Types of permissions in Jira

Jira has several layers of access controls that admins can use to restrict access and capabilities.

Restrict access across Jira

At the highest level, Jira admins can control access to their site and non-space-specific capabilities using **global permissions**. These permissions apply across the entirety of your site, and include such actions as the ability to:

- create new spaces
- make changes to multiple work items at one time, and
- share dashboards and filters

These permissions can be granted to groups created by your Organization admin. More about managing groups

> If you're an Organization admin or a Site admin, you'll need to add yourself to the `jira-administrators` group. More about administration roles outside Jira

More about granting permissions across Jira

Restrict access at the space level with permission schemes

> Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites. More about Free plans

What users can do in a space is handled by a separate and more granular set of permissions, which are managed using **permission schemes**. These permissions determine whether users can:

- make changes to a space configuration
- create new work items
- add or remove comments on work items

More about permission schemes

These schemes, which can be shared by multiple spaces, grant space permissions to groups that your organization admin has created, individual users, or to users who hold a specific role within a space – also called **space roles**. By using space roles instead of explicitly-defined users, Jira admins can use the same schemes across multiple spaces without needing to constantly update them. In more practical terms, this empowers Space admins to grant permissions to team members in the space they work without requiring help from a Jira admin. More about space roles

> If you want to hide an entire space that contains sensitive information, you can create data classification levels which Space admins can be applied to an entire space in Jira Cloud or in Jira Service Management.

Restrict access at the work item-level

Lastly, Jira admins can add restrictions to individual work items using **workflows** and **work item security schemes**.

Workflows

Using workflows, admins can limit what users can do on specific work items to:

- limit users' access while work is in a specific status
- restrict changes to a work item based on its status
- block work from progressing to a new status until it meets acceptance criteria

By these powers combined, Jira admins can systemically align Jira with their organization's ways of working. More about space workflows

Work item security schemes

Jira admins can use work item security schemes to restrict the visibility of individual work items within an otherwise accessible space. Once configured, a work item security scheme hides work items from public view, save for users who have permission to view sensitive information. This is applied independently from space permissions. More about work item security schemes

> You can use Rovo to explain and troubleshoot Jira permissions. Open Rovo Chat and enter `/manage-jira-permissions`, then tell Rovo what problem you're trying to solve, or ask for a rundown on your current permissions setup.

Work with external collaborators using guest roles

If you need to give external collaborators limited access to Jira without a full license, you can invite them as guests. Guests are free, non-billable, and restricted to a single space per site — with a fixed set of permissions that can't be expanded through permission schemes or space roles. How to invite and manage guests in Jira

Define who can access your Jira site using Permissions

- Types of permissions in Jira

What are global permissions, and what do they control?

View, grant, revoke global permissions in Jira

Check a user's access from a work item

Troubleshoot permissions configurations

On this page

Restrict access across Jira

Restrict access at the space level with permission schemes

Restrict access at the work item-level

Workflows

Work item security schemes

Work with external collaborators using guest roles

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

What are global permissions, and what do they control?

At the highest level, Jira admins can control access to their site and cross-space permissions on the **Global permissions** page. These permissions apply across the entirety of your site, and can be granted to groups created by your Organization admin. More about managing groups

On this page, we'll go through the permissions that can be granted across your entire site. For permissions within a space, see our section about permissions in spaces.

Types of global permissions

Administer Jira

> ⚠ If you're an Organization admin or a Site admin, you'll need to add yourself to the `jira-administrators` group. More about administration roles outside Jira

> Throughout this documentation, we'll refer to any user with this permission as a **Jira admin**.

Users with this permission can:

- create new spaces (both company-managed and team-managed)
- create and edit
  - configurations for work types, fields, and workflows and
  - schemes for fields, permissions, and notifications
- log in to Jira at any time, regardless of any restrictions placed on access

Users with this permission cannot:

- manage existing users or add new ones
- import and export data
- edit system email settings

Browse users and groups

Users with this permission can view the names of all users in your site when using User picker type fields or @mentioning users in comments.

Users without this permission will only be able to see users who have the **Browse spaces** permission in the space they're viewing. This is a common way to limit information when sharing spaces widely.

Share dashboards and filters

Users with this permission can share dashboards and filters with other users, provided they have permission to view it.

More about sharing data from your site

Manage group filter subscriptions

Users with this permission can create and delete group filter subscriptions.

Manage custom onboarding

Users with this permission can create and edit content for custom onboarding, and access custom onboarding analytics.

Make bulk changes

Provided they have the necessary space permissions, users with this permission can:

- edit, move, or delete multiple work items at the same time
- transition multiple work items at one time through a workflow

Create team-managed spaces

With this permission, users can only create team-managed spaces (not company-managed spaces which is defined using the **Administer Jira** permission).

What are the differences between company-managed and team-managed spaces?

Team-managed spaces in Jira Service Management

Atlassian Home for Jira Cloud project connection issue glance

Users with this permission can connect Jira work items to Projects. It is added when the Connect addon is installed.

