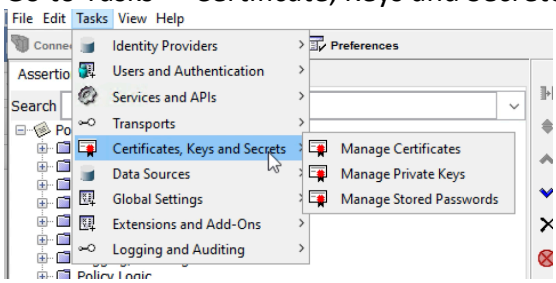
CA SSO and CA APIM Integration Guide Part 2

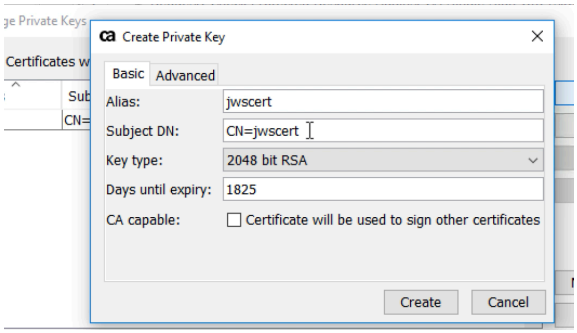
Version: CA SSO R12.8 SP1, CA API Gateway 9.3, Tool kit 4.2

CA SSO configuration – Integration with JWT Authentication

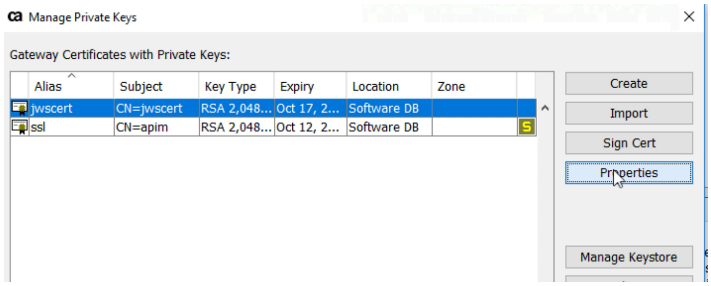
1. **Create Private Key for JWT token Signing in APIM Gateway**
    - Login APIM Policy Manager
    - Go to Tasks -> Certificate, Keys and Secretes -> Manage Private Keys



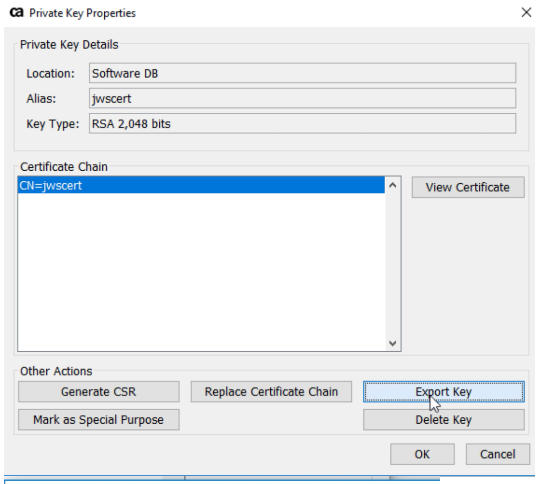
    - Create new Private Key. In Alias, input “jwscert”. Then, click “Create” button

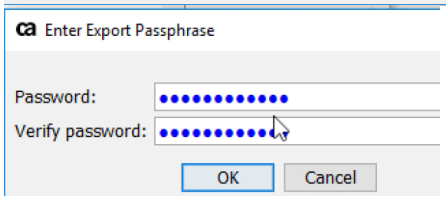


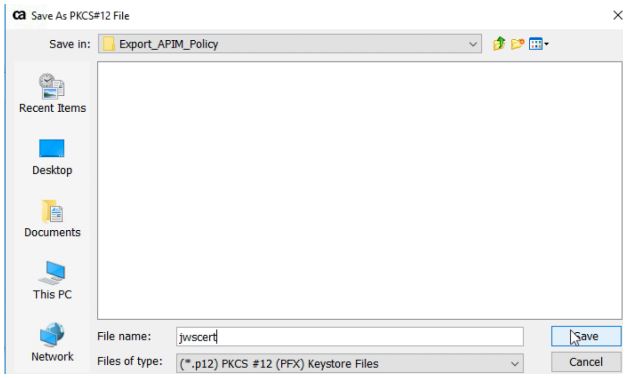
    - After creating, select newly created key (jwscert) and double click “properties”.



    - Click “Export Key” and input the password. (Any password) Then save the exported key file with p12 format.

