SELISE Blocks Localization Language Translator

Setup & Configuration Guide

Platform: SELISE Blocks Cloud

Microservices URL: api.seliseblocks.com

1. Environment Overview

This section covers the initial setup of the SELISE Blocks environment on the SELISE Blocks Cloud platform. The Environment Overview page provides all key configuration details needed to connect and deploy your application.

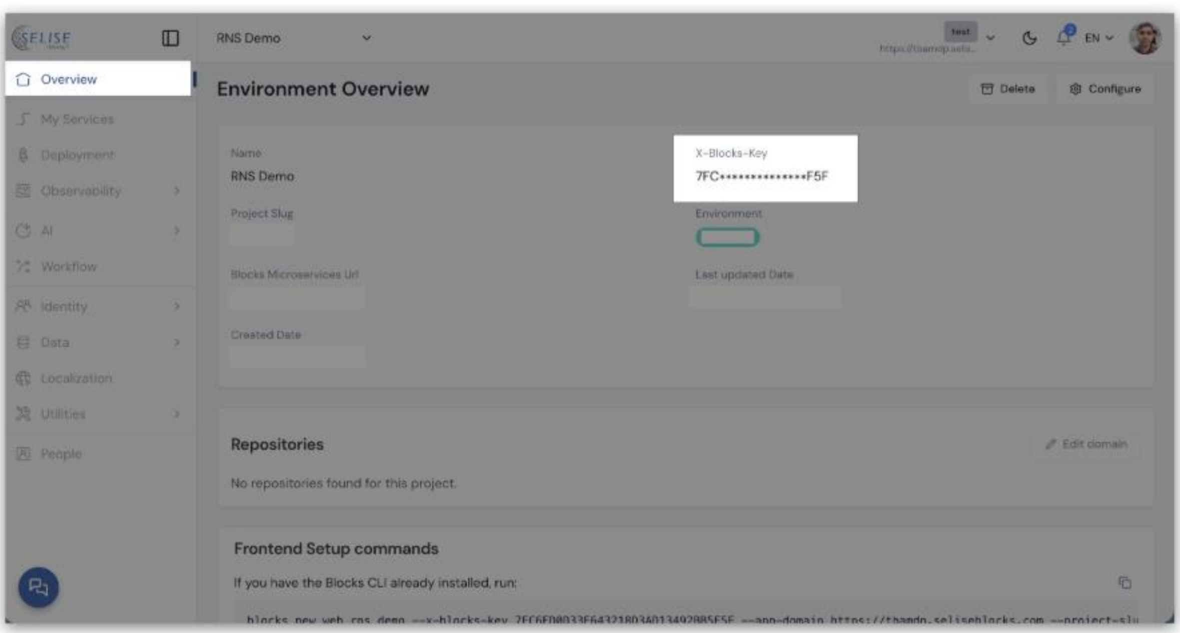
1.1 Environment Details

The following table summarizes the environment configuration:

Name	SELISE Blocks
Blocks Microservices URL	api.seliseblocks.com

1.2 Retrieving the X-Blocks-Key or Project Key

The X-Blocks-Key / Project Key is a masked API key used to authenticate requests to your Blocks environment. It is displayed on the Environment Overview page.