Define who can access your Jira site using Permissions

Types of permissions in Jira

- **What are global permissions, and what do they control?**

View, grant, revoke global permissions in Jira

Check a user's access from a work item

Troubleshoot permissions configurations

On this page

Types of global permissions

Administer Jira

Browse users and groups

Share dashboards and filters

Manage group filter subscriptions

Manage custom onboarding

Make bulk changes

Create team-managed spaces

Atlassian Home for Jira Cloud project connection issue glance

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

View, grant, revoke global permissions in Jira

The processes on this page require the **Administer Jira** permission.

At the highest level, Jira admins can control access to their site and non-space-specific capabilities using **global permissions**. These permissions apply across the entirety of your site, and can be granted to groups created by your Organization admin. More about managing groups

View global permissions

To see all your global permissions:

1. Select **Settings** ( ), then **System**.
2. Select **Global permissions** in the sidebar.

Here you can view all the users with a particular global permission, and grant or revoke access.

Grant global access

From the **Global permissions** page, use the **Grant Permission** section at the bottom of the page to grant access to a group or user. When you're ready, select **Add** to save your changes.

If you select **Anyone**, any users who access your site will be able to perform the related actions. More about publicly-accessible sites

Revoke global permissions

To revoke permissions for a group, find the permission in the list and select **Delete** under the group name.

You can use Rovo to explain and troubleshoot Jira permissions. Open Rovo Chat and enter `/manage-jira-permissions`, then tell Rovo what problem you're trying to solve, or ask for a rundown on your current permissions setup.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Define who can access your Jira site using Permissions

Types of permissions in Jira

What are global permissions, and what do they control?

- **View, grant, revoke global permissions in Jira**

Check a user's access from a work item

Troubleshoot permissions configurations

On this page

View global permissions

Grant global access

Revoke global permissions

Community

Questions, discussions, and articles

©2026 Atlassian

Check a user's access from a work item

Whether you want to test a newly created permissions setup or find out why a user can't perform an action, the **Permission helper** can validate your permissions configuration.

To see what permissions a user has on a work item:

1. Select **Settings** ( ), then **System**.
2. Under the **Admin helper** section, select **Permission helper**.
3. Select the **User**, **Work item**, and **Permission** for which you'd like to see more details.
   a. Leave the **User** field blank to view what anonymous users can do.
4. Select **Submit**.

The Permission helper lists all the permissions that user has for the work item you selected. If you select **Show failed conditions**, you'll see why this user can't perform the selected actions.

How to solve common permissions configuration problems

Was this helpful? Yes No Provide feedback about this article

Define who can access your Jira site using Permissions

Types of permissions in Jira

What are global permissions, and what do they control?

View, grant, revoke global permissions in Jira

- **Check a user's access from a work item**

Troubleshoot permissions configurations

Community

Questions, discussions, and articles

Still need help?

The Atlassian Community is here for you.

Ask the Community

Troubleshoot permissions configurations

The processes on this page require the **Administer Jira** permission.

This page outlines some common reasons and ways to troubleshoot your setup, including:

- A user has permission in the scheme, but can't perform an action
- I can't grant a space permission to a user
- My Jira integrations can't perform key actions
- My (or a user's) User Picker fields are empty

If you haven't already tried it, the **Permission helper** can help identify problems with your setups based on a specific work item. More about the Permission helper

A user has permission in the scheme, but can't perform an action

To resolve, ensure that the user has the most specific permission available related to the action.

As a general rule, permissions that grant specific capabilities take precedence over generic ones. For example, if a space doesn't have the **Assign work items** permission configured, any user with the **Edit work items** permission can update the **Assignee** field. But once you restrict the **Assign work items** permission, only users with that permission can change the **Assignee** field. Users without it can still edit other fields, just not the **Assignee** field.

This behavior ensures that only users who are explicitly granted a permission can perform certain actions. More about how permissions interact

I can't grant a space permission to a user

Some space permissions can only be granted to users who have been invited by a Site admin, and occupy a paid seat in your Jira site.

Our page on the permissions available in a space mentions which ones can only be granted to paid users.

My Jira integrations can't perform key actions

To allow users to perform actions in Jira from apps or integrations (like Slack), add the `atlassian-addons-project-access` space role to the relevant permission scheme.

More about space roles in schemes

More about integrating apps into Jira

My (or a user's) User Picker fields are empty

To resolve, make sure that the user in question has the **Browse users and groups** permission.

This permission allows users to view everyone in your site when using User picker type fields or @mentioning users in comments.

Users without this permission will only be able to see users who have the **Browse spaces** permission in the space they're viewing. This is a common way to limit information when sharing spaces widely.

More about sharing spaces publicly

To see which permissions also require the **Browse users and groups** permission, see the **space permissions page**.

Define who can access your Jira site using Permissions

Types of permissions in Jira

What are global permissions, and what do they control?

View, grant, revoke global permissions in Jira

Check a user's access from a work item

- **Troubleshoot permissions configurations**

On this page

A user has permission in the scheme, but can't perform an action

I can't grant a space permission to a user

My Jira integrations can't perform key actions

My (or a user's) User Picker fields are empty

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

What are permission schemes in Jira?

Permission schemes allow you to define what users can do within a space, as opposed to global permissions which define what users can do across your entire site.

