Step- 1: request client

* 1. First, create an OAuth2.0 client in Policy Management Tool (PMT) for your application : <https://wampmtui.cloudapps.cisco.com/loggedIn#/oauth/clients/0/10>  
     Example: 'myApp-oidc-client'
  2. Select below two 'Authorization Grant Types' for your client.  
     Authorization code, Access Token validation.
  3. Set the client\_secret.
  4. Specify the redirect URI as per the OIDC client specifications. (This is a vanity URL that must ONLY point to a path on your server protected by this module, but it must NOT point to any actual content that needs to be served)  
     Example: <http://myapp.cisco.com/oauth2/callback>
  5. Select the Bypass Approval Page option.
  6. Select the life-cycle as NPRD for stage and PROD for production.

Step- 2: setup apache2

* 1. Install libjansson: wget <http://launchpadlibrarian.net/227040047/libjansson4_2.7-3_amd64.deb>
  2. Install libapache2-mod-auth-openidc: sudo apt-get install libapache2-mod-auth-openidc
  3. Enable module:   sudo a2enmod auth\_openidc
  4. Restart apache2: sudo service apache2 restart
  5. Config this file and add below under <VirualHost ….>: sudo vim /etc/apache2/sites-available/default-ssl.conf

LoadModule auth\_openidc\_module modules/mod\_auth\_openidc.so

OIDCProviderMetadataURL <https://cloudsso.cisco.com/.well-known/openid-configuration>

OIDCRedirectURI <https://pcba-allocation.cisco.com/oauth2/callback>

OIDCCryptoPassphrase arandomsecret

OIDCClientID pcba-allocation-oidc-client

OIDCClientSecret 55eabeb17a5d48c0bd5aed1072436100

OIDCScope "openid profile email"

# Ken: Below line is causing apache2 start failure!!

#OIDCAuthRemoteUserClaim uid

#OIDCPassIDTokenAs payload

#OIDCPassClaimAs environment

#OIDCClaimPrefix USERINFO\_

<Location "/">

       Require valid-user

       AuthType openid-connect

</Location>

(<https://gluu.org/docs/gluu-server/3.1.1/integration/sswebapps/openidc-rp/>)