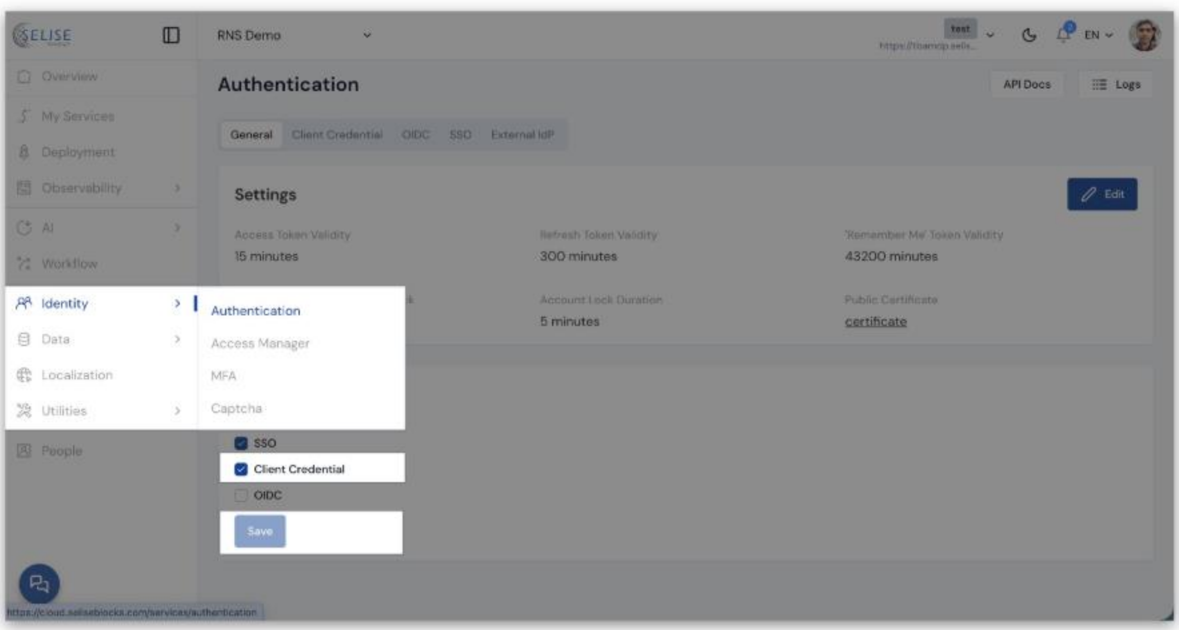
Step	Action	Details
1	**Navigate to Environment Overview**	Open the SELISE Blocks Cloud console (https://cloud.seliseblocks.com) and select your project (SELISE Blocks).
2	**Locate X-Blocks-Key**	On the Environment Overview page, find the X-Blocks-Key field. The value is displayed in masked format (e.g., Rfb**************8ac).
3	**Copy the Key**	Click the copy icon next to the masked value to copy the full key to your clipboard.

2. Authentication Configuration

The Authentication section allows you to configure how users and services authenticate with your SELISE Blocks environment. This includes token validity settings, grant types, and client credentials.

2.1 Enabling Client Credential Grant Type

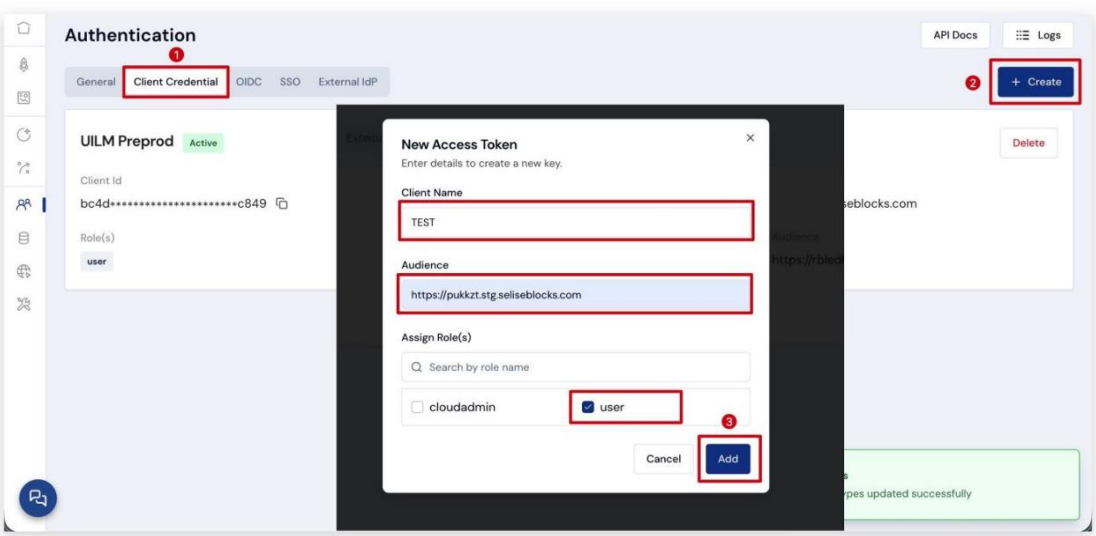
To allow machine-to-machine authentication (e.g., for backend services or APIs), the Client Credential grant type must be enabled.



