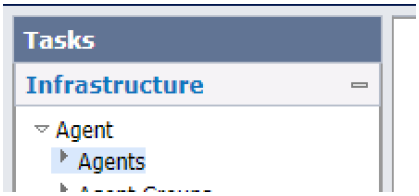
CA SSO and CA APIM Integration Guide

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

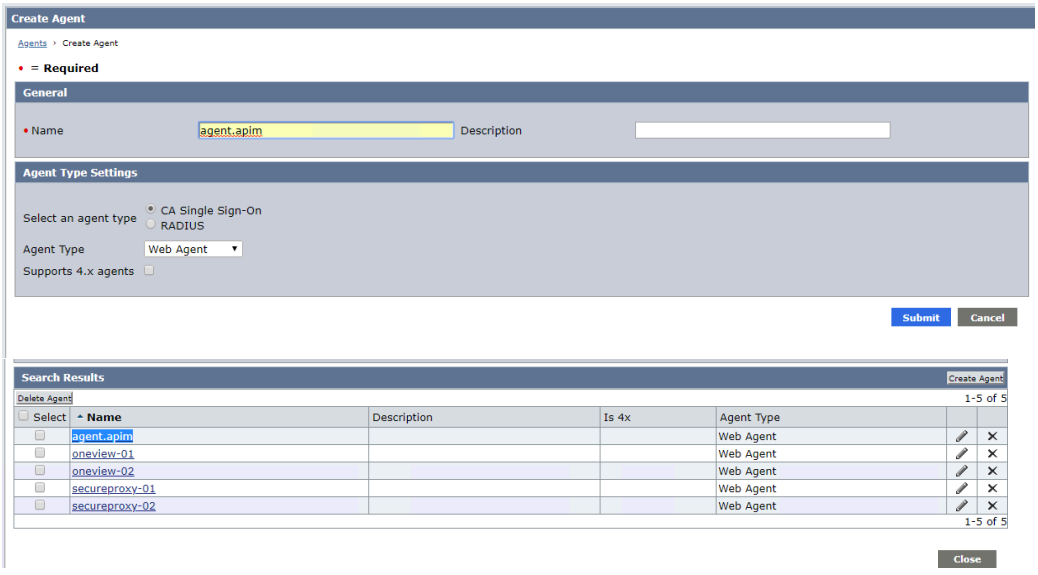
CA SSO configuration – Simple Integration with Basic Authentication

1. **Crate "Agent" and "Host Configuration Object" to communicate with CA APIM Gateway and CA SSO**
   - Login CA SSO Admin UI
   - Go to Infrastructure -> Agent-> Agent



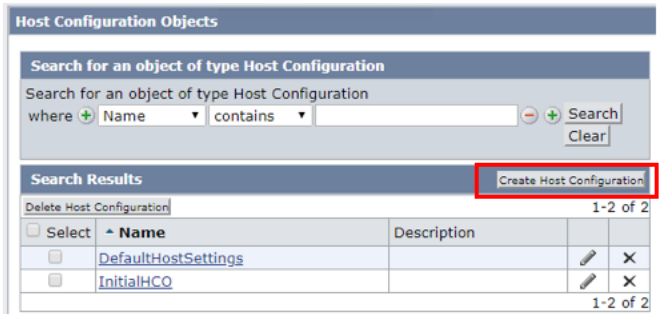
   - Click "Create Agent" button and select "create new object type of agent"

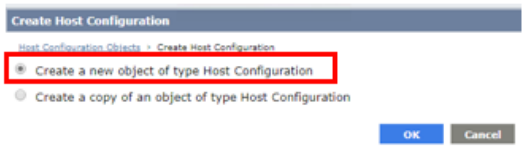
   - Input Agent name as "agent.apim" and click "Submit" button



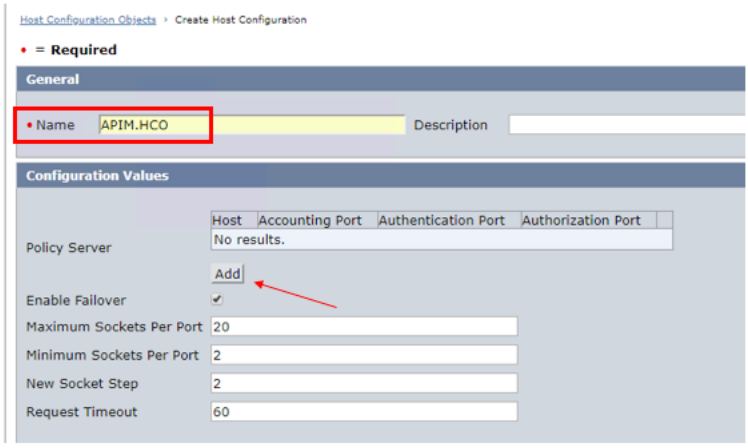
   - Go to Infra Structure -> Hosts -> Host Configuration Object in CA SSO Admin UI

- Click “Create Host Configuration” button

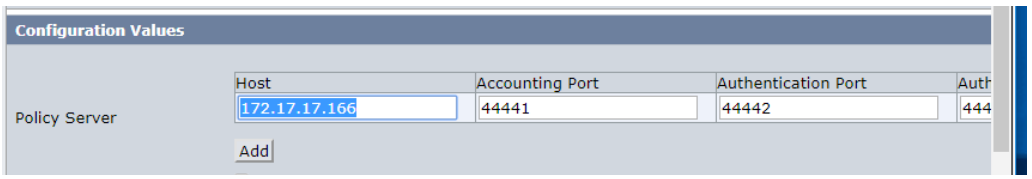




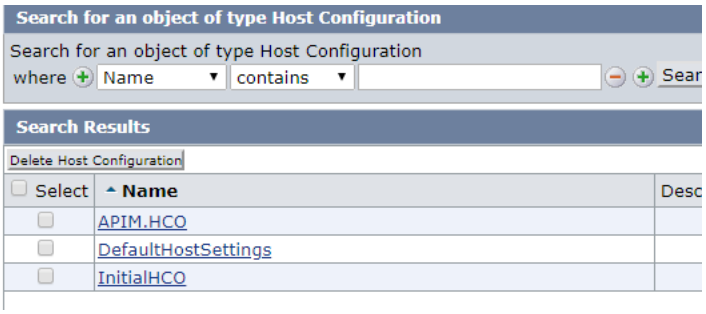
- Input Name and click “Add” button



- Input CA SSO Policy Server IP Address or Host name. (Host name can be resolved from APIM Gateway.)

