

# Sedona API / SedonaCloud POSTMAN calls and Testing

10/02/2025 9:59 am EDT

## Sedona API / SedonaCloud POSTMAN calls

If you have not yet created users for your company, you will need to log into your site using the HostAdmin account.

Using a Host Admin Credential login to your company host SW 2.0 site

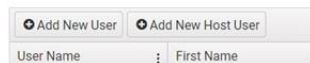
If you do not have the password and have setup your SMTP settings you can use the forgot password option.

Once logged in, you can create company user logins to access the company.

Go to Users, then select Add New User



### Users



Enter the user information and select a Role. Be sure to select the new company name for the user. [Sedona X is not required for API testing]

The image shows the 'Add User' form. It has a title 'Add User' and 'Submit' and 'Cancel' buttons. The form contains several fields: 'Company Name' (dropdown menu), 'User Name' (text input), 'First Name' (text input), 'Last Name' (text input), 'Email' (text input), 'Password' (text input with a strength indicator), 'Confirm password' (text input), 'Site Theme' (dropdown menu), and 'Enable Sedona-X Mobile' (checkbox). At the bottom, there are tabs for 'Token' and 'Permissions'.

If you are testing APIs with Postman or keys, use the information below.

The API uses OAuth 2.0.

You can use the settings below for your collection.

You will need to create a Company User account to use to get the token.

You can setup a user just for the API use or any users login.

If you have more than one company, you have to select which company they will use when sending requests.

## Add User

Company Name: Sedona Security

User Name: APIAccess

First Name: API

Last Name: User

Email: API@Email.com

Password: [masked]

Confirm password: [masked]

Site Theme: Default

Enable Sedona-X Mobile:  DISABLED

Token | Permissions

Company Admin  Role Group

These are the settings needed for Postman

Authorization type: OAuth 2.0

Add auth data to: Request Headers

Under the Configure New Token section

Grant Type: Password Credentials

**Access Token URL** [https://\[YOUR-SEDONAWEB2-SITE-HERE\]/connect/token](https://[YOUR-SEDONAWEB2-SITE-HERE]/connect/token)

**Client ID:** SedonaCloudClient

**Client Secret (API KEY):** [Provided in original Professional Svcs Project Documentation or from Octopus ]

Username: Company User Login created in the step above or designated

Password: Company User Password created in the step above or designated

**Scope:** sedonacloudapi sedonacloudscope openid offline\_access

Client Authentication: Send as Basic Auth header

The API Documentation can be found at the link below.

**URL** [https://\[YOUR-SEDONAWEB2-SITE-HERE\]/api/help/index.html](https://[YOUR-SEDONAWEB2-SITE-HERE]/api/help/index.html)

Below is the setup for a test collection in Postman.

Authorization ● Pre-request Script Tests ● Variables ●

This authorization method will be used for every request in this collection. You can override this by specifying one in

Type

The authorization data will be automatically generated when you send the request.  
[Learn more about authorization](#)

Add auth data to

**Current Token**  
This access token is only available to you. Sync the token to let collaborators on this request use it.

Access Token

Header Prefix

**Configure New Token**  
Configuration Options ● Advanced Options

Token Name

Grant Type

Access Token URL

Client ID

Client Secret

Username

Password

Scope

Client Authentication

If you need further assistance with API calls or custom work for an integration beyond user creation, this will be beyond normal support and we can have your account manager follow up with you to scope out a project for your needs.