User management

This section will show you how to manage users and user groups in your Kiuwan Account.

Contents:

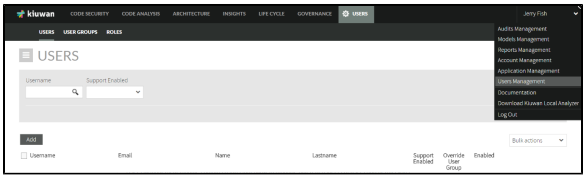
- Introduction to User Management
- Permission Model
  - Role-based Access Control (RBAC)
  - Permissions
  - Roles
  - Administration privileges
  - Users and User Groups
  - Permissions on Portfolios and Applications
- Users Management
  - Add a new user
  - Set user as owner
  - Set a new password
  - Set administration privileges
  - Set permissions on portfolios
  - Set permissions on applications
  - Bulk actions
- User groups
  - Create a new User Group
- Roles
  - Create a new Role

Introduction to User Management

In this section, let's review Permissions Management, Access Policy, and all the security-related issues of the Kiuwan account.

> **Single Sign-On**
>
> If your Kiuwan account is **Single Sign-On (SSO)** enabled, please visit How to integrate Kiuwan with SAML SSO - SSO login vs username-password login

The User Management module can be selected at the **top-left drop-down menu**.



The Users Management module contains 3 tabs that allow managing different aspects of users and permissions.

- **Users:** create, modify, and delete users; and also perform actions on selected users such as password setting, permissions granting, etc.
- **User Groups**: create sets of users that share the same privileges.
- **Roles:** manage named groupings of permissions that can be further used to grant privileges to users and user groups.

The use of these sections is straightforward if you clearly understand the concepts. So, in this document, we will focus on explaining the concepts.

Permission Model

Role-based Access Control (RBAC)

Kiuwan implements a role-based access control approach that allows you to fully define the permissions of your Kiuwan installation.

The Permission model is based in the tuple: **Subject - Role - Object**

- **Subject** means a **User** (John, Mary, etc) or a **Group of Users** (Developers, Functional Analysts, etc)
- **Role** means a grouped set of **permissions** (for example, Readonly, Write, etc)
- **Object** is any Kiuwan entity (basically, **Portfolios** and **Applications**)

A common misconception is to think that somebody can be assigned a role (John has Read role) that applies to all the objects. It does not work like this.

The three components of the tuple (Subject, Role, and Object) are always needed.

This permission model lets you define your access policy at a very fine-grain level.

Permissions

Kiuwan provides a set of **permissions** that you can grant to any user (or user group) over any portfolio or application.

Permission	Meaning
View deliveries	To view data of delivery analyses (defects, audit results, etc)
Delete deliveries	To delete delivery analyses
Execute deliveries	To execute delivery analyses
View application data	To view analysis data (defects, metrics, action plans, etc)
Execute analyses	To execute baseline analyses (CS, CA and IS)
Execute analyses in the cloud	To execute baseline analyses uploading the code to the Kiuwan cloud Saas
Delete analyses	To remove baseline analyses
Mute defects	To mute defects on baseline and delivery analyses
Change defect status	To change the status of a defect on baseline and delivery analyses
Save action plans	To create and edit actions plans
Delete action plans	To remove existing action plans
Export action plans to JIRA	To use the Jira plugin to create issue from action plans
View analyzed source code	To view the defects together with the complete source code (this option is sold separately)
Upload analyzed source code	To upload the complete source code to Kiuwan so the defects could be inspected in the full source code
Upload source code fragments	To upload only the code line where the defect is found.

Roles

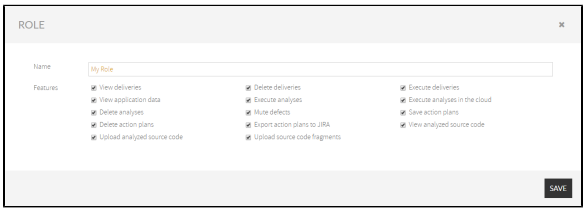
A **Role** is a **concrete set of permissions**.

Kiuwan provides several **built-in roles**. These predefined roles are commonly used and can serve as templates to create your own custom roles.

Built-in role	Common use
None	An empty set of permissions. It means no access at all.

Readonly	Users that should only be granted read-only access to analysis data (baselines and deliveries)
Readonly deliveries	Similar to Read only, but restricted to data coming from deliveries analyses, not granted to see baseline data
Write	Suitable for users that should have full access to an application (execute analyses, delete them, etc)
Write deliveries	For users that should only be allowed to execute (and view) delivery analyses, not being permitted to access baseline data.