These schemes can be shared with other spaces, but any changes will be applied to all that use it. How to create a new permission scheme

Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites. More about Free plans

Use space roles to grant permissions

Along with users and groups, Jira admins can also grant capabilities to roles within a space that can later be defined by Space admins. Jira calls these **space roles**, and they give permission schemes the flexibility to be used in multiple spaces without granting unwanted access. It also allows Space admins to update permissions in their spaces without requiring help from a Jira admin.

More about space roles

You can use Rovo to explain and troubleshoot Jira permissions. Open Rovo Chat and enter `/manage-jira-permissions`, then tell Rovo what problem you're trying to solve, or ask for a rundown on your current permissions setup.

Was this helpful? Yes No Provide feedback about this article

Grant space permissions using permission schemes

- What are permission schemes in Jira?

Create a new permission scheme

Grant or revoke permissions in a scheme

Change which permission scheme a space uses

How permissions interact with each other

Show more

Community

Questions, discussions, and articles

Still need help?

The Atlassian Community is here for you.

Ask the Community

Create a new permission scheme

Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites.
More about Free plans

Permission schemes determine who can do what in a space. Like other schemes in Jira, these can be used by multiple spaces, allowing admins to quickly update permissions at scale.

The processes on this page require the **Administer Jira** permission.

To create a permission scheme:

1. Select **Settings** ( ), then **Work items**.
2. Under **Work item attributes**, select **Permission Schemes**. You may need to scroll down since it's at the bottom of the list.
3. To create a new permission scheme, select **Add Permission Scheme**.
4. Give your new scheme a name and a short description, then select **Add**.

Once you've created a permission scheme, you can use it to grant access to users, and then associate it to a space.

Grant space permissions using permission schemes

What are permission schemes in Jira?

- **Create a new permission scheme**

Grant or revoke permissions in a scheme

Change which permission scheme a space uses

How permissions interact with each other

Show more

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant or revoke permissions in a scheme

Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites. More about Free plans

Once you've created a permission scheme, use it to define what actions users can perform in your spaces. What permissions I grant in a space?

The processes on this page require the **Administer Jira** permission.

To grant permissions using a scheme:

1. Select **Settings** ( ), then **Work items**.
2. Under the **Work item attributes** section, select **Permission Schemes**. You may need to scroll down since it's at the bottom of the list.
3. Select either the name of the scheme you want to update or **Permissions** in the actions column. This opens the detailed view of the permissions in this scheme.
4. Find the permission you want to edit and select **Update**.
5. Next, select who you'd like to grant this permission to. Permissions in a scheme can be given to:
   a. **Space roles** - this refers to any custom space roles that you've set up – More about managing space roles
   b. **Application access** - any user with access to an app
   c. **Group** - these groups are managed by your Organization admin. Reach out to them to update group membership or to remove users from a group
   d. **Public** - More about publicly available spaces
   e. **Any logged in user**
   f. **Current assignee** - this grants access to anyone listed in a work item's **Assignee** field
   g. **Reporter** - this grants access to anyone listed in a work item's **Reporter** field
   h. **Group custom field value** - this grants access to anyone listed in a **Group picker** (single or multi-select) type field on a work item. You'll be asked which field you want to reference.
   i. **Space lead** - this grants access to anyone listed as the **Space owner** on a space's **Details** page. This is not the same as the **Administer spaces** permission.
   j. **Single user** - any user invited by your admin
   k. **User custom field value** - this grants access to anyone listed in a **User picker** (single or multi-select) type field on a work item. You'll be asked which field you want to reference.
6. When you're done, select **Update.**

Grant space permissions using permission schemes
What are permission schemes in Jira?
Create a new permission scheme
• Grant or revoke permissions in a scheme
Change which permission scheme a space uses
How permissions interact with each other
Show more

Community
Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Change which permission scheme a space uses

Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites.
More about Free plans

Once you've created and set up your new permission scheme, you'll need to associate it to company-managed spaces to enforce those restrictions.

If you're managing permissions in a team-managed space, see permissions in team-managed spaces.

The processes on this page require the **Administer Jira** permission.

To associate a permission scheme to a company-managed space:

1. Next to the name of your space in the sidebar, select **More actions** (•••), then **Space settings**.
2. Select **Permissions** from the sidebar.
3. Select **Actions,** then **Use a different scheme**.
4. Use the **Scheme** dropdown menu to select the permission scheme you want use in this space.
5. Select **Associate** to save your change. Any changes to space access or capability are applied immediately.

Grant space permissions using permission schemes

Show more

Create a new permission scheme

Grant or revoke permissions in a scheme

- **Change which permission scheme a space uses**

How permissions interact with each other

Permissions limitations in Free Jira sites

Show more

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

How permissions interact with each other

On this page, we'll cover the most common ways that permissions can interact with each other, including:

- Spaces that share workflows and work item layouts
- Permissions for actions that involve multiple spaces
- Tasks that require multiple permissions
- How Jira handles overlapping restrictions

Spaces that share workflows and work item layouts

Those who hold the **Edit workflows** and **Manage work item layouts** permission in a scheme can only make changes if their space is the only one using those configurations. If the space shares its workflows or work item layouts with another space, users need the **Administer Jira** permission to update them.