Step	Action	Details
1	**Navigate to Authentication**	In the left sidebar, click the Identity/Access Manager icon, then select Authentication.
2	**Review Token Settings**	On the General tab, verify the token validity settings. Default values: Access Token = 15 min, Refresh Token = 300 min, Remember Me = 43200 min, Account Lock Duration = 5 min.
3	**Enable Client Credential**	In the Grant Types section, click Edit and check the Client Credential checkbox.
4	**Save**	Click Save to apply the updated grant types.

2.2 Creating a New Client Credential (Access Token)

After enabling the Client Credential grant type, you can create new access tokens for client applications.

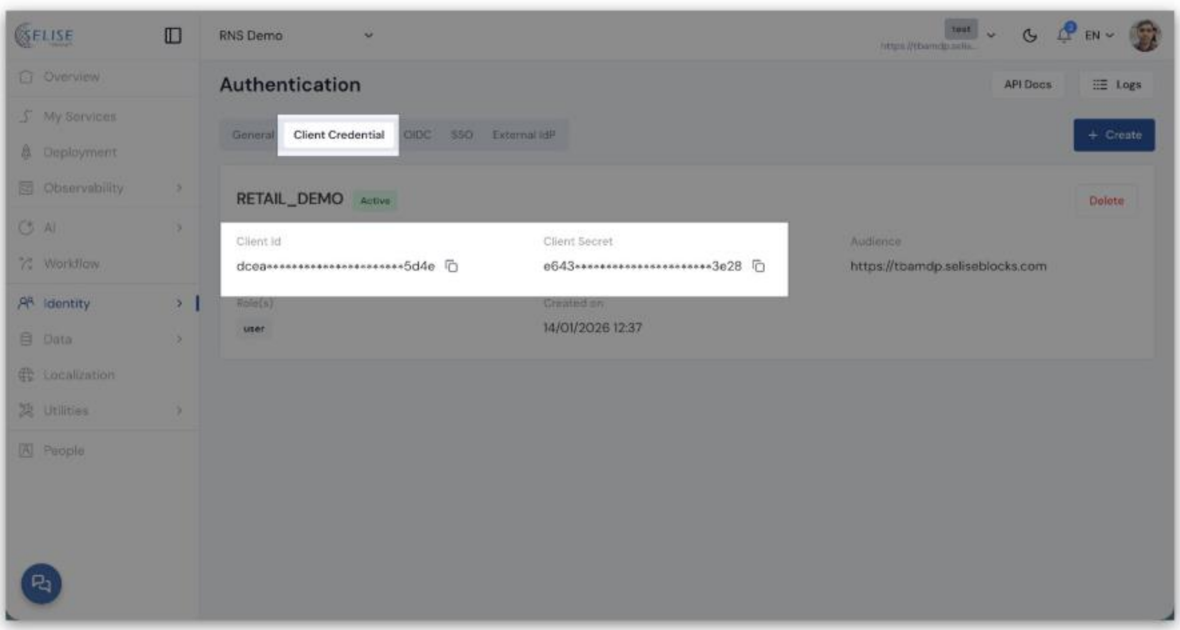


Step	Action	Details
1	**Go to Client Credential Tab**	In the Authentication page, click the Client Credential tab.

2	**Click + Create**	Click the + Create button in the top-right corner to open the New Access Token dialog.
3	**Fill in Token Details**	Enter the Client Name (e.g., TEST), Audience URL (e.g., https://pukkzt.stg.seliseblocks.com), and assign the required Role(s) by checking the appropriate checkboxes (e.g., user).
4	**Add the Token**	Click Add to create the access token.

2.3 Viewing Client Credentials

Once a client credential is created, you can view the Client ID and Client Secret from the Client Credential tab.



Client ID	bc4d*********************c849 (masked — copy using the icon)
Client Secret	4da6*********************0c60 (masked — copy using the icon)
Audience	https://rbledk.seliseblocks.com
Role(s)	user

Note: The Client Secret is only fully visible immediately after creation. Store it securely, as it cannot be retrieved again after leaving the page.

3. Identity and Access Management (IAM)

The Identity and Access Management (IAM) module controls permissions, roles, and user access within the SELISE Blocks environment. It is accessible from the left sidebar under the people/identity icon.