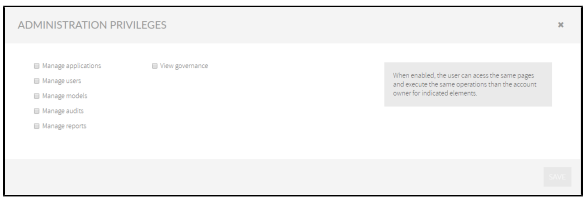
Built-in roles cannot be modified but you can create as many **custom roles** as you need, selecting among the available permissions.



Keep in mind that roles are assigned to Portfolios or Applications. There are not global roles: a role always applies to some object.

Administration privileges

In addition to permissions and roles, there are some **Administration privileges** that can be granted to users or groups of users.



Admin privileges	Description
Manage applications	Any user with this privilege is allowed to create, edit, and delete Applications and Portfolios. Granting this privilege to a user will allow full access to the Application Management module where that user will be able to create and manage Kiuwan apps (to classify the app on portfolios, to assign a quality model and audits, etc). See Applications management for further information on this subject.
Manage users	Granting this privilege to a user will allow full access to Users Management module where that user will be able to: ○ Create and delete account users ○ Change the account owner ○ Grant Admin privileges to users Additionally, combined with “Manage applications”, the user will be able to: ○ Create user groups and new roles ○ Assign permissions on portfolios or applications to users (or group of users)
Manage models	To create, modify, publish, and delete Models, as well as to configure the Default Model. Granting this privilege to a user will allow full access to the Models Management module where the user will be able to create and manage Quality Models. See Models Manager User Guide for further information on this subject.

Manage audits	To create, modify, publish, and delete Audits as well as to configure the Default Audit. See Audits Management for further information on this subject.
Manage reports	To create, modify, publish, and delete Custom Reports. See Custom Reports for further information on this subject.

Important :

- Any user granted with **ALL admin privileges** becomes an "**admin**"
- **The account owner** is the full "admin" of the account and can create additional admins by granting all the admin privileges.

Global permissions	Meaning
View governance	Access to the Governance module. Even with this privilege, the user will only see aggregated data from "allowed" applications (i.e. at least with Readonly role) See Kiuwan Governance Doc for further info on this subject.
Support Enabled	Access to Kiuwan Technical Support (chat or ticket-based)

Users and User Groups

You can create single **Users** as well as **User Groups**, and assign permissions to single Users or to User Groups.

- If a user belongs to one User Group, the permissions granted to that user will be those granted to the User Groups he belongs to.
- If a user belongs to more than one User Group, the resulting set of granted permissions is the union (OR) of every user group's permissions, i.e. the user will have permissions from one group plus the permissions from the other groups.

If you want to avoid this "user group's inheritance", select "**Override User Group**" and that user will be granted only with the permissions exclusively assigned to him, regardless of his /her membership to any user group.

Permissions on Portfolios and Applications

Any application can be classified according to the available Groups of Portfolios.

There are two **built-in groups of portfolios**: Business Value and Provider

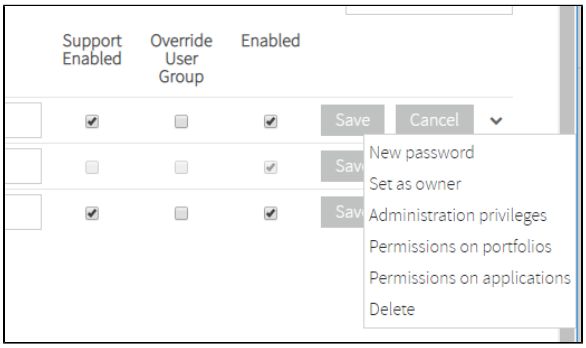
Group of Portfolio	Meaning	Values
Business Value	Classification of the app according to this value from a business point of view	Fixed and not-modifiable set: • Critical, High, Medium, Low and Very Low
Provider	Company in charge of developing/maintaining the application	Empty by default: • custom values can be defined

Besides these built-in groups, you can create as many **custom groups of portfolios** as you need.

Any application will always have a value for each of the existing groups of portfolios:

- either a concrete value
- or **unassigned** (if that app has not been explicitly classified into that group

Then, if you want to grant permissions based on Portfolios, just select the option: **Permissions on portfolios**.



Then, you can select the specific access Role (i.e. the set of permissions) to every portfolio of the available groups.

IMPORTANT: If some application is **unassigned** in some group, **None** role is assumed (i.e. no-access)

Since any application can be classified in **several portfolio groups**, the final permissions set for the app is the **union of allowed actions for every role assigned to every portfolio group**.

Here is an **example:**

- You define a user with **ReadOnly** permissions on apps with portfolio value **High** in a **Business Value** portfolio.
    - This means that for any application classified as such, that user will have the allowed actions defined in ReadOnly role.
- Also, you define for the same user **None** as the role for apps with value **South Africa** in the **Pro vider** portfolio group.