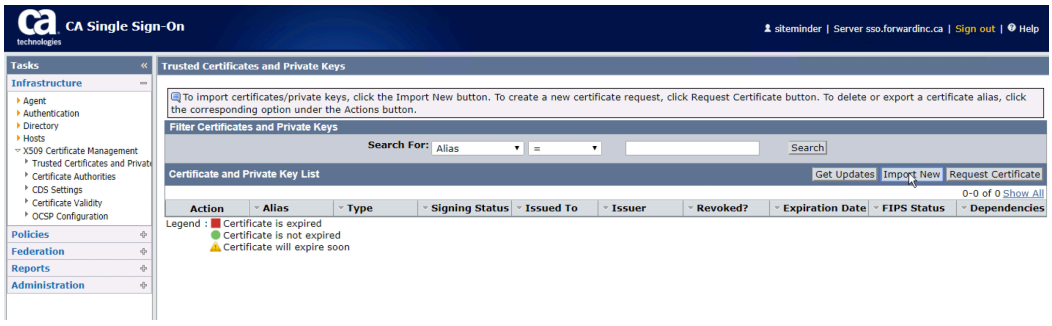






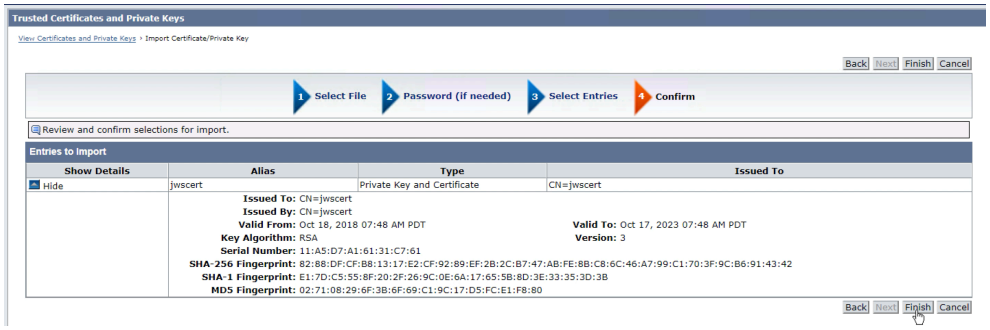
2. **Create JWT Authentication Scheme in CA SSO**

- Login CA SSO Admin UI and go to Infrastructure -> X509 Certificate Management -> Trusted Certificates and Private Key. Then, click “Import New”

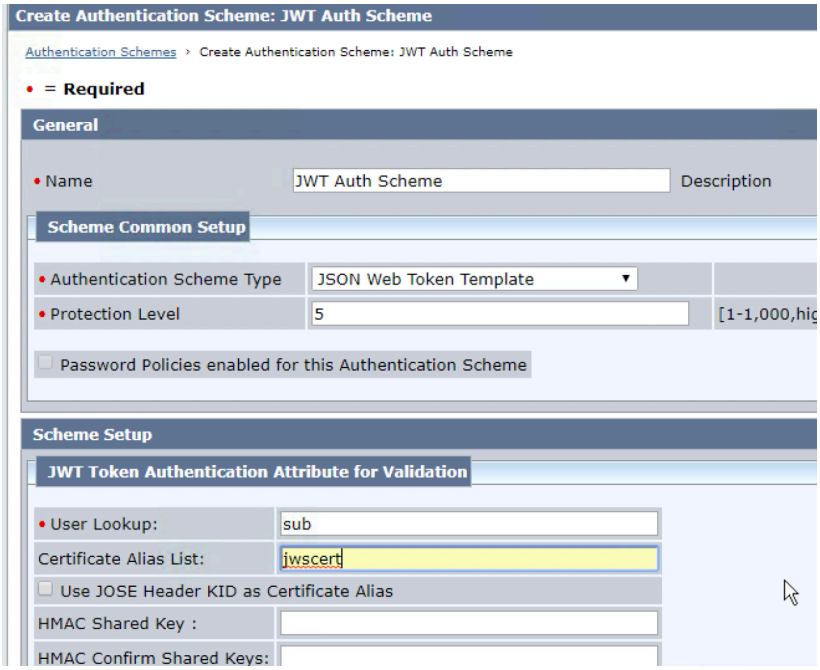


- Import certificate, which is exported from API Gateway(jwscert). Then, input the password.

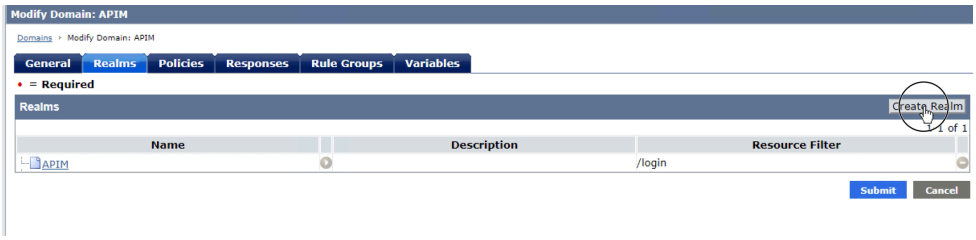
- After verify the certificate, click “Finish” button.