Actions that require permissions in multiple spaces

In order to make changes that span multiple spaces, such as managing cross-space boards or moving work from one space to another, users need to have permissions in all impacted spaces.

For example:

- To update sprints that contain work from multiple spaces, users need to have the **Manage sprints** in all spaces where the work items live
- To link work items in different spaces, users need the **Link work items** permission in both spaces.

Tasks that require multiple permissions

Jira's permissions are very granular, meaning that some common actions require multiple permissions to complete, such as:

- Almost all work item permissions require the **Browse spaces** permission.
- The **Manage sprints** permission only allows a user to update a sprint – not the work within it. To make changes to work items, users need work item-specific permissions such as **Edit work items** and **Schedule work items**.
- The **Move work items** permission allows a user to move work items between spaces, but they also need the **Create work items** permission in the space to which they're moving the work.

How Jira handles overlapping restrictions

As as general rule, only users who have been explicitly granted permission can perform an action in Jira. Jira also has permissions with varying levels of specificity which often overlap. When two permissions overlap, the most specific applicable permission determines who can perform an action.

For example, the **Edit work items** permission allows a user to update all fields on a work item. However, the **Assign work items** permission grants users the ability to update the **Assignee** field, specifically. If your scheme only defines the **Edit work items** permission, anyone who has it can edit any field on a work item, including the **Assignee** field. But once you configure the **Assign work items** permission in your scheme:

- only users granted the **Assign work items** permission can update the **Assignee** field.
- users who only have the **Edit work items** permission can still change other fields – just not the **Assignee** field.
- users with the **Assign work items** permission but not the **Edit work items** permission can only change the **Assignee** field, and no others.

Workflow conditions like the jira.issue.editable condition or the jira.permission* condition can further limit when a field can be edited based on its status. They're applied using the same logic that favors specific restrictions over generic ones.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant space permissions using permission schemes

Show more

Grant or revoke permissions in a scheme

Change which permission scheme a space uses

- How permissions interact with each other

Permissions limitations in Free Jira sites

Use permissions to make a space publicly visible

Show more

On this page

Spaces that share workflows and work item layouts

Actions that require permissions in multiple spaces

Tasks that require multiple permissions

How Jira handles overlapping restrictions

Community

Questions, discussions, and articles

 ©2026 Atlassian

Permissions limitations in Free Jira sites

Those using free Jira sites can't:

- assign space roles in Jira Cloud (or in Jira Service Management)
- configure work item security schemes
- restrict permissions using schemes

Upgrade to unlock all of these features

If you downgrade from a paid version of Jira or migrating from Jira Data Center to a Free Jira Cloud site, your existing permissions schemes, space roles, and work item security schemes will be preserved but can't be edited. The only way to make changes to them is to upgrade to Standard, Premium, or Enterprise versions of Jira.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant space permissions using permission schemes

Show more

Change which permission scheme a space uses

How permissions interact with each other

- **Permissions limitations in Free Jira sites**

Use permissions to make a space publicly visible

How to use space roles

Show more

Community

Questions, discussions, and articles

Use permissions to make a space publicly visible

Standard, Premium, and Enterprise Jira sites can share spaces publicly. This page details how to control what data in a space is available to the public.

Spaces from Free Jira sites can't be opened to the public.

Allow anyone to view a space

The Browse spaces permission can reveal the details of spaces in the directory and in search

If you grant this permission to **User custom field value**, **Group custom field value, Reporter**, or **Current assignee** in your permission scheme, any user who is logged into your site can see the name of the space on the **View All Spaces** page and when searching for work items. They cannot view the work items inside the space.

This is a known bug. See JAC for more

Set the **Browse spaces** permission to **Public** in the permission scheme to allow anyone to view a space and the work within it. This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

More about the **Browse spaces** permission

Limit the names visible in spaces

Users who have been granted the **Browse users and groups** permission can see all of the users in your site when using User picker type fields or @mentioning users in comments. Users without this permission will only be able to see users who have the **Browse spaces** permission in the space they're viewing. This is a common way to limit information when sharing spaces widely.

Allow anyone to create work items in a space

Set the **Create work items** permission to **Public** in the permission scheme to allow anyone with access to your site to create a new work item. Work items created by users who aren't logged in show "Anonymous" in the **Reporter** field.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.Make sure you also grant public users other relevant permissions, such as the **Create attachments** permission or permission to edit required fields. More about overlapping permissions

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant space permissions using permission schemes

Show more

How permissions interact with each other

Permissions limitations in Free Jira sites

- **Use permissions to make a space publicly visible**

How to use space roles

Create a new space role

Show more

On this page

Allow anyone to view a space

Limit the names visible in spaces

Allow anyone to create work items in a space

Community

Questions, discussions, and articles

©2026 Atlassian

How to use space roles

Instead of explicitly-defining users, Jira admins can assign qualities in a scheme to roles within a space. These roles can later be defined by the Space admin at their discretion, allowing Jira admins to use the same scheme for multiple spaces without sacrificing granularity or constantly updating schemes. In more practical terms, this empowers those working in a space to delegate responsibilities and permissions without requiring the intervention of Jira admins.