What would be the permissions for an app that is High (in Business Value) and South Africa (in Provider)?

As said above, it would be the **union set**, being in this case equal to the ReadOnly role.

Another **example**.

- You define a **Mute defects** role with only Mute defects action, and a **Create Notes** role with only Create Note action.
- You associate Mute defects to **High** and Create Notes to **South Africa**.

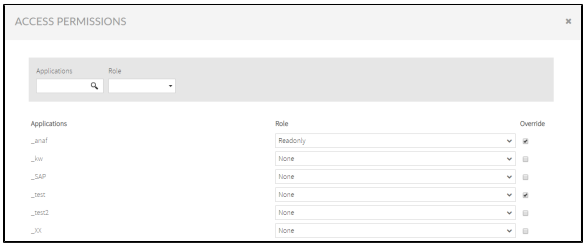
What would be the resulting set for any app classified as such?

The user will be able to Mute defects AND Create Notes.

Because every application is always classified into every group of the portfolio, **permissions on portfolios take precedence to permissions on applications**.

If you need to **override** this behavior and grant permissions directly to the application (regardless of its classification):

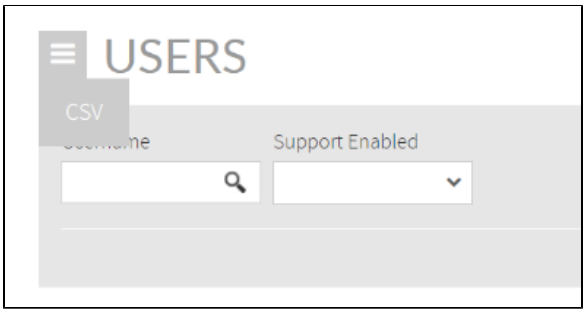
- select **Permissions on applications**
- select the Role and
- be sure to check **Override** (otherwise, the portfolios permissions will apply).



Users Management

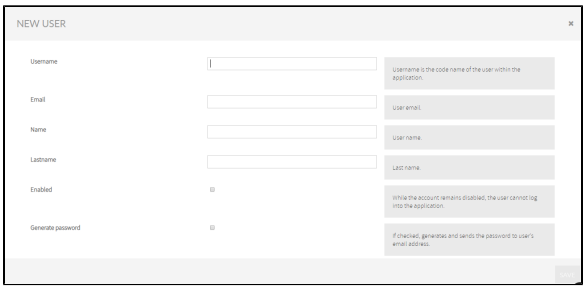
The User Management section allows you to manage the users and their permissions associated with your account.

Open the hamburger menu and select **CSV** to export a full list of users and permissions to a CSV file.



Add a new user

Click **Add** to open the **New User form**.



Name	Description

Username	This is the unique identifier of a Kiuwan user. The user must specify this username whenever accessing Kiuwan. The username must be unique so it's recommended to use a suffix that identifies all users in your organization.
Email	This is the email address of the user so any Kiuwan notification will be sent to that email address. Email does not need to be unique, so there can be users with the same email address.
Name & Lastname	These are descriptive fields to further identify the user.
Enabled	This checkbox allows enabling/disabling the user to access the Kiuwan account.
Generate Password	If this checkbox is checked, Kiuwan will send a new password to the user. New users cannot access Kiuwan until they receive their password.

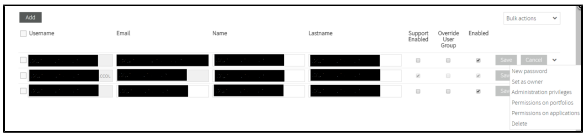
Set user as owner

In the dropdown menu of each user, select **Set user as owner** to change the account owner.

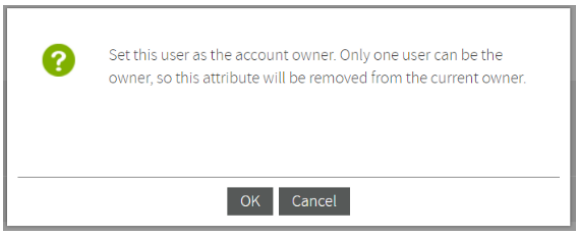
Every Kiuwan account has a unique account owner. The account owner is granted full permissions on account administration, applications, and portfolios.

> Any user can be set as Account Owner by the current owner, and by assigning this role to a new user the current owner will cease to be the current owner.

Once a new user is set as the owner, the old owner will be set with default permissions (none).