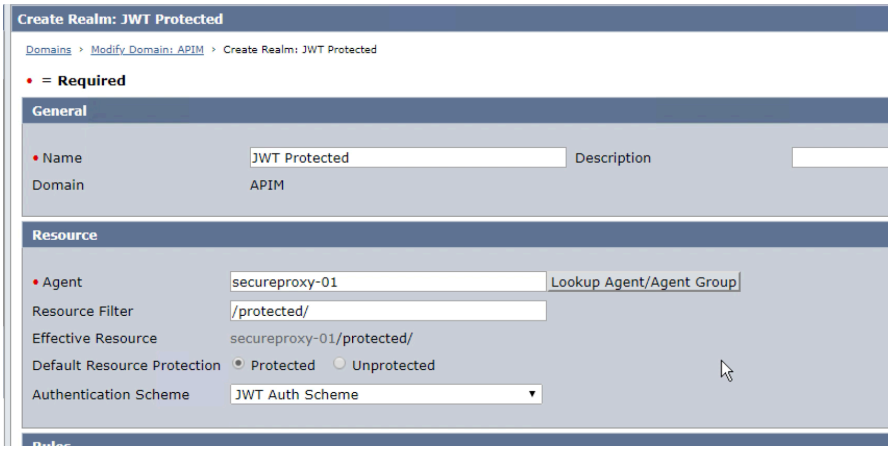
- Go to Infrastructure -> Authentication -> Authentication Scheme -> Create Authentication scheme.
    - Name : JWT Auth Scheme
    - Authentication Scheme Type: JSON Web Token Template
    - User Lookup : sub
    - Certificate Alias List: jwscert



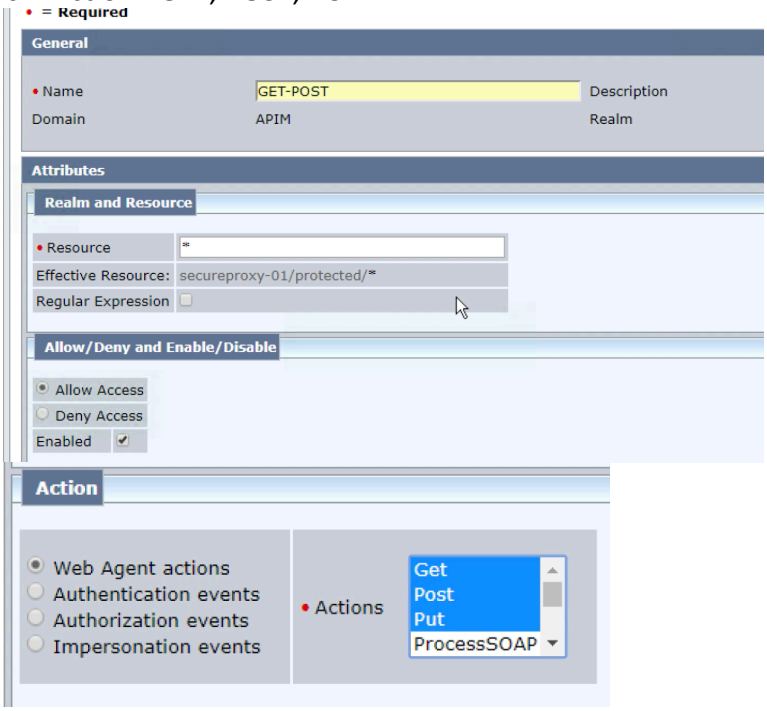
- Go to APIM Domain (which is created in part 1) and click modify button. Go to Realms and click “Create Realm”.



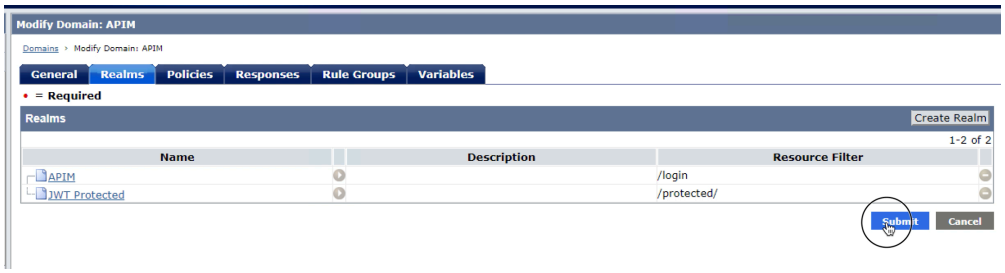
- Create new Realm
  - Name : JWT Protected
  - Agent: secureproxy-01
  - Resource Filter : /protected/
  - Authentication Scheme : JWT Auth Scheme



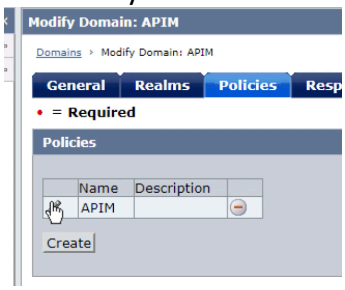
- Create Rule
  - Name : GET-POST
  - Resource : *
  - Action : GET, POST, PUT