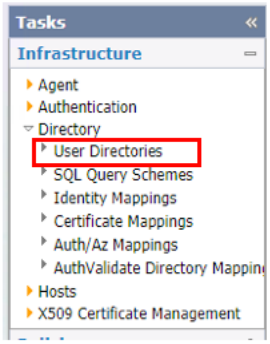


- Click “Submit” button

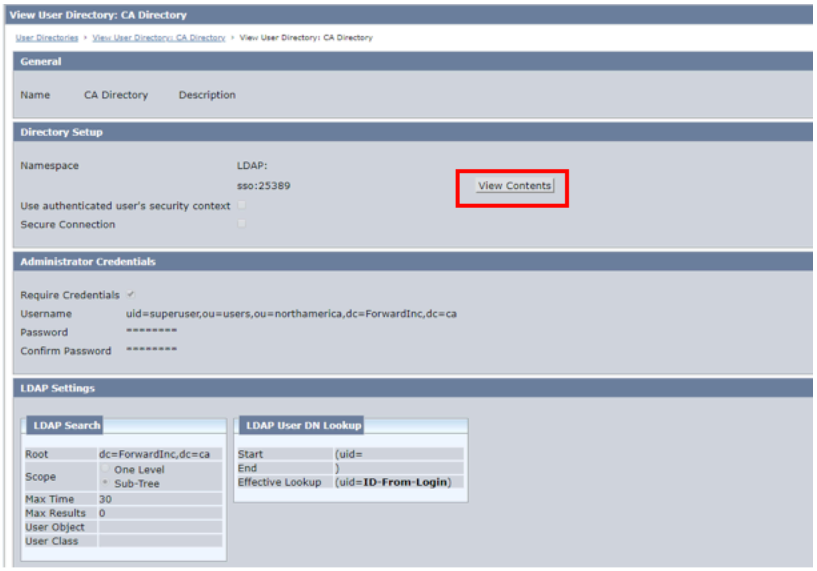


2. User Directory Check

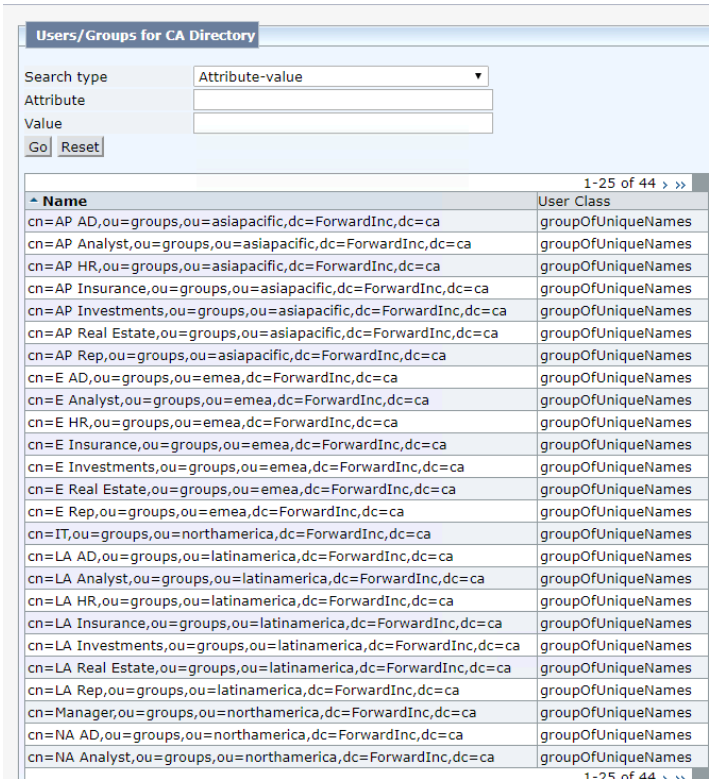
- In CA SSO Admin UI, go to Infrastructure -> Directory- > User Directory



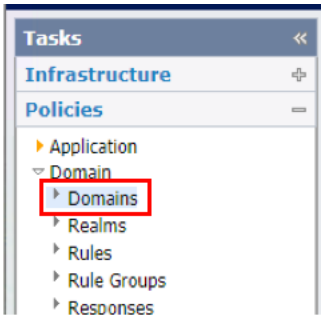
- Click “CA Directory” . (If there is no CA Directory, please create CA Directory.)
- Click “View Content” button



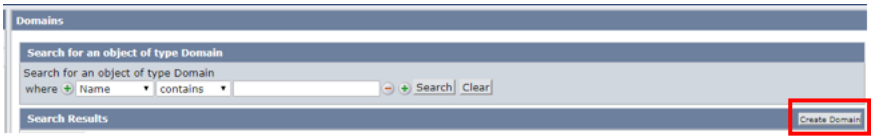
- Verify the result. (When it shows any error message, please check CA Directory service status and validate the configuration.)



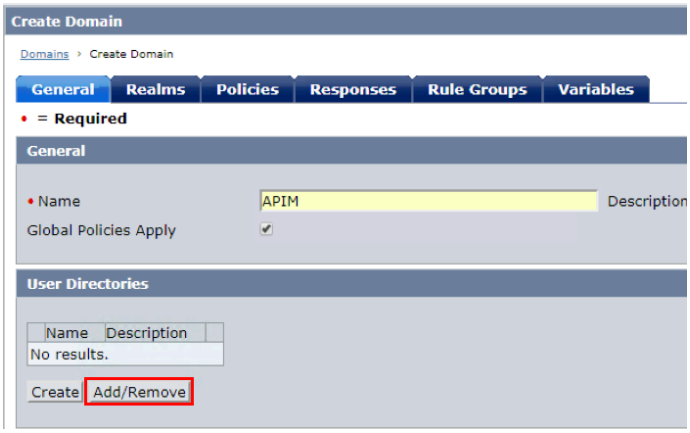
3. **Create Domain/Application in CA SSO Admin UI (Instead of Domain, Application can be created.)**
    - **Go to Policies -> Domain -> Domain**



