1. **/v1/user/{**id}

* Username
* **Account\_info**: {

First\_name, last\_name,

Email, phone #,

Group\_name,

}

List\_of\_Project\_name,

List\_of\_devices

List\_of\_workflows

List\_of\_tokens

}

**Update**: change email, passwd,

**Result: verify user profile, updates**.

: get: check validity of user related information

: make sure log – in with user credential works. Log in can’t use token.

: update user information.

1. /devices/:deviceID

Devices related info and ops.

1. /projects/ New feature: project based resource sharing; **test-project management or test management**.

Idea: within a project, resources: devices, **tests**, workflows, reports can be shared/updated by users added to the project.

* During internal testing/customer feed back, noticed that user/credential with group to manage devices is not efficient when devices are shared
* Recommend add API team, which is project based.
* Team/projects, within a project or team, all users have same access rights to the devices, tests, and work\_flows.
* Project manager is created as superuser. Who can create a project, add users to the project, add resources/ devices etc.

1. Cross check /interconnect API call

Devices/deviceID 🡺 same device info as project/devices/deviceID

****

1. Token test

Focus on :

* https://stackoverflow.com/questions/42652695/is-it-ok-to-store-user-credentials-in-the-jwt

create a token, delete a token

how many token can a user have

token expiration time

JWT token carries username and group id to identify user.

Benefits of using JWT

How token carries info about scope (based on usr’s role)

## **Permissions**

https://support.atlassian.com/jira-cloud-administration/docs/manage-project-permissions/?permissionViolation=true

**Most operations in this API require permissions**. **The calling user must have the required permissions for an operation** to use it.

In user profile: there is a key: list of active projects:

Regular/project user can’t edit active projects endpoint. Only project\_admin can.

**Permission scheme is created by IT admin**. When users are created, their permission level is determined based on their **role**. When user create an account, need to get a one-time temp API key from IT first and use it when creating an account.

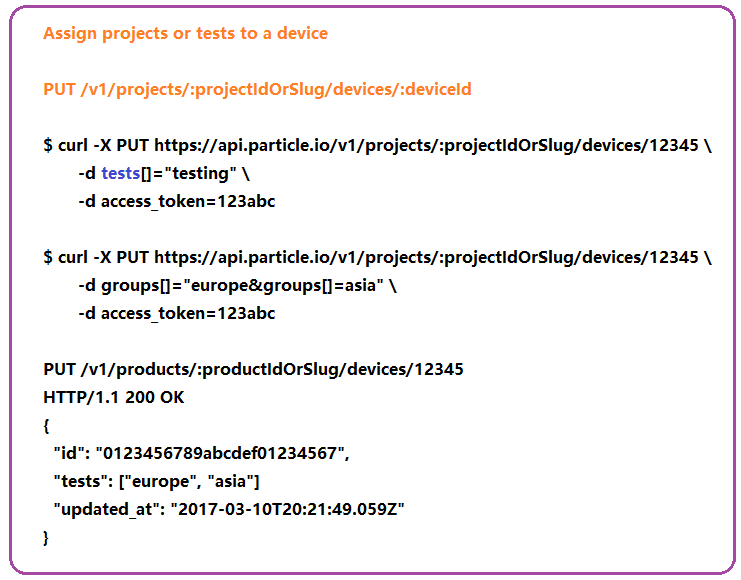
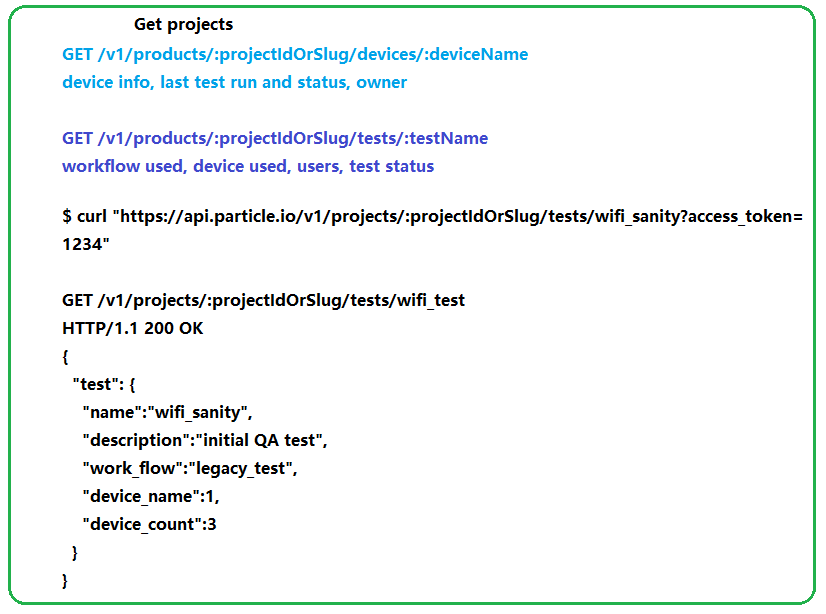
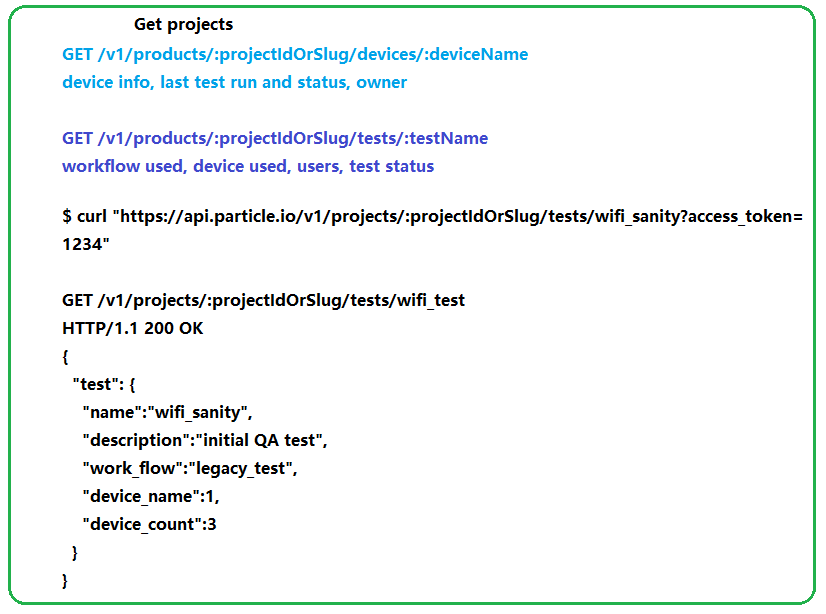
* Regular Users bounded to a group
* Super-users (project admin) (right across multiple groups)
* Project-user:
* One employee could have multiple level of permissions, depending on roles in projects
* Users and its associated token is determined by permission scheme depending on **user’s role** within the organization or group.

1. Error Checking of response
2. My API a little extra

API/v1/workflow

Api/v1/workflow/tech (wifi, bt, zigbee, uwb)

Api/v1/workflow/tech/wifi (11ac, abgn, ax, 11be)

****

1. Pagination, sort, order, search

* API offers
* Search
* Sort
* Filter/categorize
* Retrieve data with criterial
* Rate-limiting
* Pagination

1. 