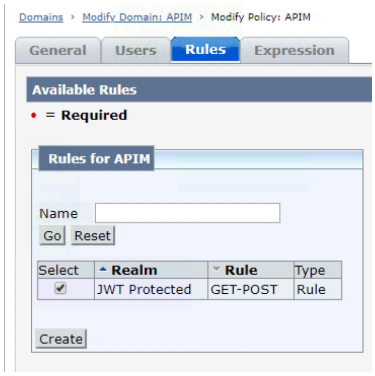
- Click “OK” button and Submit



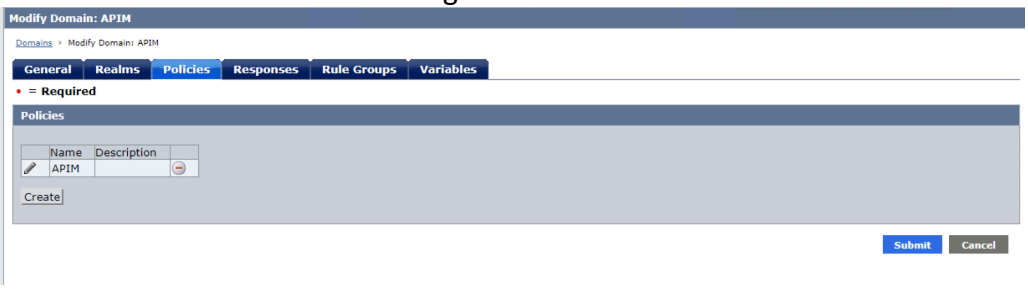
- Go to APIM Domain again and click modify button again. Then, go to policies tab. In policies, click APIM modify.



- In policies, go to Rule tab and click “Add rule” button. Then, select JWT Protected Realm

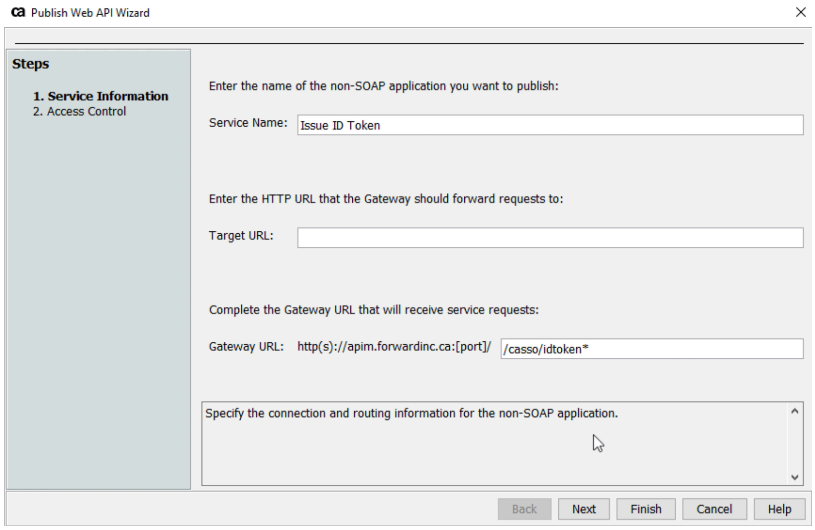


- Click OK button and click Submit Button again.



3. Create JWT Assertion in APIM Policy Manager

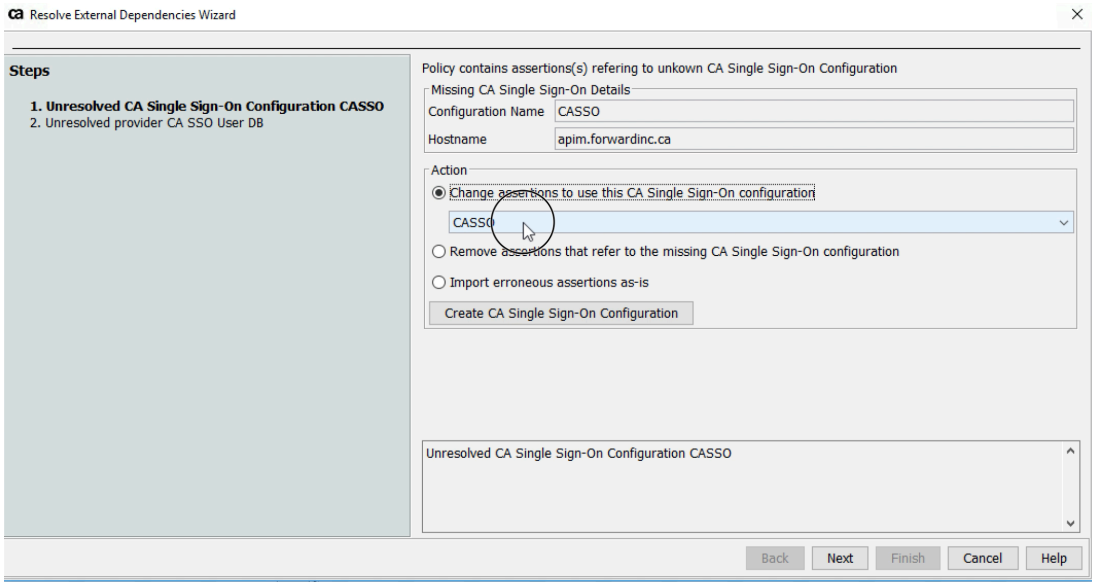
- Login API Gateway Policy Manager and create “Publish Web API”
  Service Name : Issue ID Token
  Gateway URL: /casso/idtoken*



