Managing Users and Permissions

As of API Management 21.1 all users and permissions are maintained in the Scheer PAS Administration. Refer to the Scheer PAS | Administration Guide for more information on this.
If you do not want to stick with the standard API Management roles but want to configure your own dedicated roles, refer to Managing API Management Roles further below.

Managing API Management Access

API Management uses the **Scheer PAS** *Administration* to manage its users. Refer to this guide for more information on the related tasks.

API Management uses the Identity Management to manage its users. This tool can manage users for multiple applications. Data for each application is stored in so called "realms":

- Users of Identity Management itself are stored to realm **Master**.
- Users of API Management and Log Analyzer are stored to realm **Apiman**.

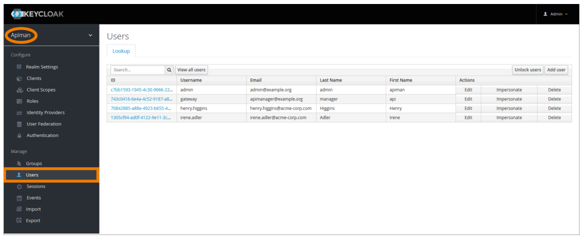
Thus, you need to have to separate admin accounts: one for Identity Management, and one for API Management.

Managing Users

To work on users for API Management,

1. Go to the Keycloak UI at https://<my API Management host>:<Keycloak port>, e.g. https://api.scheer-acme.com:8445 .
2. Log in as a **Keycloak** admin.
   A Keycloak admin account has been created during the installation of API Management.
3. Select realm **Apiman**.

Go to tab **Users** to add, change or delete users.



Users

ID	Username	Email	Last Name	First Name	Actions		
c7bb1593-1945-4c30-9666-22...	admin	admin@example.org	admin	apiman	Edit	Impersonate	Delete
743c0416-6e4a-4c52-9187-a8...	gateway	apimanager@example.org	manager	api	Edit	Impersonate	Delete
70842885-a88e-4923-b655-4...	henry.higgins	henry.higgins@acme-corp.com	Higgins	Henry	Edit	Impersonate	Delete
1305cf94-ad0f-4122-9e11-3c...	irene.adler	irene.adler@acme-corp.com	Adler	Irene	Edit	Impersonate	Delete

The user list shows two users **admin** and **gateway** that have been created during the installation process, and all additional users that have already been created.

- Assign group **API-Mgmt-Users** to users that should be able to login to API Management.
- Assign group **API-Mgmt-Kibana-Users** to users that should be able to generate reports with Kibana.
- Assign group **API-Mgmt-Devportal-Users** to users that should be able to access APIs via the Developer Portal.
- Assign group **API-Mgmt-Administrators** to users that should be an API Management admin.

For more information on group management and permissions, refer to Managing Groups below.

> Never delete or change the generated user **gateway**. This may result in API Management not working anymore.

Refer to the Keycloak documentation for more information on all options.

Managing Groups

To manage API Management user groups

1. Go to the Keycloak UI at https://<my API Management host>:<Keycloak port>, e.g. https://api.scheer-acme.com:8445 .
2. Log in as a **Keycloak** admin.
   A Keycloak admin account has been created during the installation of API Management.

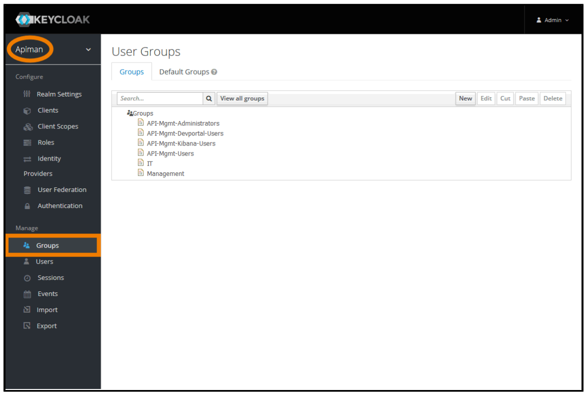
On this Page:

Related Documentation:

- Scheer PAS | Administration Guide
- Official Keycloak Documentation

3. Select realm **Apiman**.

Go to the **Groups** tab to add, change or delete groups.



