

# Role and Permission

User access levels are handled by assigning different roles to users.

A role is a set of permissions that can be granted to a user in one or all projects thus controlling access to the projects and various features in the Web UI.

A permission is an authorization granted to a TeamCity user to perform particular operations, e.g. to run a build or modify build configuration settings.

On this page:

- [Authorization Mode](#)
- [Changing Authorization Mode](#)
- [Simple Authorization Mode](#)
- [Per-Project Authorization Mode](#)
- [Agent Management Permissions](#)

## Authorization Mode

TeamCity authorization supports two modes: simple and per-project.

In the simple mode, there are only three types of authorization levels: guest, logged-in user and administrator.

In the per-project mode, you can assign users Roles in projects or server-wide. The set of permissions in roles is editable.

Permissions within a role granted at the project level are automatically propagated in all the subprojects of this project.

The View project and all parent projects permission allows you to view not only the project (with its subprojects) but its parent projects too.

## Changing Authorization Mode

Unless explicitly configured, the simple authorization mode is used when TeamCity is working in the Professional mode and per-project is used when working in the Enterprise mode.

To change the authorization mode, use the Enable per-project permissions check box on the Administration | Authentication page.

## Simple Authorization Mode

|                |  |
|----------------|--|
| Administrator  | Users with no restrictions; corresponds to the System Administrator role in the per-project authorization mode   |
| Logged-in user | Corresponds to the default Project Developer role granted for all projects in the per-project authorization mode |
| Guest user     | Corresponds to the default Project Viewer role granted for all projects in the per-project authorization mode    |

## Per-Project Authorization Mode

Roles are assigned to users by administrators on a per-project basis - a user can have different roles in different projects, and hence, the permissions are project-based. A user can have a role in a specific project or in all available projects, or no roles at all. You can [associate a user account with a set of roles](#). A role can also be granted to a user group. This means that the role is automatically granted to all the users that are included into the group (both directly or through other groups).

By default, TeamCity provides the following roles:

| Role                 | Description   |
|----------------------|---|
| System Administrator | TeamCity System Administrators have no restrictions in their permissions, and have all of the project administrator's permissions. They can create and manage users' accounts, authorize build agents and set up projects and build configurations, edit the TeamCity server settings, manage TeamCity licenses, configure server data clean-up rules, change VCS roots, and etc. |
| Project Viewer       | Project Viewer has read-only access to projects and can only view the project, its parent and subprojects. Project Viewer does not have permissions to <a href="#">view agent details</a> .   |

|                       |  |
|-----------------------|--|
| Project Administrator | Project Administrator is a person who can customize general settings of a project and settings of build configurations, assign roles to the project users, create subprojects, and who has all the project developer's permissions. Prior to TeamCity 10, this role included in the Agent Manager role, since TeamCity 10 <a href="#">agent management permissions</a> (see below) replace the inherited Agent Manager role.                                     |
| Project Developer     | Project Developer is a person who usually commits changes to a project. He/she can start/stop builds, reorder builds in the build queue, label the build sources, review agent details, start investigation of a failed build.   |
| Agent Manager         | The Agent Manager role grants a user permissions for customizing and managing <a href="#">Build Agents</a> ; changing the run configuration policy, <a href="#">enabling/disabling</a> build agents, and <a href="#">pausing/resuming</a> build queue.<br><br>Prior to TeamCity 10.0, this role is included in the Project Administrator role. Since TeamCity 10, new agent management permissions have been introduced. See the <a href="#">section below</a> . |

When per-project permissions are enabled, server administrators can modify the roles, delete them, or add new roles with any combination of permissions right in the TeamCity Administration web UI, or by modifying the `roles-config.xml` file stored in `<TeamCity Data Directory>/config` directory. When assigning roles to users, the View role permissions link in the web UI displays the list of permissions for each role in accordance with their current configuration.

## Agent Management Permissions

TeamCity has 6 permissions to perform a task on an agent: a user must have a specific permission granted in a project. A user can perform a task controlled by one of these permissions on all the agents belonging to some [pool](#) provided this permission is granted to the user in all the projects associated with this pool. For example, a user with 'Enable / disable agents associated with project' permission in some projects can enable or disable agents which belong to the pools of the related projects if the permission is granted in all the projects associated with the pools.

In new installations, these project-related permissions are added to the Project Administrator role and the Agent manager role is no longer included in it.

In the existing installations after [upgrade](#), the new permissions are added to the Agent Manager role (which is included in the Project Administrator role). It is recommended to remove the inherited Agent Manager role manually and add the required permission(s) to the Project Administrator role.

The new permissions are:

- 1) Enable / disable agents associated with project
- 2) Start / Stop cloud agent for project
- 3) Change agent run configuration policy for project
- 4) Administer project agent machines (e.g. reboot, view agent logs, etc.)
- 5) Remove project agent
- 6) Authorize project agent

The last permission and the recently introduced "[maximum number of agents](#)" setting for an agent pool enable you to set up the system in a way which allows project administrators to run new agents and authorize/add them to their pools without involving the global system administrator.

See also:

Concepts: [User Account](#)  
Administrator's Guide: [Enabling Guest Login](#) | [Managing Users and User Groups](#)