Then, click “Finish” button

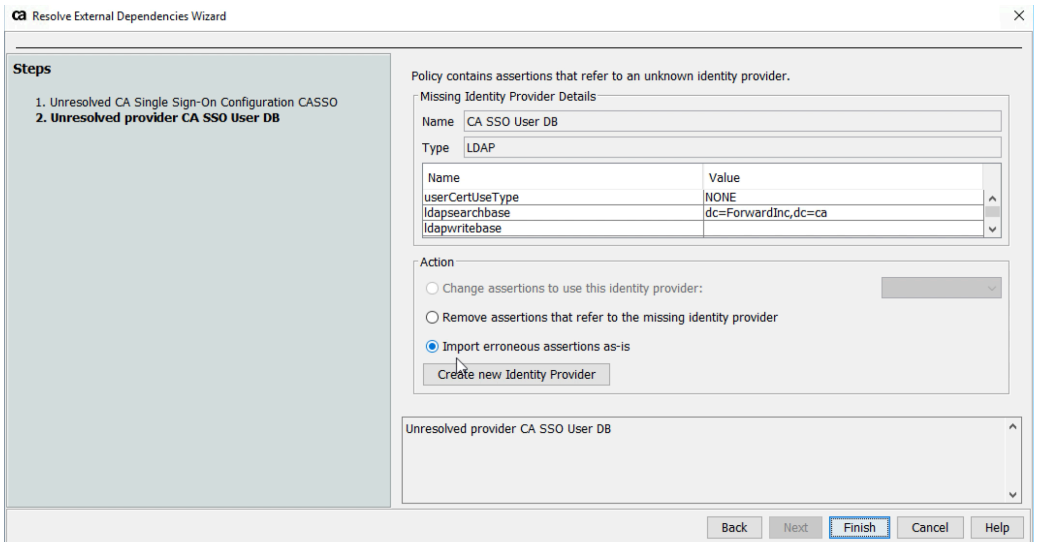
- Click “Import Policy” and select “Issue ID Token (JWT).xml” file.

- It shows Resolve External Dependencies Wizard. For CA SSO, please select “Change assertions to use this CA Single Sign-On configuration. “CA SSO”. (It is CA SSO configuration, which is created in part 1.)