Confirm this action in the pop-up window that shows up once you have selected the *Set as owner* option for any user:



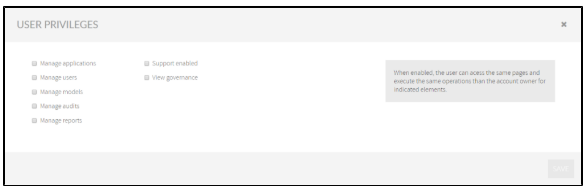
Set a new password

In the dropdown menu of each user, you can also select **New password** for the selected user.

Selecting this option will generate a new password and send it to the user's email address.

Set administration privileges

Administration privileges can be granted to any users, which enable them to manage applications, users, quality models and/or audits as if they were the account owner.



For a full explanation of admin privileges, see Administration privileges

Set permissions on portfolios

The account owner (or any user with **Manage Users** privilege) can assign application permissions based on the app classification in portfolio groups.

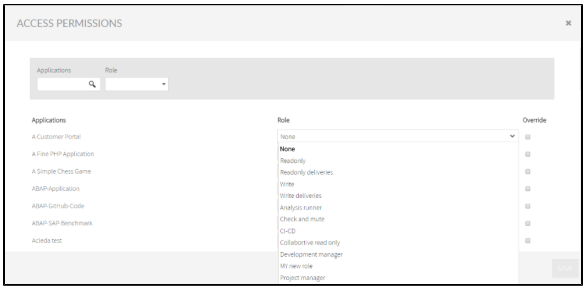
Permissions can be assigned to portfolio values by selecting a Role (i.e. a defined set of allowed actions) for every portfolio value.

Please see Permissions on Portfolios and Applications to fully understand the permissions assignment.

> **Important**: Permissions based on portfolio values take precedence over app permissions.
>
> In case you want app permissions to take precedence over portfolios permissions, you should check **Override** in Application Access Permissions.

Set permissions on applications

The account owner (or any user with **Manage User** privilege) is entitled to assign specific application permissions.



> Select **Override** to prioritize the role assigned to that user and application over the role selected on Access permissions to Portfolios.

Refer to the section Permissions on Portfolios and Applications to fully understand the permission assignment.

Bulk actions

If you want to set the same option for several users at once, you can do it by selecting those users. Then, choose the corresponding option on Bulk actions dropdown menu, as shown below:

User groups

A User Group is a set of users that shares the same permissions (admin privileges and/or permissions on apps and portfolios).

When you need to assign the same permissions on the same entities (apps and portfolios), you can create a **User Group** and then define the set of privileges and assign users to that User Group.

Doing this way, with one click you will be able to grant all the users of that group the same permissions instead of granting one by one.

For example, you can divide users into development teams, so the users in the same user group will be able to manage the applications they are working with the same set of privileges.

Any user can be assigned to many user groups. In this case, **a union of all user group's permissions will be granted to that user**.

- If a user belongs to **one** User Group, the permissions granted to that user will be those granted to the User Groups he belongs to.
- If a user belongs to **more than one** User Group, the resulting set of granted permissions is the **union** (OR) of every user group's permissions, i.e. the user will have permissions from one group plus the permissions from the others group.

In case of **conflicting permissions** on the same entities (apps and portfolios), **the most permissive set is applied**.

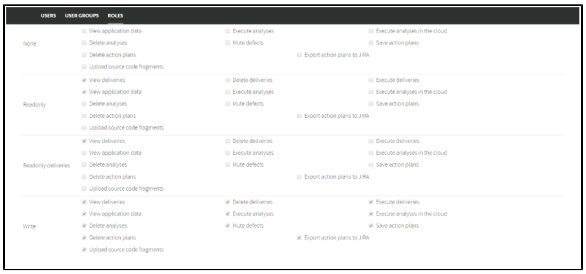
> Once a user belongs to a User Group it will not be possible to assign individual permissions for that user.
>
> If you want to avoid this user group inheritance, select **Override User Group** and that user will be granted only with the permissions exclusively assigned to him, regardless of his membership to any user group.
>
> In this way, individual permissions will be granted instead of a user group's permissions.

Create a new User Group

To create a new User Group, click on **Add** button and **drag&drop users** from **Not Member Users** to **Group Members**.

Roles

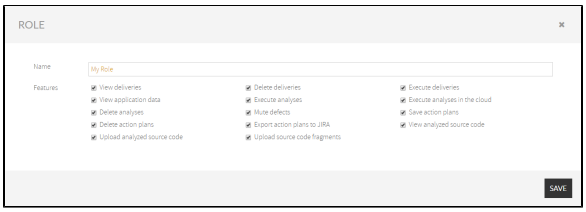
You can manage the different user roles by clicking on the namesake button in User Management.



Please visit Roles for details.

Create a new Role

You can add new roles and select their enabled actions by clicking on **Create New Role**.



You can manage the actions the different roles can perform by selecting the appropriate checkboxes for each role.