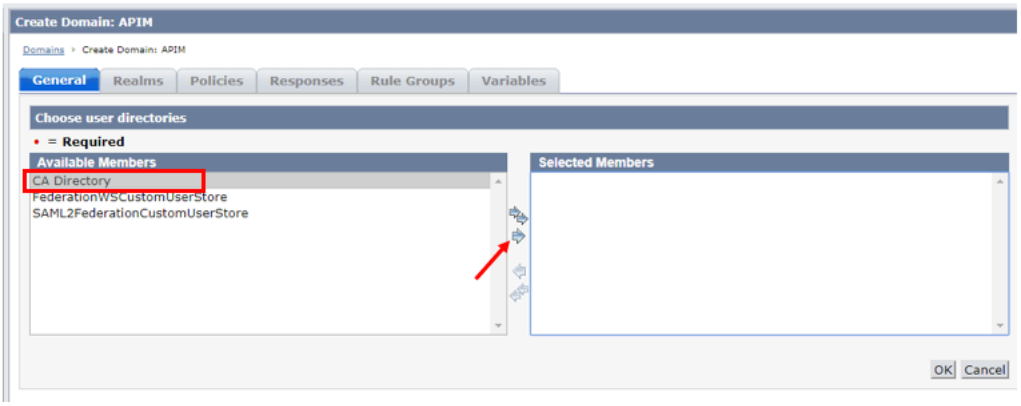
    - Click “Create Domain” button



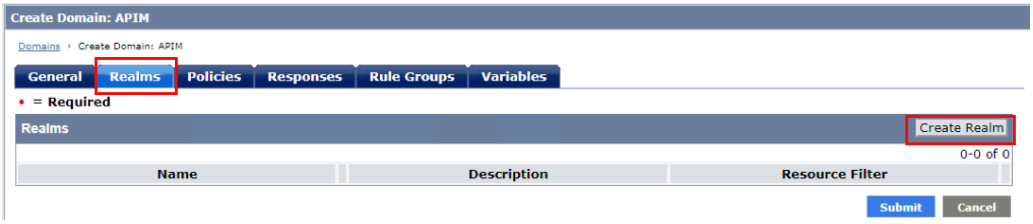
    - Input Name and click “Add/Remove” button in User Directories



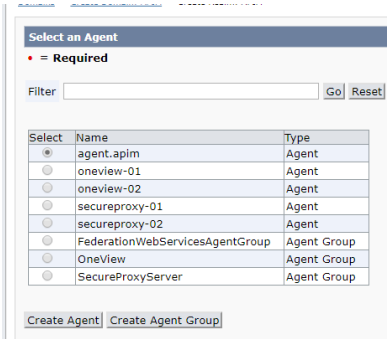
- Select “CA Directory” and click right arrow button. Then, click “OK” button



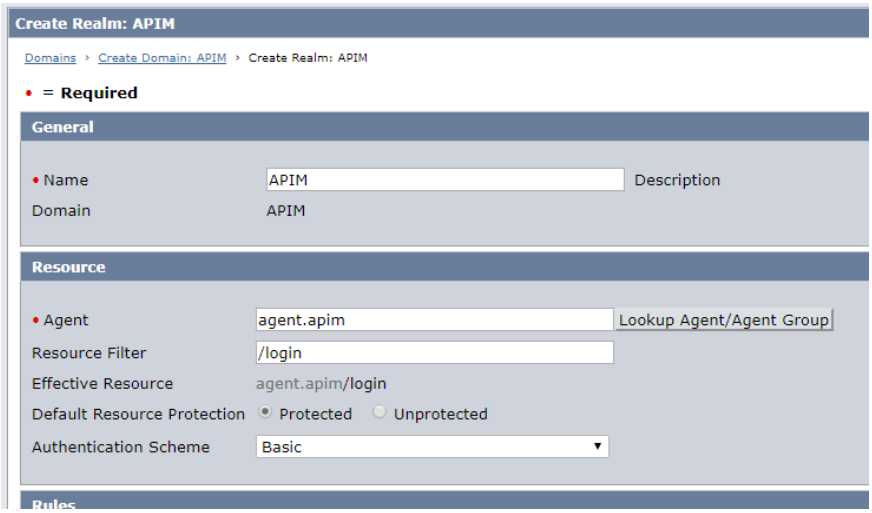
- Click “Realms” tab and click “Create Realm” button



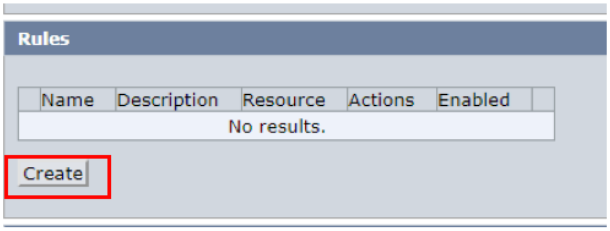
- Input the following information
  - Name: APIM
  - Agent Name: agent.apim (click lookup agent/agentGroup and select agent.apim)



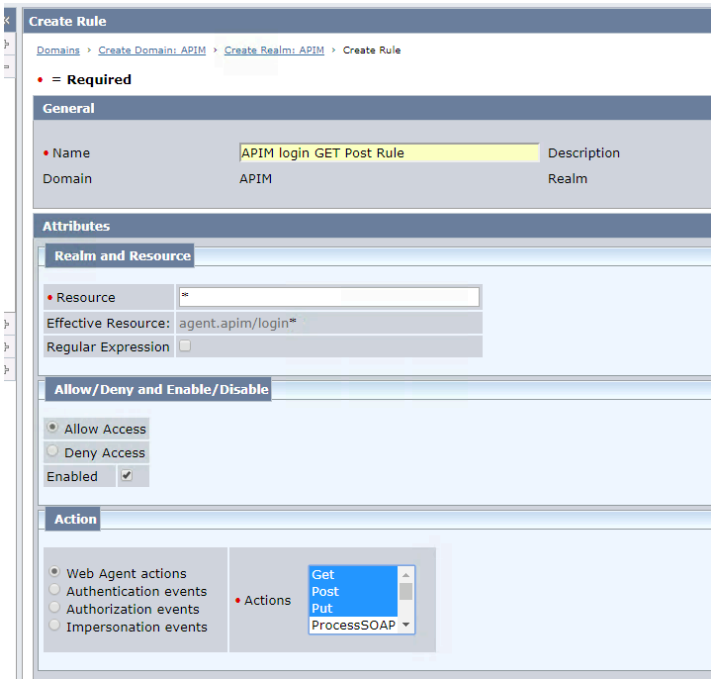
  - Resource Filter: /login
  - Authentication Scheme : Basic