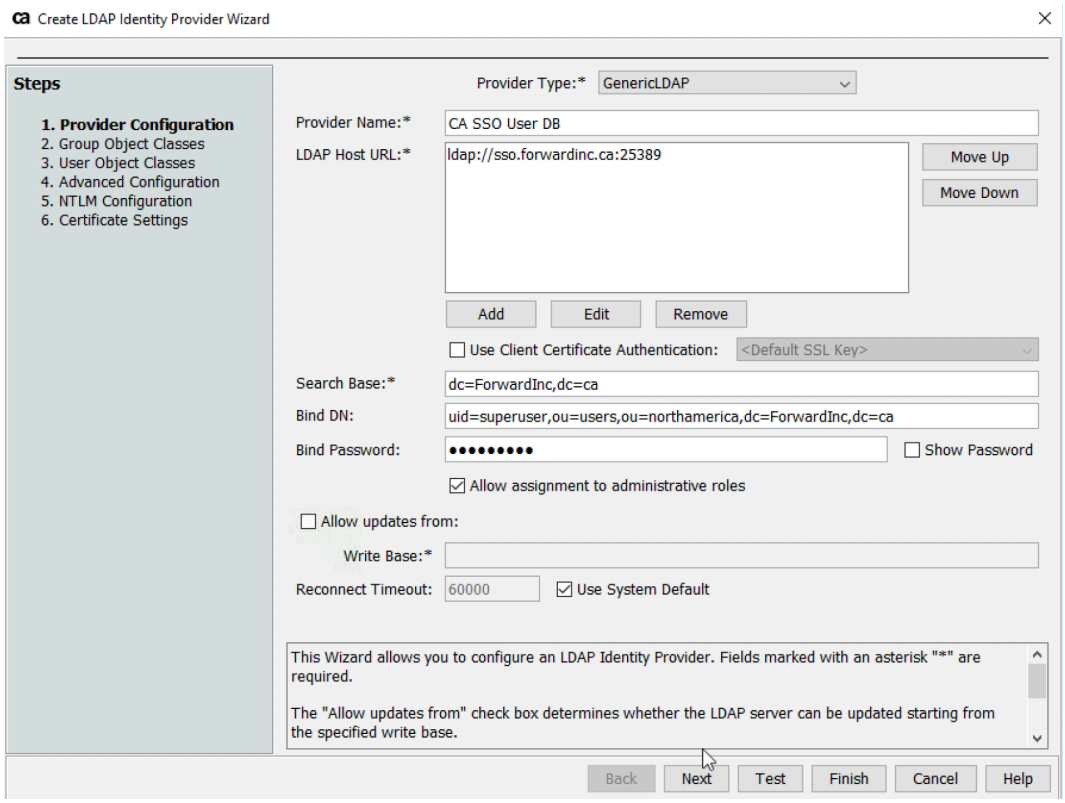


Then, click next

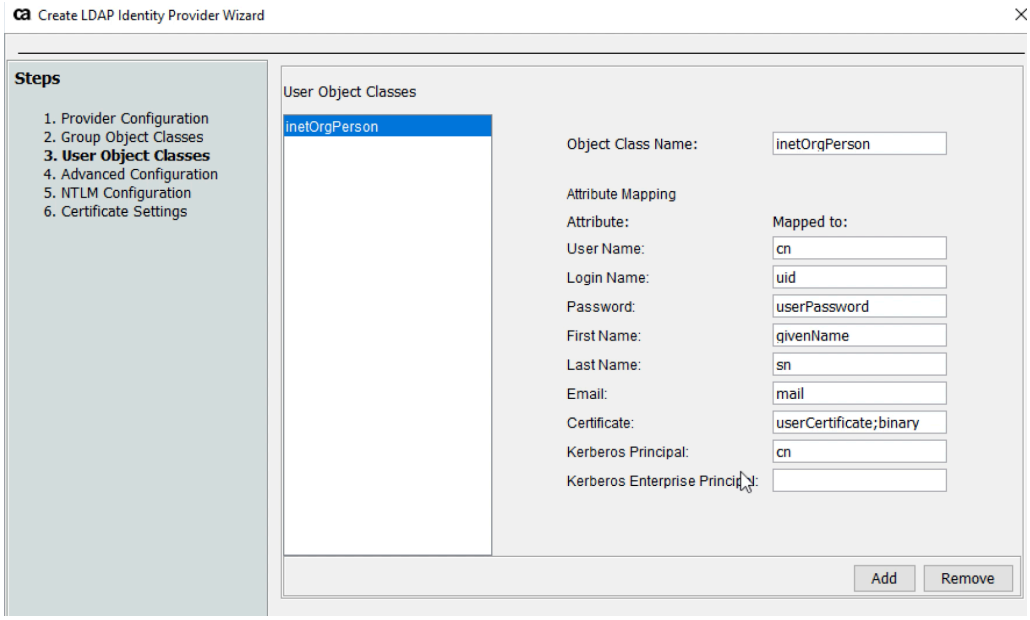
- In Wizard, select Import erroneous assertion as-is. “Create New Identity Provider”. It will connect CA SSO User Directory.



- It shows “Create LDAP Identity Provider Wizard” and input correct Bind Password. (CAdemo123). Using “Test” button, please verify the connection. Depending on the environment, LDAP Host file and other information can be changed.

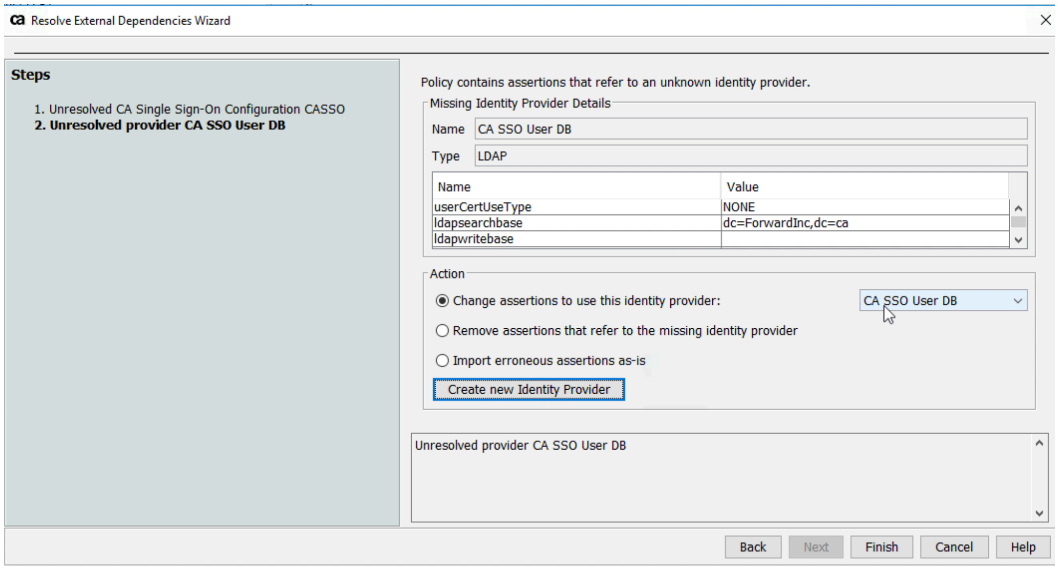


- Then, click “Next” continually. In User Object classes screen, please verify the Login Name. In CA LDAP, default Login Name should be “uid”. When you are using other user directory, it can be different.



