1. Hitting the authorization endpoint – This will ask user to login and after successful login, we are redirected to redirect url. We get authorization code in query string.
2. Hitting the token endpoint –

Base64 encode the client\_id and client\_secret and attach other parameters including authorization\_code and send a post request to token endpoint. We receive the access\_token in json format.

1. Hitting the userinfo endpoint –

Use the access token and send a get request to userinfo endpoint. It will return the userid, name and email (what we have asked in scope)

#SSO For Admin console

Dynamic parameters

authorization\_url = https://qcwa.honeywell.com/as/authorization.oauth2?

token\_url = https://qcwa.honeywell.com/as/token.oauth2

userinfo\_url = https://qcwa.honeywell.com/idp/userinfo.openid

client\_id = Client\_10000

client\_secret=12345@key

scope=openid+profile+email

response\_type=code

redirect\_uri=https://qvpa.honeywell.com/hrdirectaccess/adminLoginIdEmp.htm

grant\_type=authorization\_code