In Jira, these placeholders are called **Space roles**, and they can be used to:

- grant permissions in permissions schemes
- set up email notification schemes
- set up work item security levels
- trigger workflow conditions
- grant access to filters and dashboards

> Space permission schemes, space roles, and work item security schemes aren't available on Free Jira sites.
> More about Free plans

Jira admins can create space roles to match how their organization works, or grant permissions to users selected in a field, such as:

- the **Assignee** field (also called **Current assignee**)
- the **Reporter** field
- any **Group by** field
- any **User select** field

Any users who appear in that field (or are in the groups that appear in that field) are granted this permission. More about the roles that come with Jira Cloud and the roles that come with Jira Service Management.

> **Grant permissions to apps and integrations**
>
> To allow users to perform actions in Jira from apps or integrations (like Slack), add the `atlassian-addons-project-access` space role to the relevant permission scheme. More about integrating apps into Jira

How space roles simplify permissions management

For example, let's say that you – the Jira admin – want to restrict the ability to create new sprints to a specific user in a space that shares a permission scheme with other spaces. If you explicitly assign a user to this permission in your scheme:

- users with the **Manage sprints** permission would be able to do so in all spaces that use the scheme or
- you would need to use a different scheme for each space to limit access

In both situations, changing who can manage sprints requires a Jira admin.

Space roles allow for more flexibility within these shared structures. Instead of nominating specific users, you can create a space role called **Lead Developer**, then grant it the **Manage sprints** permission in your scheme.

In each space that uses this scheme, the Space admin can nominate whoever they want to the **Lead Developer** role, granting them the **Manage sprints** permission – but only in that space. In this way, your permission scheme grants access to users in different spaces without a Jira admin intervening.

Grant space permissions using permission schemes

Show more

Permissions limitations in Free Jira sites

Use permissions to make a space publicly visible

- How to use space roles

Create a new space role

View space role usage

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Create a new space role

When using permission schemes, Jira admins can grant permissions to a role in a space as a placeholder that can later be defined by the Space admin. Jira refers to these as **Space roles**. More about space roles

To create a new space role:

1. Select **Settings** ( ), then **System**.
2. Under the **Security** section, select **Space roles**.
3. Under **Add Space roles**, enter a role name and description.
4. Select **Add Space roles** to save it.

Once created, include it in your permission scheme. When a user is assigned to that space role in a Jira Cloud space or in a Jira Service Management space, they'll inherit this permission.

Automatically add a user to a role in new spaces

As a Jira admin, you can automatically add user to a space role in new spaces.

> This process only adds users to a role in *new spaces* – not existing ones.

To add users or groups to a space role in all new spaces:

1. Select **Settings** ( ), then **System**.
2. Under the **Security** section, select **Space roles**.
3. Select **Manage Default Members** in the **Actions** column of a space role you want to edit.
4. The next page shows any existing default users and groups in this role. Select **Edit**.
5. Add or remove users or groups:
   a. To add a user, start typing in the box beneath **Add user(s) to Space role**, then select a user. Select **Add** to save your change.
   b. To add a group, either type the name into the box (which won't return any group names) or select the icon next to the text box to show a list of available groups. Select **Add** to save your change.
   c. To remove a user or group, select them from the list, then select **Remove**.
6. Once you're done, select **Return to viewing space role** to return to the previous screen.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant space permissions using permission schemes

Show more

Permissions limitations in Free Jira sites

Use permissions to make a space publicly visible

How to use space roles

- **Create a new space role**

View space role usage

Community

Questions, discussions, and articles

View space role usage

When using permission schemes, Jira admins can grant permissions to a role in a space as a placeholder that can later be defined by the Space admin. Jira refers to these as **Space roles**. More about space roles

To view space role usage in your site:

1. Select **Settings** ( ), then **System**.
2. Under the **Security** section, select **Space roles**.
3. Select **View Usage.**

From here, you can see the permission schemes, email notification schemes, work item security levels, and workflow conditions that use this space role.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant space permissions using permission schemes

Show more

Permissions limitations in Free Jira sites

Use permissions to make a space publicly visible

How to use space roles

Create a new space role

- View space role usage

Community

Questions, discussions, and articles

Space access and configuration permissions

Use permission schemes to grant the permissions listed on this page.

Administer spaces

On Free Jira sites, all users have this permission. More about Free plans

Jira admins automatically inherit the **Administer spaces** permission.

Only users with this permission can:

- assign users to a space role
- edit components
- edit versions
- edit some space details including:
  - space name
  - URL
  - space lead
  - description

It can only be granted to users who have been invited by an admin.

Browse spaces

This permission is a prerequisite for almost all permissions in a space.

The **Browse spaces** permission allows users to view a space, see its work items, and search for them (unless work items have been hidden by work-level security settings).

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.This is a common way to make a space public.