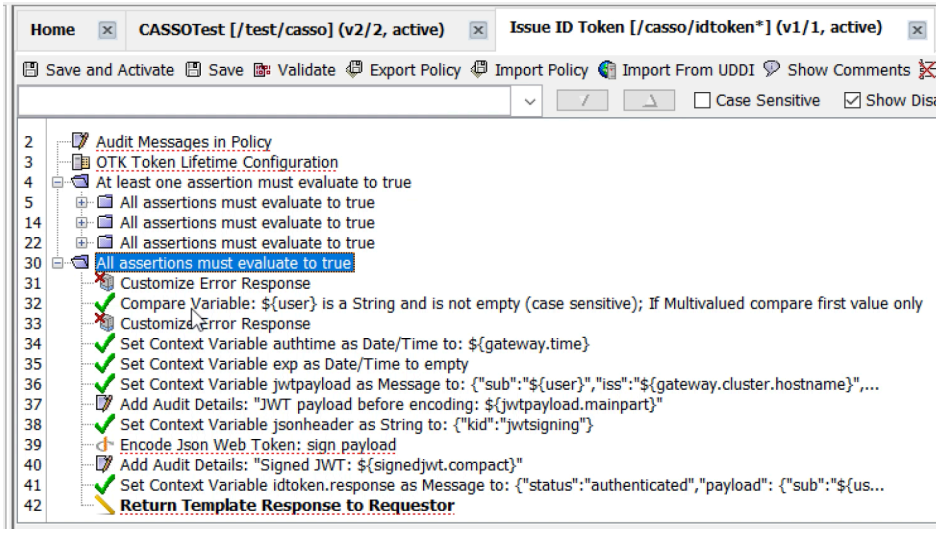
Then, click Finish button.

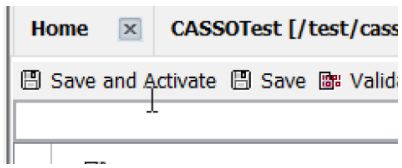
- In Resolve External Dependencies Wizard, please select “CA SSO User DB” in Action.



Then, click “Finish” button.

- Then, you can see the imported policies in UI. Click “Save and Activate” icon in UI.



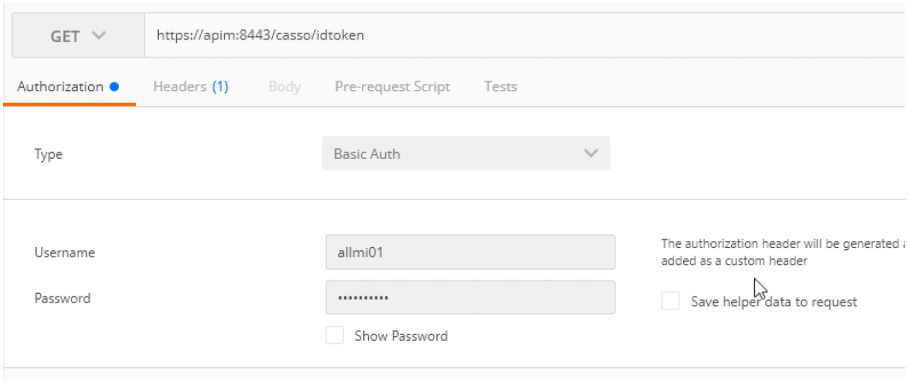


- It shows Resolve External Dependencies Wizard. For CA SSO, please select “Change assertions to use this CA Single Sign-On configuration. “CA SSO”.

4. Test CA SSO and CA API Gateway Integration

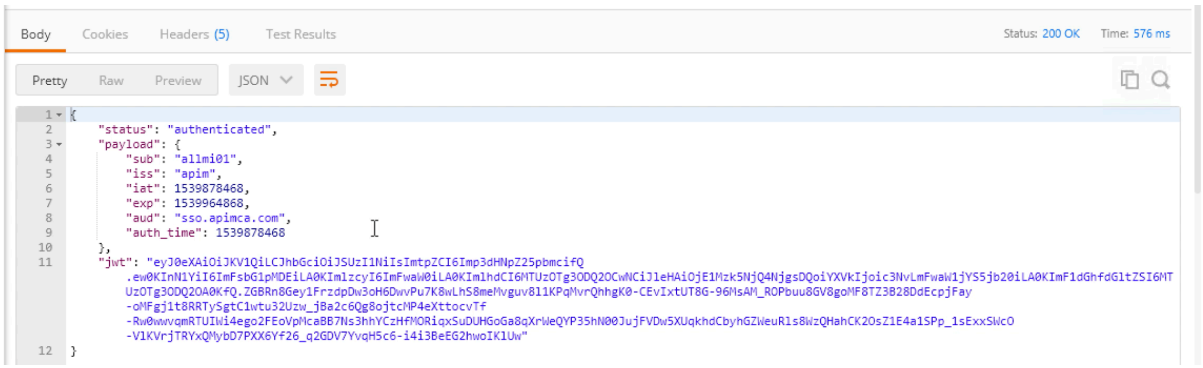
- Download PostMan (REST API Client) and execute it.

