Third-party application access via OAuth
- SSH authentication
- Creation of public projects
- Invitation of GitHub user accounts



For more information, see Change application connection & security policies for your organization.

Manage extensions

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

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

For example, to support code search, install the Code Search extension .

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

Install Code Search

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

Adjust time zone and other organization settings

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

- Time zone settings and usage
- Add a privacy policy URL for your organization

Configure DevOps settings

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

- Add agent pools
- Define pipeline retention settings
- Define repository settings:
  - Default branch name for new repositories
  - Gravatar images.

Customize work-tracking processes

All work-tracking tools are available immediately after you create a project. Often, one or more users might want to customize the experience to meet one or more business

needs. Processes are easily customized through the user interface. However, you might want to establish a methodology for who manages the updates and evaluates requests.

For more information, see the following articles:

- About process customization and inherited processes
- Customize a project
- Add and manage processes

Alert users with information banners

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

Review and update notifications

Many notifications are predefined at the organization or collection level. You can manage subscriptions or add new subscriptions.

Scale your organization or collection

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

- About projects and scaling your organization
- Plan your organizational structure

Related articles

- About projects
- FAQs about signing up and getting started
- Organization management
- About user, team, project, and organization-level settings

Feedback

Was this page helpful? Yes No

Provide product feedback