- Rules section, click “Create” button

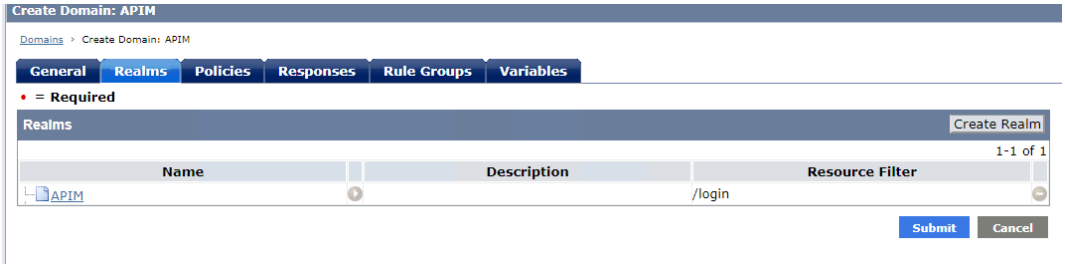


- Input the following information
  - Name: APIM login GET Post Rule
  - Resource: *
  - Action
    - Select “Get”, “POST” and “PUT”

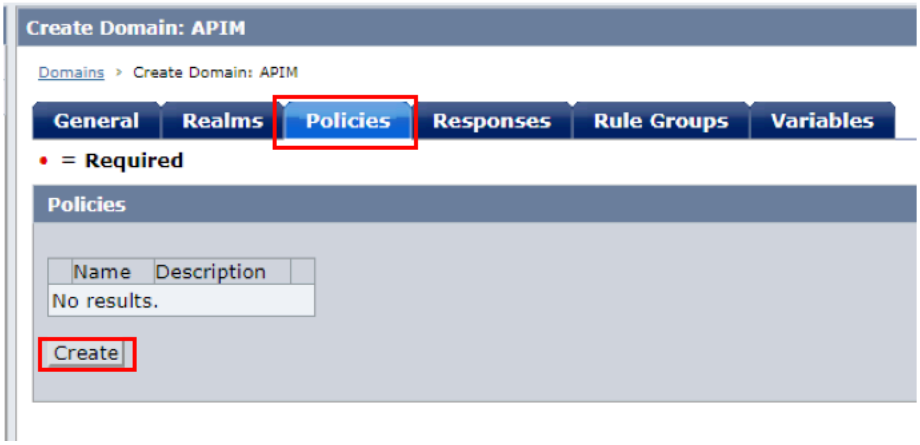


- Click “OK” button and exit rule setting

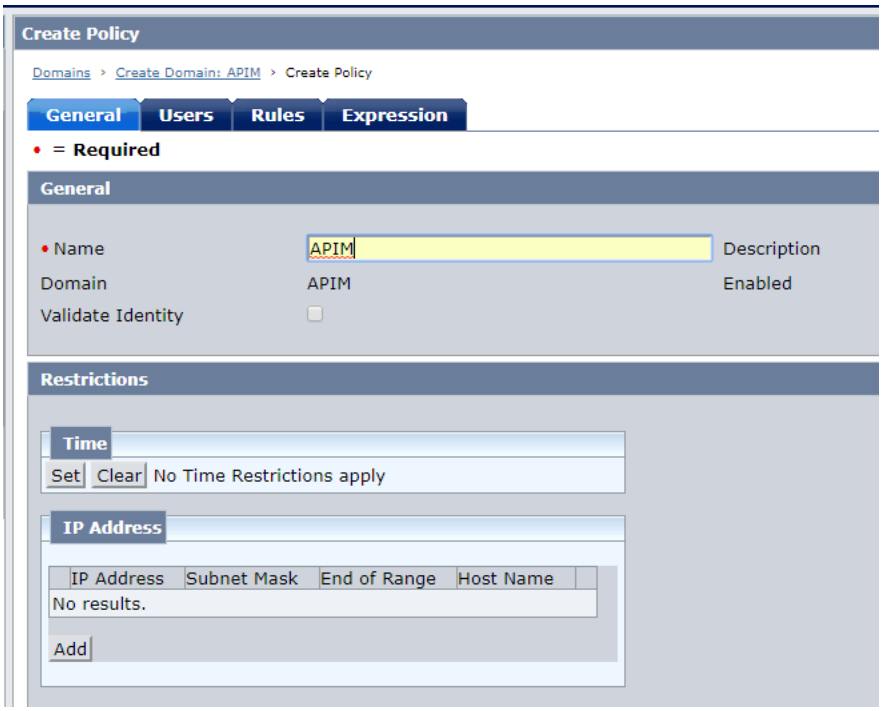
- Click “OK” button and exit Realm setting



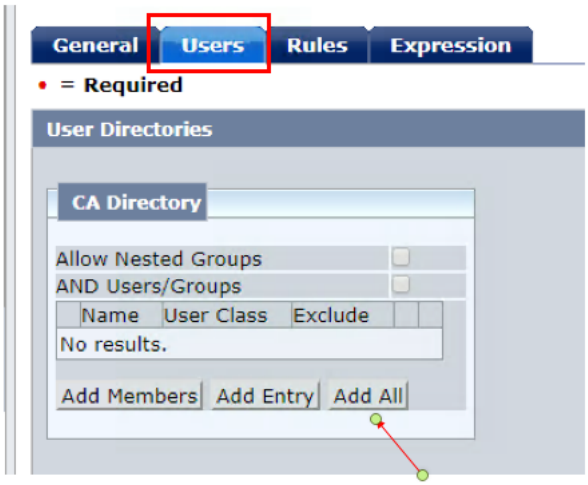
- Click Policies tab and click “Create” button



  - In General tab, input name “APIM”

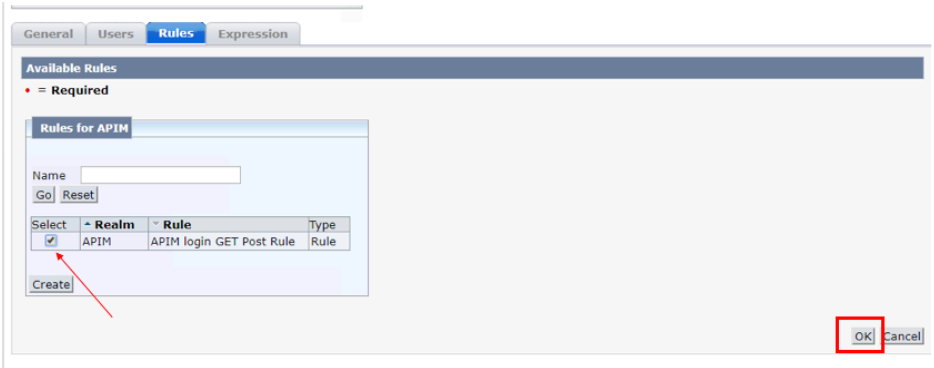


  - In Users tab, click “Add All” button. (it means that every users in user DB can access the resource.)