3.1 Adding a New Permission

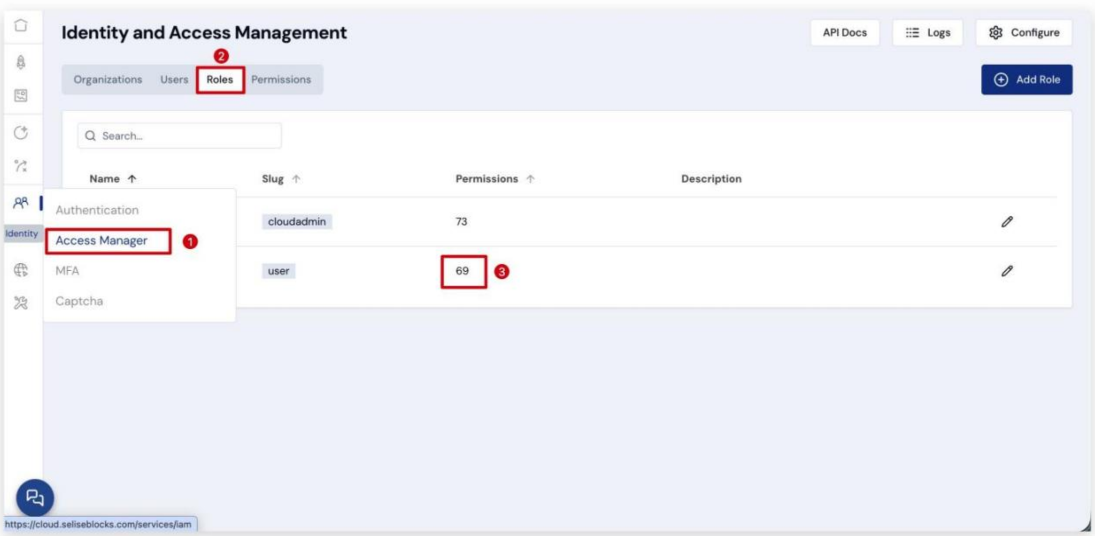
Permissions define specific actions that can be performed on resources. Follow these steps to add a new permission.

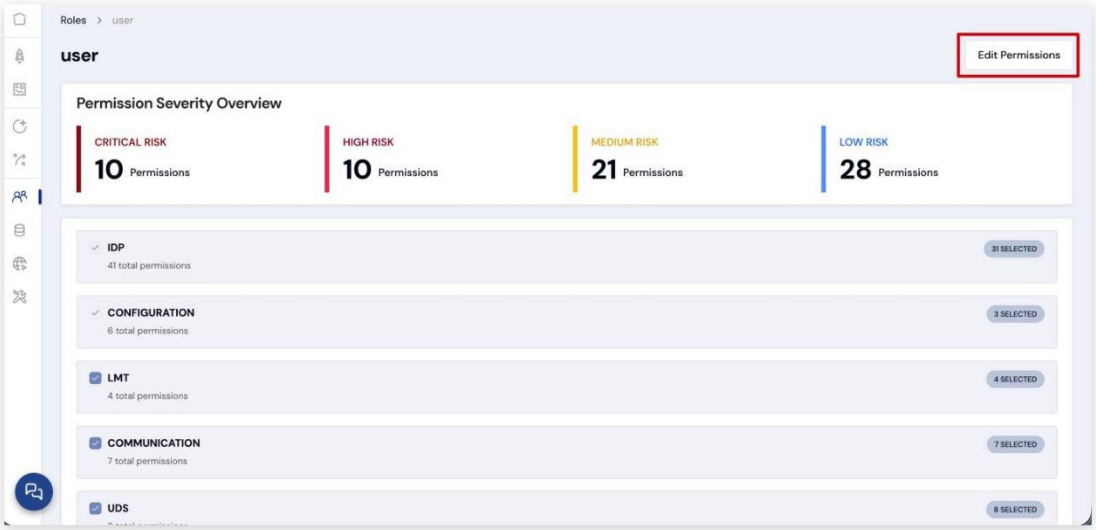
Step	Action	Details
1	**Navigate to IAM**	In the left sidebar, click the Identity/Access Manager icon to open the IAM module.
2	**Go to Permissions Tab**	Click the Permissions tab in the IAM navigation bar.