The Browse spaces permission can reveal the details of spaces in the directory and in search

If you grant this permission to **User custom field value**, **Group custom field value, Reporter**, or **Current assignee** in your permission scheme, any user who is logged into your site can see the name of the space on the **View All Spaces** page and when searching for work items. They cannot view the work items inside the space.

This is a known bug. See JAC for more

Manage work item layouts

Users also need the **Browse spaces** permission to perform these actions. More about how permissions interact

This permission can't be granted in Jira Service Management spaces. Read more

The **Manage work item layouts** permission allows a user to change which fields appear on work in their space using the **Layout** settings page. They can add existing fields, but this permission doesn't allow them to create new ones.

This permission can only allows a user to change a workflow if the screens used in the **Layout** panel are not shared with any other spaces. More about how permissions interact

It can only be granted to users who have been invited by an admin.

Edit workflows

Users also need the **Browse spaces** permission to perform these actions. More about how permissions interact

This permission can't be granted in Jira Service Management spaces. Read more

The **Edit workflows** permission allows a user to update statuses and transitions in a workflow using the **Workflow** settings page. Users with this permission must use the new workflow editor.

It can only be granted to users who have been invited by an admin.

This permission can only allows a user to change a workflow if it's not used by any other spaces. More about how permissions interact

Manage versions (releases)

The **Manage versions (releases)** permission allows users to create, release, archive, merge, edit and delete versions using the **Releases** feature. More about releases

Manage sprints

The **Manage sprints** permission allows users to create, start, and complete sprints as well as adjust the sprint duration and goal.

- This permission does not allow users to update the work contained in a sprint. For that, users need the **Schedule work items** and **Edit work items** permissions. More about how permissions interact
- If a sprint contains work from multiple boards, users need the **Manage sprints** permission in all spaces to update the sprint. Space roles can simplify handling this permission in complex setups. More about space roles
- If your boards use complex JQL queries that unite work from multiple spaces, you may need to grant users the **Manage sprints** in all spaces in your site. An easier way to resolve problems from complex queries is to simplify your boards' JQL queries.

View aggregated data

The **View aggregated data** permission allows users to see insights about their board, backlog, and deployments. This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Even if users don't have access to a space, this permission can expose information such as:

- the average estimations or work item count of a space
- the work types used in a space
- the names of epics in a space, even if child work items are restricted by work-level security settings
- a team's deployment frequency, even if work is restricted by work-level security settings

View development tools

The **View development tools** permission allows a user to view the Development panel. It can only be granted to users who have been invited by an admin.

View (read-only) workflow

The **View (read-only) workflow** permission allows users to view a workflow using the **View workflow** link. This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Types of permissions you can grant in a space scheme

- Space access and configuration permissions
- Work item permissions in a space
- Time tracking permissions
- Voters, watchers, comment, and attachment permissions

On this page

Administer spaces
Browse spaces
Manage work item layouts
Edit workflows
Manage versions (releases)
Manage sprints
View aggregated data
View development tools
View (read-only) workflow

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Work item permissions in a space

Use permission schemes to grant the permissions listed on this page.

> Users also need the **Browse spaces** permission to perform these actions. More about how permissions interact

Archive work items

The **Archive work items** permission allows users to archive work items. This is commonly granted instead of the **Delete work items** permission, as archived work items can be recovered.

It can only be granted to users who have been invited by an admin.

Assign work items

The **Assign work items** permission allows users to update the **Assignee** field on work items. This doesn't allow work items to be assigned to a user. For that, see **Assignable user**.

> This permission overlaps with the **Edit work items** permission. More about how permissions interact

It can only be granted to users who have been invited by an admin.

Assignable user

The **Assignable user** permission allows users to be assigned work items via the **Assignee** field. This doesn't allow a user to update the **Assignee** field. For that, see **Assign work items**.

It can only be granted to users who have been invited by an admin.

Close work items

The **Close work items** permission allows users to set the **Resolution** field to a closed state on a work item. It can only be granted to users who have been invited by an admin.

> To close out work items, users may also need the **Transition work items** and **Resolve work items** permissions. More about how permissions interact

Create work items

The **Create work items** permission allows users to create work items in a space, even if they don't have the **Browse spaces** permission. This permission doesn't require Jira app access, and can be granted to any user who has access to your site. More about using this permission in public spaces

Delete work items

The **Delete work items** permission allows users to delete work items including their associated data, even if the user doesn't have **Delete all comments** or **Delete all attachments** permissions. However, it doesn't allow users to delete individual comments or attachments.

It can only be granted to users who have been invited by an admin.

Edit work items

The **Edit work items** permission allows users to edit a work item's fields, unless they're restricted by other permissions, such as:

- the **Assignee** field, which can be restricted by **Assign work items**
- the **Reporters** field, which can be restricted by **Modify reporters** and
- date fields, which can be restricted by **Schedule work items**

More about how permissions interact

It can only be granted to users who have been invited by an admin.

Link work items

The **Link work items** permission allows users to link work items (if your site allows it). To view links between work items in separate spaces, users need this permission in both spaces.

It can only be granted to users who have been invited by an admin.

Modify reporters

The **Modify reporters** permission allows users to change the **Reporter** field on a work item, which is set automatically when the work item is created.

It can only be granted to users who have been invited by an admin.