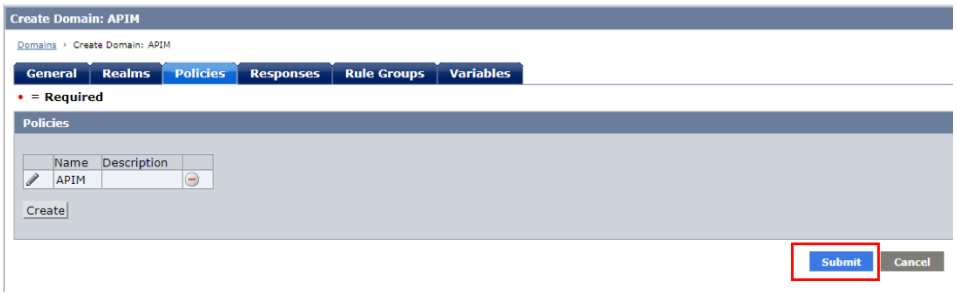


- In Rules tabl, please click “Add Rule” button

- Click “Select” box and click “OK” button

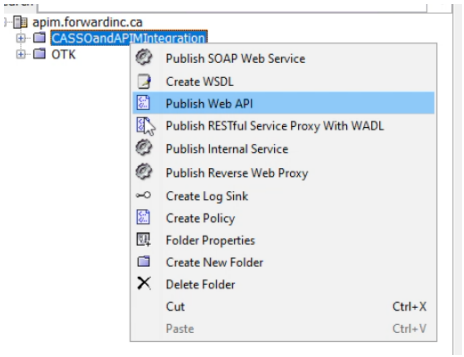


- Click “OK” button and exit Policies tab.
- Click “Submit” button to save the domain


Create Domain: APIM
Domains › Create Domain: APIM
General
Realms
Policies
Responses
Rule Groups
Variables
• = Required
Policies
Name
Description
APIM
Create
Submit
Cancel

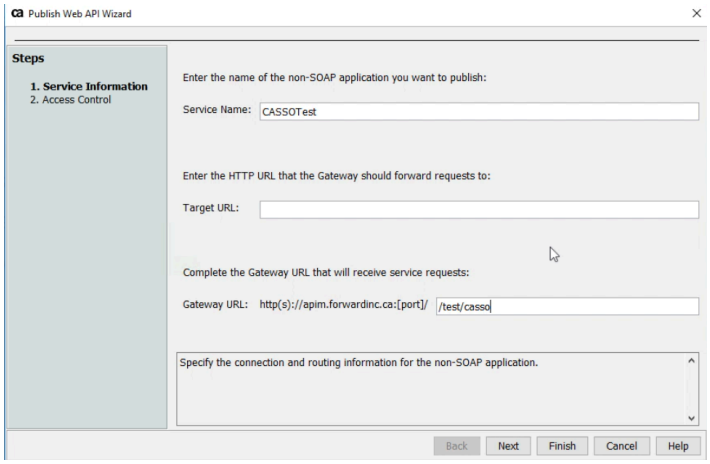
CA APIM configuration – Simple Integration with CA SSO SDK

1. **Create New Web API for CA SSO Integration**
    - **Login into CA APIM Policy Manager and publish web API**

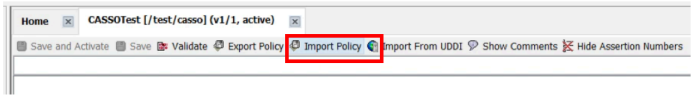


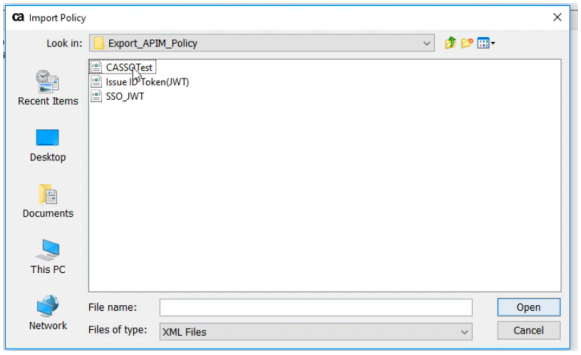
    - **Input Service information and click "Finish" button**

      Service Name : CASSOTest
      Gateway URL: /test/casso

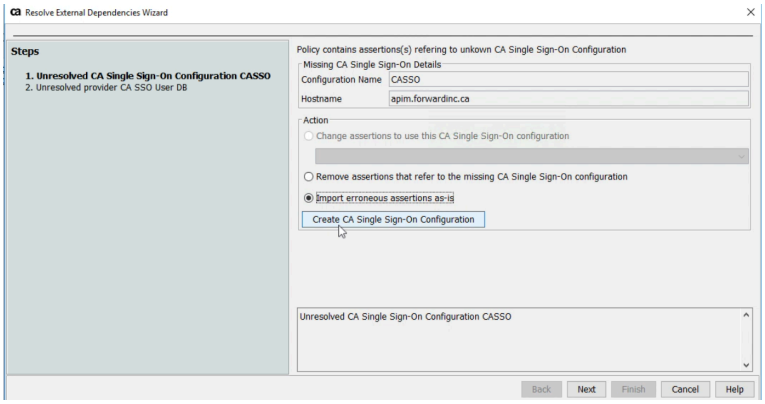


    - **Import "CASSOTest" policy, which is download from the site. (CASSOTest.xml)**