3	**Click Add Permission**	Click the + Add Permission button in the top-right corner.
4	**Fill in Permission Details**	Complete the form using below informatons: • Name: localization::config::savewebhook • Type: Endpoint • Resource: blocks-localization-api::config::savewebhook • Group: localization • Severity: Medium
5	**Save**	Click Save to create the permission.

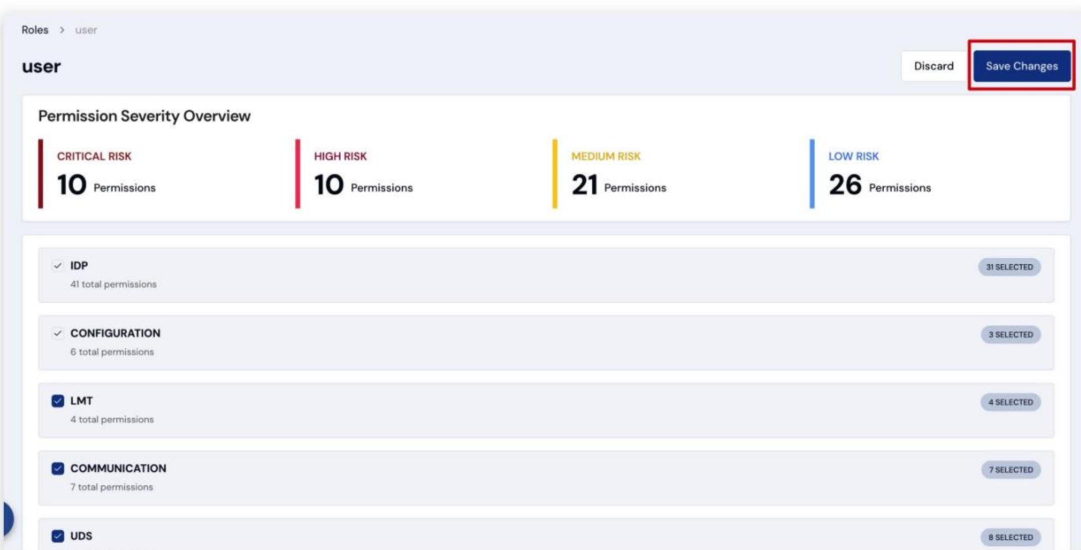
3.2 Managing Roles

Roles group permissions together and can be assigned to users or client credentials. The IAM module provides a Roles tab to view and manage all roles.




Roles > user
user
Edit Permissions
Permission Severity Overview
CRITICAL RISK
10 Permissions
HIGH RISK
10 Permissions
MEDIUM RISK
21 Permissions
LOW RISK
28 Permissions
IDP
41 total permissions
31 SELECTED
CONFIGURATION
6 total permissions
3 SELECTED
LMT
4 total permissions
4 SELECTED
COMMUNICATION
7 total permissions
7 SELECTED
UDS
8 SELECTED


LOCALIZATION
15 total permissions
13 SELECTED
localization::module::gets
Retrieves a list of all available modules
LOW ENDPOINT
localization::language::gets
Retrieves all available languages
LOW ENDPOINT
localization::key::gets
Retrieves all available keys based on filters
LOW ENDPOINT
localization::key::gettimeline
Retrieves key timeline with pagination
MEDIUM ENDPOINT
localization::key::get
Retrieves specific item by ID
LOW ENDPOINT
localization::key::getuilmfile
Returns a JSON UILM file for the specifed module and language
LOW ENDPOINT
localization::config::savewebhook
No description available.
LOW ENDPOINT


Roles > user
user
Discard
Save Changes
Permission Severity Overview
CRITICAL RISK
10 Permissions
HIGH RISK
10 Permissions
MEDIUM RISK
21 Permissions
LOW RISK
26 Permissions
IDP
41 total permissions
31 SELECTED
CONFIGURATION
6 total permissions
3 SELECTED
LMT
4 total permissions
4 SELECTED
COMMUNICATION
7 total permissions
7 SELECTED
UDS
8 SELECTED

Step	Action	Details
1	**Navigate to Roles**	Click the Roles tab in the IAM navigation bar.
2	**View Existing Roles**	The roles list shows all available roles. In this environment: • cloudadmin — 73 permissions • user — 69 permissions
3	**Access Role Details**	Click on a role (e.g., user) to view a detailed Permission Severity Overview, including Critical, High, Medium, and Low risk permission counts.