> This permission overlaps with the **Edit work items** permission. More about how permissions interact

Move work items

The **Move work items** permission allows users to:

- move a work item to another space or
- change it to a different work type

It can only be granted to users who have been invited by an admin.

> This permission requires the **Create work items** permission in the destination space. More about how permissions interact

Resolve work items

The **Resolve work items** permission allows users to:

- update the **Resolution** field and
- view the **Fix version** field on work items

It can only be granted to users who have been invited by an admin.

> Users may also need the **Transition work items** and **Close work items** permissions to close out work items. More about how permissions interact

Restore archived work items

The **Restore archived work items** permission allows users to restore work items that have been archived. It can only be granted to users who have been invited by an admin.

Schedule work items

The **Schedule work items** permission allows users to:

- change a work item's **Due date** and
- change work item ranking on a board and backlog

It can only be granted to users who have been invited by an admin.

> This permission overlaps with the **Edit work items** permission. More about how permissions interact

Set work item security

The **Set work item security** permission allows users to change the security level of a work item in spaces that use work item security schemes.

It can only be granted to users who have been invited by an admin.

Transition work items

The **Transition work items** permission allows users to update a work item's status to trigger workflow conditions.

It can only be granted to users who have been invited by an admin.

> Users may also need the **Resolve work items** and **Close work items** permissions to close out work items. More about how permissions interact

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Types of permissions you can grant in a space scheme

- Space access and configuration permissions
- Work item permissions in a space
- Time tracking permissions
- Voters, watchers, comment, and attachment permissions

On this page

- Archive work items
- Assign work items
- Assignable user
- Close work items
- Create work items
- Delete work items
- Edit work items
- Link work items
- Modify reporters
- Move work items
- Resolve work items
- Restore archived work items
- Schedule work items
- Set work item security
- Transition work items

Community

- Questions, discussions, and articles

 ©2026 Atlassian

Time tracking permissions

Use permission schemes to grant the permissions listed on this page.

> Users also need the **Browse spaces** permission to perform these actions. More about how permissions interact

It can only be granted to users who have been invited by an admin.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Work on work items

The **Work on work items** permission allows users to log time using the time tracking field in a space. It can only be granted to users who have been invited by an admin.

Delete all worklogs

The **Delete all worklogs** permission allows users to delete anyone's work log entries. It can only be granted to users who have been invited by an admin.

Delete own worklogs

The **Delete own worklogs** permission allows users to delete their own work log entries. It can only be granted to users who have been invited by an admin.

Edit all worklogs

The **Edit all worklogs** permission allows users to edit anyone's work log entries. It can only be granted to users who have been invited by an admin.

Edit own worklogs

The **Edit own worklogs** permission allows users to edit their own work log entries. It can only be granted to users who have been invited by an admin.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Types of permissions you can grant in a space scheme

Space access and configuration permissions

Work item permissions in a space

- **Time tracking permissions**

Voters, watchers, comment, and attachment permissions

On this page

Work on work items

Delete all worklogs

Delete own worklogs

Edit all worklogs

Edit own worklogs

Community

Questions, discussions, and articles

Voters, watchers, comment, and attachment permissions

Use permission schemes to grant the permissions listed on this page.

Users also need the **Browse spaces** permission to perform these actions. More about how permissions interact

Manage watchers

The **Manage watchers** permission allows users to add or remove watchers from a work item. It can only be granted to users who have been invited by an admin.

View voters and watchers

The **View voters and watchers** permission allows users to see who's watching work items. This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Add comments

The **Add comments** permission allows users to add comments or internal notes to work items or requests.

It can only be granted to users who have been invited by an admin.

Delete all comments

The **Delete all comments** permission allows users to remove comments (including customer comments!) and internal notes from work items. It can only be granted to users who have been invited by an admin.

Delete own comments

The **Delete own comments** permission allows users to remove their own comments on work items.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Edit all comments

The **Edit all comments** permission allows users to edit comments or internal notes added by anyone. It can only be granted to users who have been invited by an admin.

Edit own comments

The **Edit Own Comments** permission allows users to edit their own comments in a space.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Create attachments

The **Create attachments** permission allows users to attach files to a work item in a space, if your space allows attachments.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Delete all attachments

The **Delete all attachments** permission allows users to remove attachments from any work item in a space. It can only be granted to users who have been invited by an admin.

Delete own attachments

The **Delete own attachments** permission allows users to remove attachments they've added to a work item.

This permission doesn't require Jira app access, and can be granted to any user who has access to your site.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Types of permissions you can grant in a space scheme

Space access and configuration permissions

Work item permissions in a space

Time tracking permissions

- **Voters, watchers, comment, and attachment permissions**

On this page

Manage watchers

View voters and watchers

Add comments

Delete all comments

Delete own comments

Edit all comments

Edit own comments

Create attachments

Delete all attachments

Delete own attachments

Community

Questions, discussions, and articles

 ©2026 Atlassian

What are work item security schemes?

While permission schemes manage who can access a space, work item security schemes let you control who can see specific work items within that space. If someone isn't assigned to a security scheme, they won't be able to view those work items, even if they can access the rest of the space.