User Groups

- Groups
  - API-Mgmt-Administrators
  - API-Mgmt-Devportal-Users
  - API-Mgmt-Kibana-Users
  - API-Mgmt-Users
  - IT
  - Management

API Management comes with four standard groups:

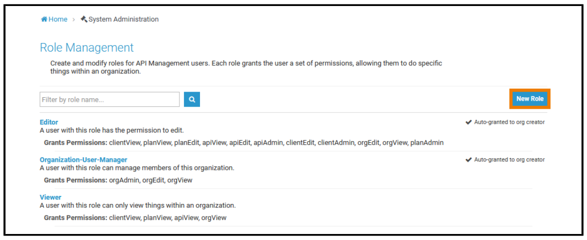
Role Name	Description
API-Mgmt-Administrator	This group grants users administration rights for API Management. ✓ Use this group to create additional API Management admins, see How to Create Additional Admins.
API-Mgmt-Devportal-Users	This group grants users access to the Developer Portal. This is the default group when a new user is created in the administration of the Developer Portal.
API-Mgmt-Kibana-Users	This group grants users access to the Kibana reporting tool.
API-Mgmt-Users	This group is for API Management users. All users must have this group assigned to be able to log into API Management at all.

⚠ Do not change the default groups. This may result in API Management not working anymore. You can always add own groups.

Managing API Management Roles

API Management allows to set up roles and permissions allowing your user to do specific things within an API Management organization. Your API Management installation comes with a standard set of roles and permissions but you can extend these to meet specific requirements.

Select **Administration > Manage Roles** to open role management.
On the **Role Management** page, administrators can create and modify roles for API Management users.



Role Management

Create and modify roles for API Management users. Each role grants the user a set of permissions, allowing them to do specific things within an organization.

Editor
A user with this role has the permission to edit.
✓ Auto-granted to org creator
Grants Permissions: clientView, planView, planEdit, apiView, apiEdit, apiAdmin, clientEdit, clientAdmin, orgEdit, orgView, planAdmin

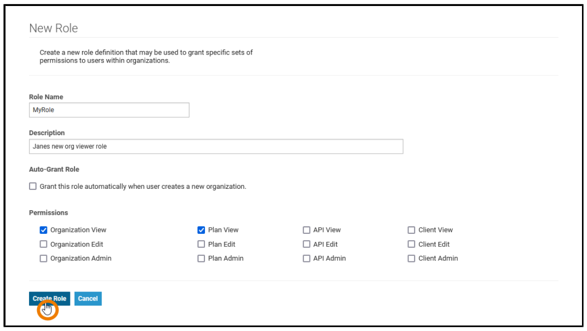
Organization-User-Manager
A user with this role can manage members of this organization.
✓ Auto-granted to org creator
Grants Permissions: orgAdmin, orgEdit, orgView

Viewer
A user with this role can only view things within an organization.
Grants Permissions: clientView, planView, apiView, orgView

API Management comes with three standard roles:

Role Names	Description	Permissions

Editor	Grants the user the permission to edit.	API Admin, API Edit , API View, Client Admin, Client Edit , Client View, Organization Edit, Organization View, Plan Admin , Plan Edit, Plan View
Organizations-User-Manager	Users with this role can manage members of this organization.	Organization Admin, Organization Edit, Organization View
Viewer	Grants the user read-only access to an organization.	API View, Client View , Organization View, Plan View

 New Role Create a new role definition that may be used to grant specific sets of permissions to users within organizations. Role Name: MyRole Description: Janes new org viewer role Auto-Grant Role ☐ Grant this role automatically when user creates a new organization. Permissions ☑ Organization View ☑ Plan View ☐ API View ☐ Client View ☐ Organization Edit ☐ Plan Edit ☐ API Edit ☐ Client Edit ☐ Organization Admin ☐ Plan Admin ☐ API Admin ☐ Client Admin 	Click **New Role** if you need additional roles for your users. On page **New Role** you will find the following configuration options: • **Role Name** • **Description** (optional) • **Auto-Grant Role** • **Permission** After having configured the new role, click **Create Role** to finish and save your changes.

The following permissions can be granted for roles:

Permission	Description
API Admin	Users with this permission are allowed to delete, edit, publish and retire APIs.
API Edit	This permission includes viewing, creating and editing of APIs.
API View	Grants the user the permission to view APIs.
Client Admin	Users with this permission are allowed to edit, delete, register and re-register clients.
Client Edit	This permission includes viewing, creating and editing of clients.
Client View	Grants the user the permission to view clients.
Organization Admin	Users with this permission are allowed to add new members to it and manage the roles of organization members.

Organization Edit	This permission includes viewing and editing of organizations.
Organization View	Grants the user the permission to view an organization and its members.
Plan Admin	Users with this permission are allowed to edit, delete and lock plans.
Plan Edit	This permission includes viewing, creating and editing of plans.
Plan View	Grants the user the permission to view plans.