3.3 Editing Role Permissions

You can add or remove permissions from a role using the Edit Permissions workflow.

Step	Action	Details
1	**Open Role Details**	From the Roles tab, click on the role you want to edit (e.g., user).
2	**Click Edit Permissions**	Click the Edit Permissions button in the top-right corner of the role details page.
3	**Select Permissions by Group**	Permissions are organized by group (IDP, CONFIGURATION, LMT, COMMUNICATION, UDS, LOCALIZATION, etc.). Expand a group and check/uncheck individual permissions as needed.
4	**Save Changes**	Click Save Changes to apply the updated permission set. Click Discard to cancel.

3.4 Localization Permissions Reference

The LOCALIZATION group contains 15 total permissions. The following table lists the available localization permissions and their risk levels:

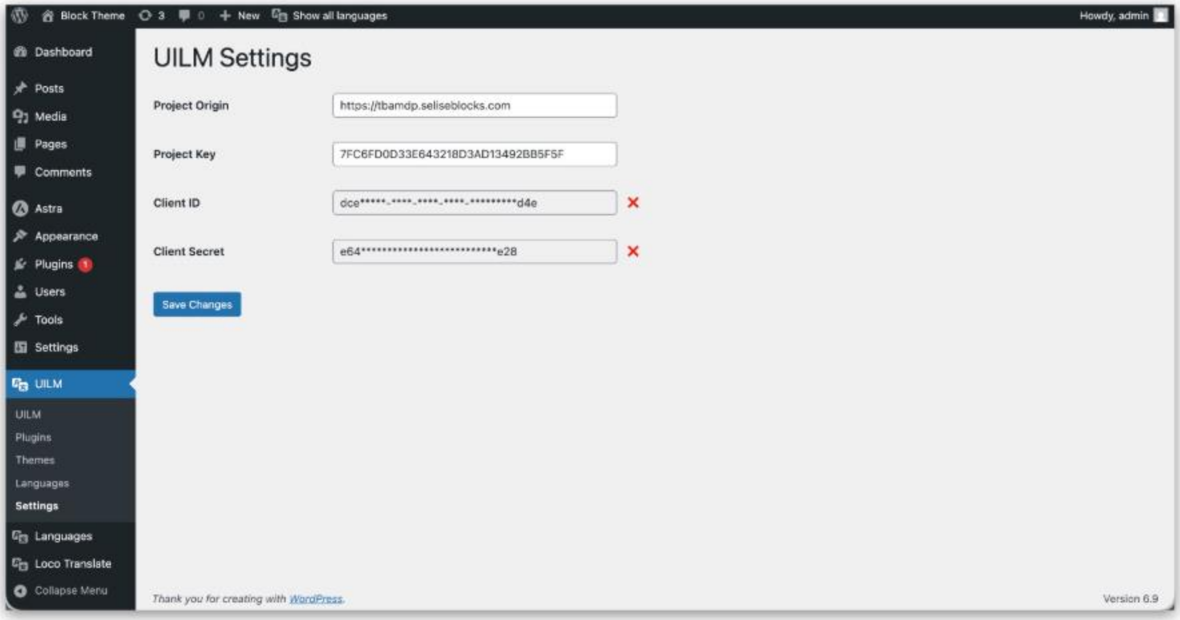
Permission	Description	Severity

`localization::module::gets`	Retrieves a list of all available modules	LOW
`localization::language::gets`	Retrieves all available languages	LOW
`localization::key::gets`	Retrieves all available keys based on filters	LOW
`localization::key::gettimeline`	Retrieves key timeline with pagination	MEDIUM
`localization::key::get`	Retrieves specific item by ID	LOW
`localization::key::getuilmfile`	Returns a JSON SELISE Blocksfile for the specified module and language	LOW
`localization::config::savewebhook`	Saves webhook configuration	LOW

4. Plugin Setup

Once the environment and authentication are configured, you can set up your frontend application using the Blocks CLI.

1. Go back to your **WordPress Admin Dashboard**.
2. Open the **AI Language Translator** plugin settings.
3. Paste the following details:
    a. Project Origin
    b. Project Key
    c. Client ID
    d. Client Secret



4. Save the settings.

🎉 Your plugin is now fully configured and ready to use.