- In Postman, input the following information.
  - Method: GET
  - URL : https:// <API GW FQDN>:8443/casso/idtoken
  - User name: allmi01
  - Password: P@ssword01

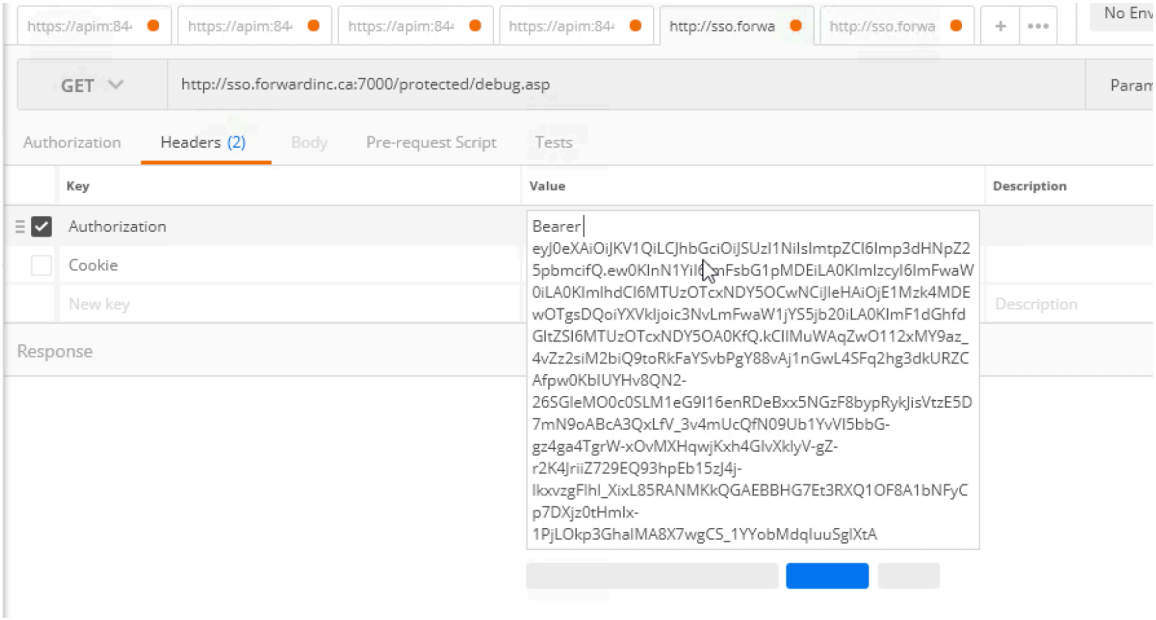


Then, click “Send” button.

- After successful authentication in API Gateway, it returns JWT token.

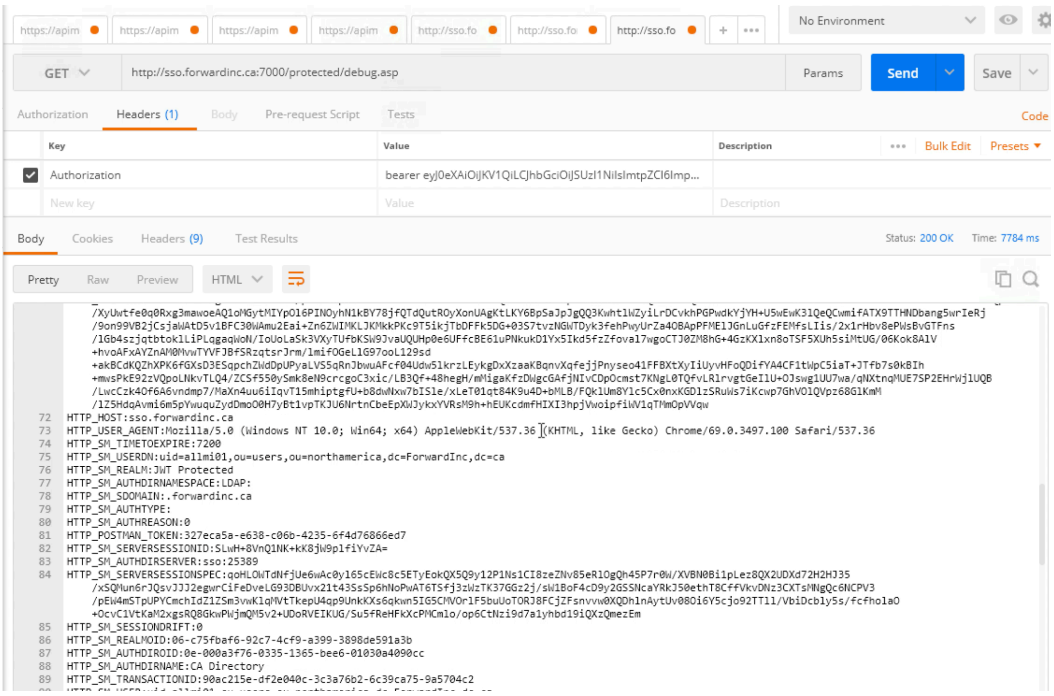


- After coping JWT toke and sends it to CA SSO protected web page. In Postman client, please input the following information.
  - Method: GET
  - URL : http//<Access Gateway FQDN>:7000/protected/debug.asp (Instead of debug.asp, any page can be used as long as it is existed in backed.)
  - Header : Authorization
  - Value : Bearer <JWT value> (There is space between Bearer and <JWT value>).



Click “Send” button

- It shows backend result after JWT Authentication.



- After closing Postman client and execute again. It requests to access the resource, which is protected JWT token without providing any token value. It rejects the request.