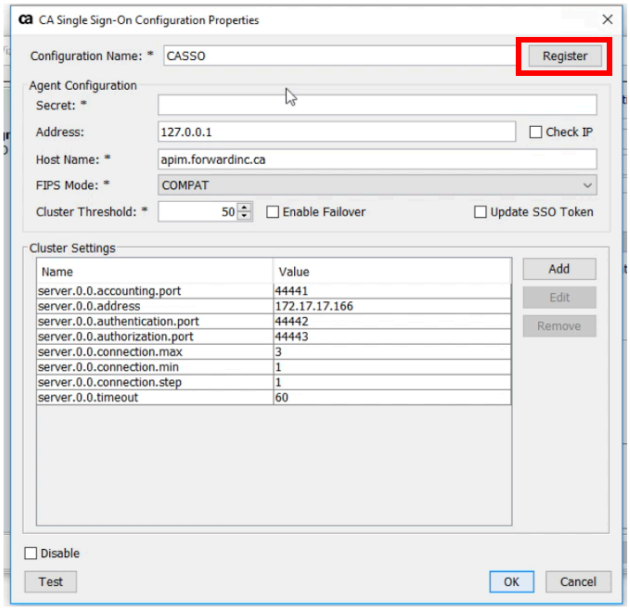




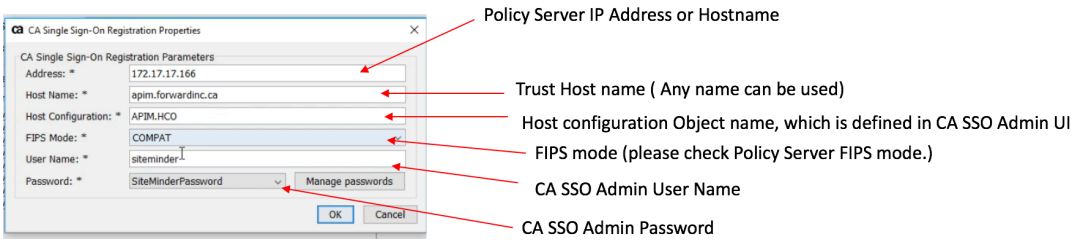
- **Pop up “Resolve External Dependency Wizard” windows and select “Import erroneous assertion as-is”. Then, click “Create CA Single Sign-On Configuration”.**

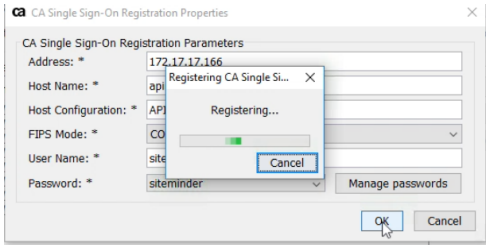


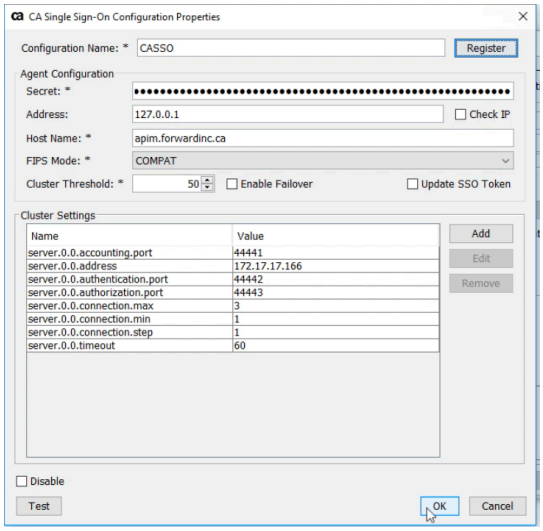
- **CA Single Sign-on Configuration properties windows pop up. Then, click “Register” button**



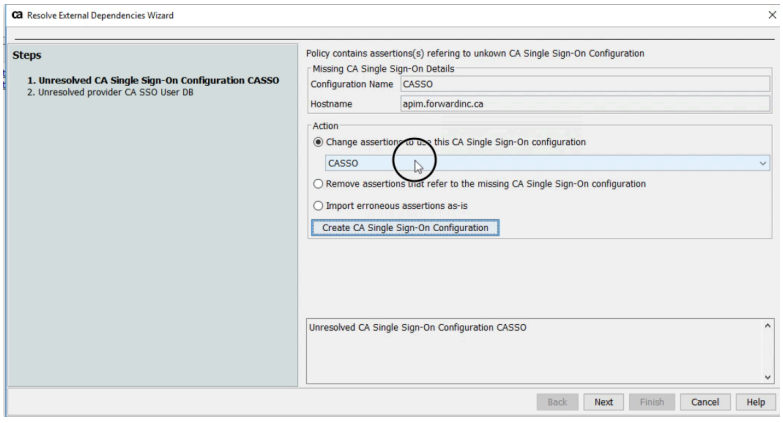
- **Provide CA SSO connection related information in UI and click “OK” button**



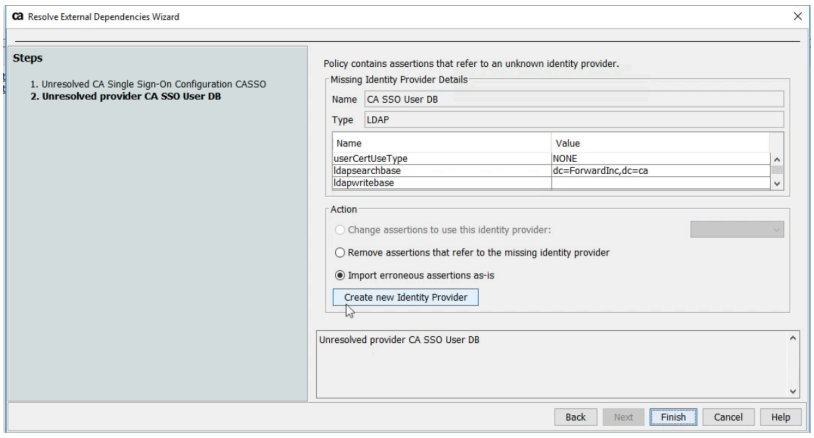




- **Select “Change assertion to use this CA Single Sign-on configuration”. Then, click “Next” button**

