Accessing Insight

This chapter will demonstrate how you can make Insight for Jira Cloud more powerful and customized using our Cloud REST API.

**Note:**

Only a Jira Administrator can access this section and generate/manage Tokens

To use the REST API, you must have a valid personal access token. You can get a personal access token from within the Configuration menu.

Generate a personal access token to allow secure access to Insight. You can use this token to call REST APIs.

1. Click Insight > Insight Access Tokens
2. Click Create a token
3. In the wizard, enter a name for the new token.
4. The token will now be displayed. Click Copy to copy the token into the clipboard.
5. Click Close to close the dialog.

Once the Token details dialog is closed, you won't be able to view the token again.

You can delete - or revoke - unneeded tokens.

Revoke a personal access token to make it unusable. This action cannot be undone.

1. Click Insight > Insight Access Tokens
2. Select the token to delete and click on the Delete icon.
3. In the dialog box, click on Revoke to revoke the token.

Use the personal access token as your Authorization when using the REST APIs. The domain for the API calls will be insight-api.riada.io, like the example below:

```
GET http://insight-api.riada.io/rest/insight/1.0/objectschema/list
Authorization: Bearer [enter personal access token here]
Content-Type: application/json
```

- REST API - IQL
- REST API - Objects
- REST API - Object type attributes
- REST API - Object types
- REST API - Object schema
- REST API - Object attachments
- REST API - Statuses
- REST API - Comments