To view and update work item security schemes:

- users need to have the **Set work item security** permission. More about work item permissions
- spaces need to have the **Work item security** field included on their **Layout** page. Add fields to a layout

Create a new work item security scheme

When you move work from one space to another, the work item will be assigned to the default work item security level in the new space. If that space has no security scheme, this work will be visible to anyone with access to the space.

If you want to restrict an entire space, create a data classification level that can be applied to across an entire Jira Cloud space or a Jira Service Management space.

Restrict sensitive data using work item security schemes

- What are work item security schemes?

Create a new work item security scheme and security levels

Grant users access to security levels in a work item security scheme

Change which work item security scheme a space uses

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Create a new work item security scheme and security levels

While permission schemes manage who can access a space, work item security schemes let you control who can see specific work items within that space. If someone isn't assigned to a security scheme, they won't be able to view those work items, even if they can access the rest of the space. Set up your space for work item security schemes

The processes on this page require the **Administer Jira** permission.

Create a new work item security scheme

1. Select **Settings** ( ), then **Work items**.
2. Under the **Work item attributes** section, select **Work item security schemes**. You may need to scroll down since it's at the bottom of the list.
3. Select **Add work item security scheme**.
4. Name your new scheme, then select **Add**.

View and create security levels in a scheme

Next, you'll need to set up the levels of access. Select **Security Levels** in the **Action** column, which shows the existing security levels in this scheme, if any. To create a new one, add a name and description to the **Add security level** section on the page, and select **Add security level**.

If you'd like to apply this level to all work items in the spaces that use this scheme, select **Default** in the **Actions** column.

Once you've set up the security levels, you can grant users access to these levels and associate a work item security scheme to spaces.

Restrict sensitive data using work item security schemes

What are work item security schemes?

- **Create a new work item security scheme and security levels**

Grant users access to security levels in a work item security scheme

Change which work item security scheme a space uses

On this page

Create a new work item security scheme

View and create security levels in a scheme

Community

Questions, discussions, and articles

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Grant users access to security levels in a work item security scheme

Once you've created your work item security scheme, you'll need to define which users can access each security level. If someone isn't assigned to a security scheme, they won't be able to view those work items, even if they can access the rest of the space.

The processes on this page require the **Administer Jira** permission.

To give users access to a security level:

1. Select **Settings** ( ), then **Work items**.
2. Under the **Work item attributes** section, select **Work item security schemes**. You may need to scroll down since it's at the bottom of the list.
3. Select **Add** in the **Actions** column of the work item security scheme you'd like to add users to.
4. Select who you'd like to allow to access this security level based on:
5. Next, select who you'd like to grant access to. Choose from:
   a. **Space roles** - this refers to any custom space roles that you've set up – More about managing space roles
   b. **Application access** - any user with access to an app
   c. **Group** - these groups are managed by your Organization admin. Reach out to them to update group membership or to remove users from a group
   d. **Public** - More about publicly available spaces
   e. **Any logged in user**
   f. **Current assignee** - this grants access to anyone listed in a work item's **Assignee** field
   g. **Reporter** - this grants access to anyone listed in a work item's **Reporter** field
   h. **Group custom field value** - this grants access to anyone listed in a **Group picker** (single or multi-select) type field on a work item. You'll be asked which field you want to reference.
   i. **Space lead** - this grants access to anyone listed as the **Space owner** on a space's **Details** page. This is not the same as the **Administer spaces** permission.
   j. **Single user** - any user invited by your admin
   k. **User custom field value** - this grants access to anyone listed in a **User picker** (single or multi-select) type field on a work item. You'll be asked which field you want to reference.
6. Select **Add** to save your changes.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Restrict sensitive data using work item security schemes

What are work item security schemes?

Create a new work item security scheme and security levels

- **Grant users access to security levels in a work item security scheme**

Change which work item security scheme a space uses

Community

Questions, discussions, and articles

Change which work item security scheme a space uses

Once you've created your work item security scheme, you can apply it to any company-managed spaces across your site.

The processes on this page require the **Administer Jira** permission.

To give users access to a security level:

1. Select **Settings** ( ), then **Work items**.
2. Expand **Work items** in the space settings sidebar, then select **Security**.
3. Open the **Actions** menu, then select **Use a different scheme.**
   a. If you're adding a work security scheme to this space for the first time, this button will say **Select a scheme** instead.
4. Use the **Scheme** dropdown menu to select the work item security scheme you want use in this space, then select **Next**.
5. Use the dropdown menus to map work items with existing security restrictions to levels of the new scheme.
   a. Select **None** to remove work item restrictions.
   b. If you're adding a work security scheme to this space for the first time, this page will be empty. You can skip this step.
6. Select **Associate** then **Acknowledge** to save your changes.

Was this helpful? Yes No Provide feedback about this article

Still need help?

The Atlassian Community is here for you.

Ask the Community

Restrict sensitive data using work item security schemes

What are work item security schemes?

Create a new work item security scheme and security levels

Grant users access to security levels in a work item security scheme

- **Change which work item security scheme a space uses**

Community

Questions, discussions, and articles