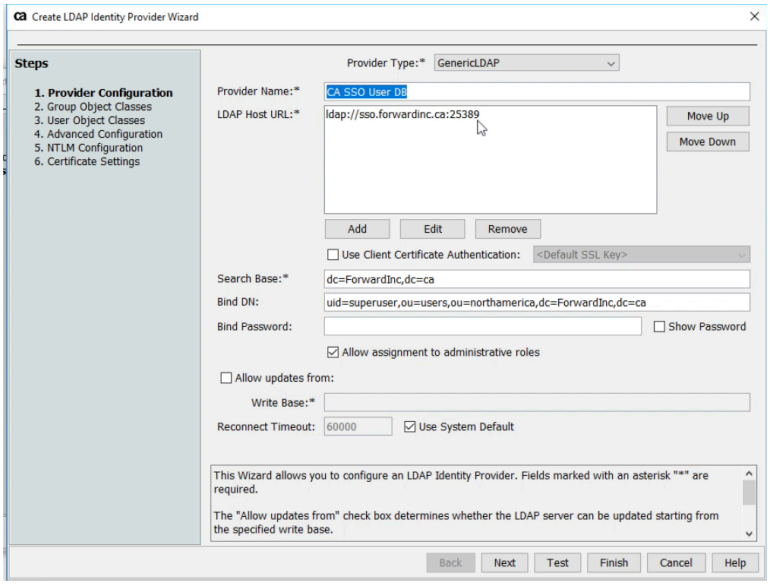


- **Unresolved provider CA SSO User DB. Select “Import erroneous assertion as-is” and click “Create new Identity Provider”**

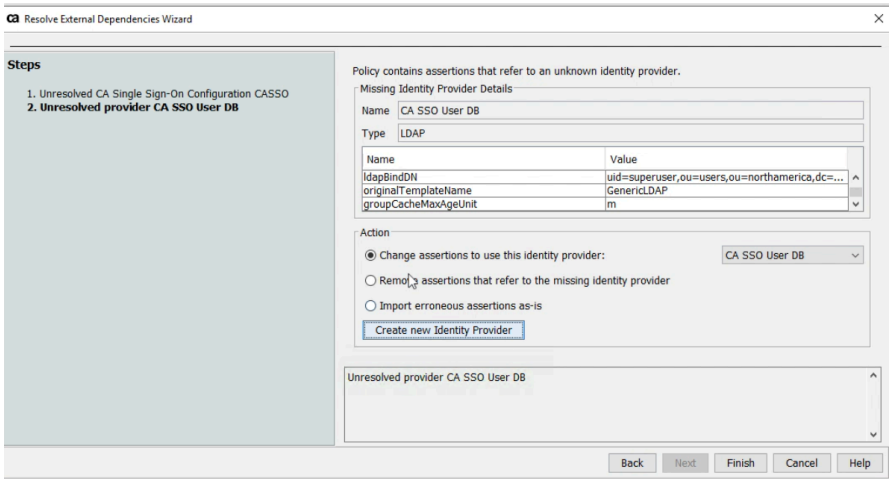


- **Change LDAP Identity Provider Wizard based on user directory in CA SSO. You can find the in detail connection information from CA SSO User Directory.**

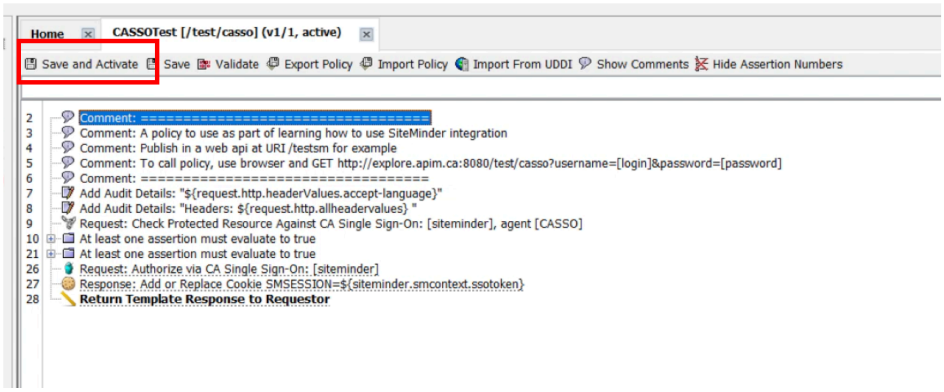
  In this example, superuser password is “CAdemo123”. After creating LDAP Identity Provider, check the connection with “Test” button.
  Click “Next” button and accept the default setting.



- **In Action panel, select “Change Assertion to use this Identity Provider : CA SSO User DB”. Then, click “Finish” button.**



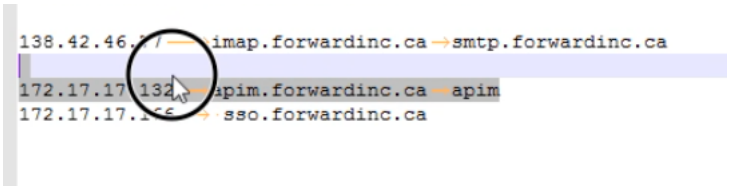
- **When it shows imported assertions in the UI, please click "Save and Activate" icon.**



Now, CA APIM is ready for testing !!!!.

Optional.

When you are using private IP address in APIM and CA SSO. Please change hosts (client) side to connect CA APIM and CA SSO with FQDN.



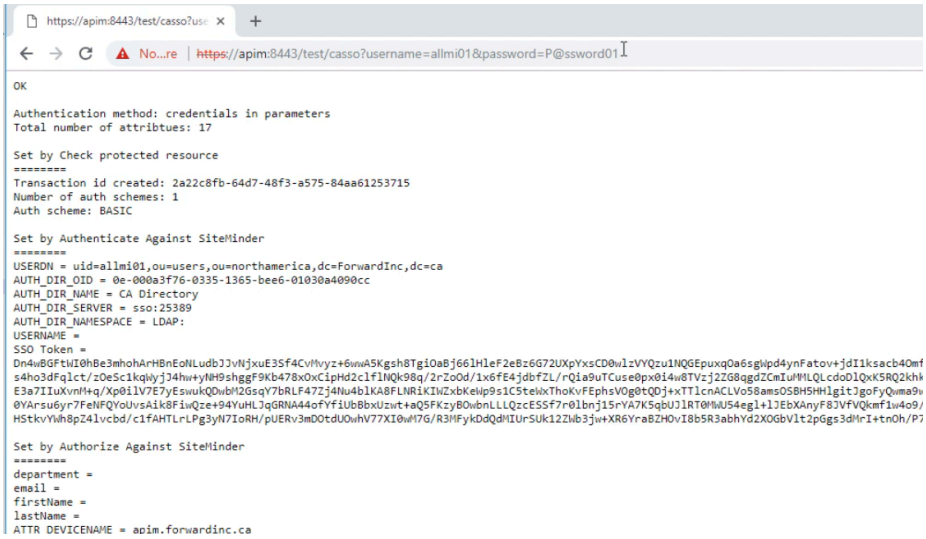
Test 1.

In browser, type https://apim:8443/test/casso.

It shows kind of waning message with guide.

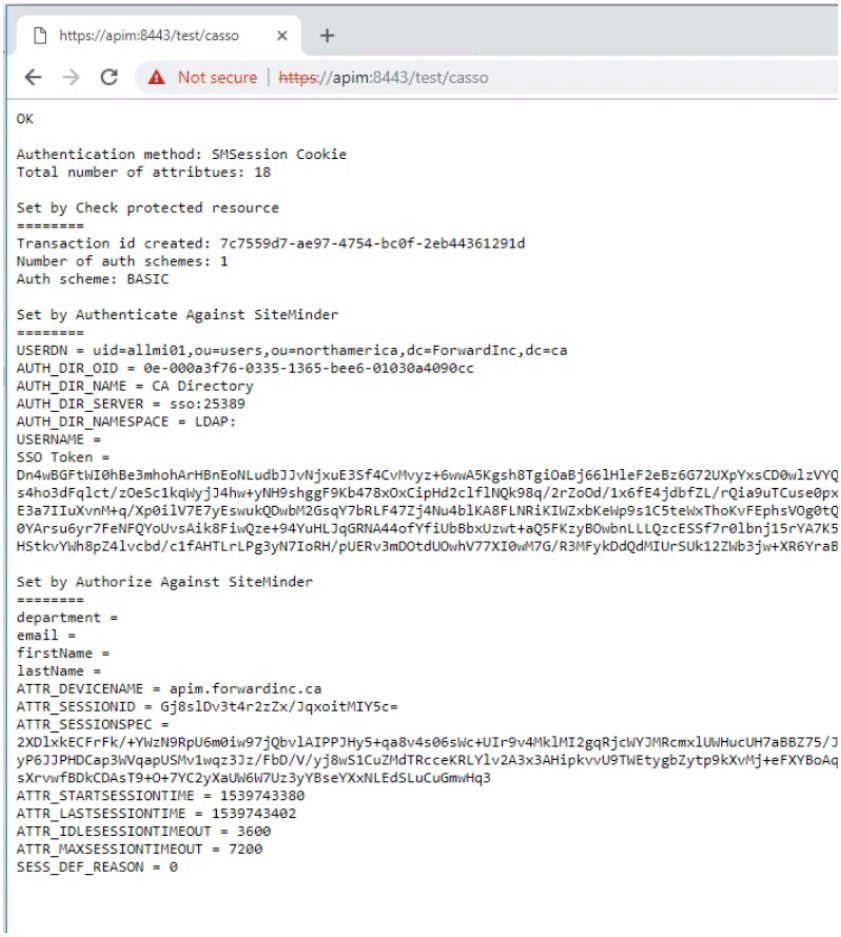
Test 2.

In browser, type https://apim:8443/test/casso?username=allmi01&password=CAdemo123
It returns smsession cookie and CA SSO related information.



Test3

Without closing browser, it access https://apim:8443/test/casso again. The user can access the page without any error because smession cookie is saved in the brower.


https://apim:8443/test/casso
Not secure | https://apim:8443/test/casso
OK
Authentication method: SMSession Cookie
Total number of attribtues: 18
Set by Check protected resource
========
Transaction id created: 7c7559d7-ae97-4754-bc0f-2eb44361291d
Number of auth schemes: 1
Auth scheme: BASIC
Set by Authenticate Against SiteMinder
========
USERDN = uid=allmi01,ou=users,ou=northamerica,dc=ForwardInc,dc=ca
AUTH_DIR_OID = 0e-000a3f76-0335-1365-bee6-01030a4090cc
AUTH_DIR_NAME = CA Directory
AUTH_DIR_SERVER = sso:25389
AUTH_DIR_NAMESPACE = LDAP:
USERNAME =
SSO Token =
Dn4wBGFtWI0hBe3mhohArHBnEoNLudbJJvNjxuE3Sf4CvMvyz+6wwA5Kgsh8TgiOaBj66lHleF2eBz6G72UXpYxsCD0wlzVYQ
s4ho3dFqlct/zOeSc1kqWyjJ4hw+yNH9shggF9Kb478xOxCipHd2clflNQk98q/2rZoOd/1x6fE4jdbfZL/rQia9uTCuse0px
E3a7IIuXvnM+q/Xp0ilV7E7yEswukQDwbM2GsqY7bRLF47Zj4Nu4blKA8FLNRiKIWZxbKeWp9s1C5teWxThoKvFEphsVOg0tQ
0YArsu6yr7FeNFQYoUvsAik8FiwQze+94YuHLJqGRNA44ofYfiUbBbxUzwt+aQ5FKzyBOwbnLLLQzcESSf7r0lbnj15rYA7K5
HStkvYWh8pZ4lvcbd/c1fAHTLrLPg3yN7IoRH/pUERv3mDOtdUOwhV77XI0wM7G/R3MFykDdQdMIUrSUk12ZWb3jw+XR6YraB
Set by Authorize Against SiteMinder
========
department =
email =
firstName =
lastName =
ATTR_DEVICENAME = apim.forwardinc.ca
ATTR_SESSIONID = Gj8slDv3t4r2zZx/JqxoitMIY5c=
ATTR_SESSIONSPEC =
2XDlxkECFrFk/+YWzN9RpU6m0iw97jQbvlAIPPJHy5+qa8v4s06sWc+UIr9v4MklMI2gqRjcWYJMRcmxlUWHucUH7aBBZ75/J
yP6JJPHDCap3WVqapUSMv1wqz3Jz/FbD/V/yj8wS1CuZMdTRcceKRLYlv2A3x3AHipkvvU9TWEtygbZytp9kXvMj+eFXYBoAq
sXrvwfBDkCDAsT9+O+7YC2yXaUW6W7Uz3yYBseYXxNLEdSLuCuGmwHq3
ATTR_STARTSESSIONTIME = 1539743380
ATTR_LASTSESSIONTIME = 1539743402
ATTR_IDLESESSIONTIMEOUT = 3600
ATTR_MAXSESSIONTIMEOUT = 7200
SESS_DEF_REASON = 0