

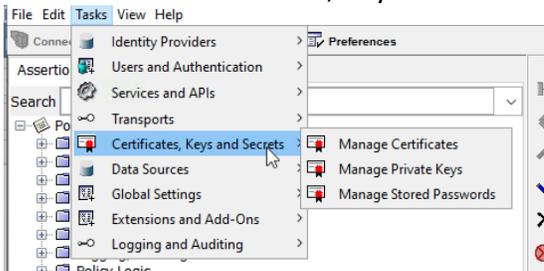
# CA SSO and CA APIM Integration Guide Part 2

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

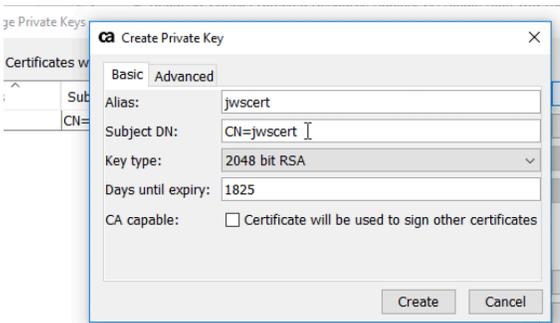
## CA SSO configuration – Integration with JWT Authentication

### 1. Create Private Key for JWT token Signing in APIM Gateway

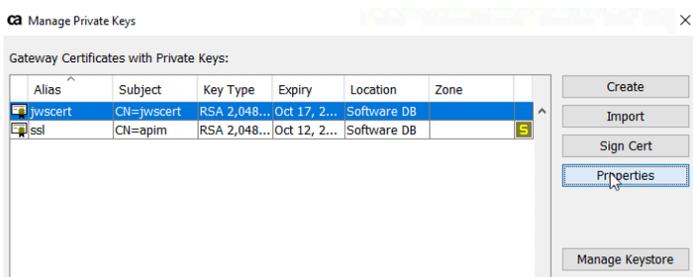
- Login APIM Policy Manager
- Go to Tasks -> Certificate, Keys and Secretes -> Manage Private Keys



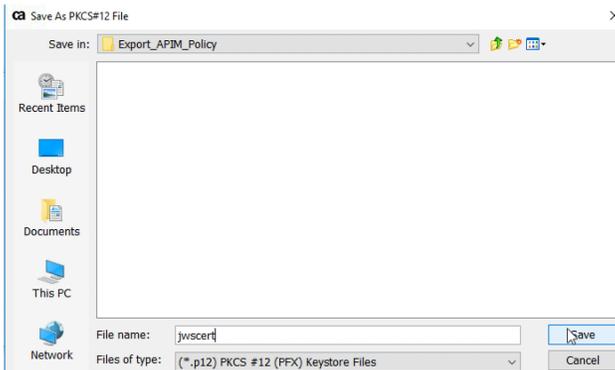
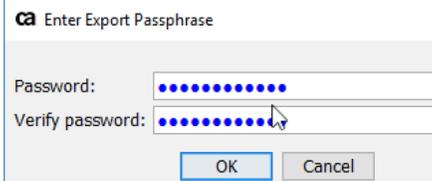
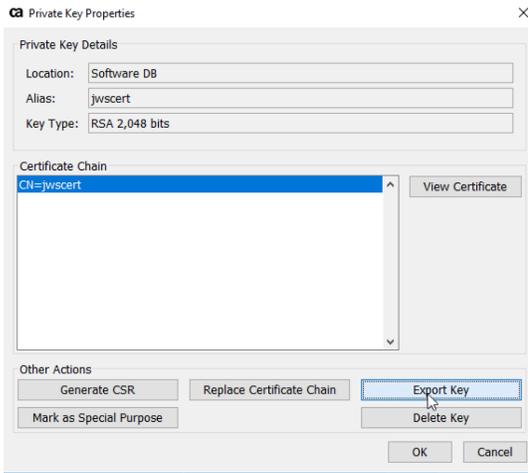
- Create new Private Key. In Alias, input "jwscert". Then, click "Create" button



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

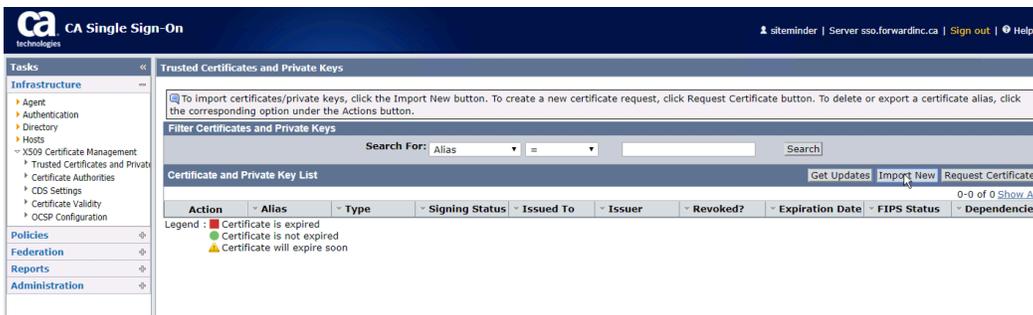


- Click "Export Key" and input the password. (Any password) Then save the exported key file with p12 format.



## 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.

1 Select File 2 Password (if needed) 3 Select Entries 4 Confirm

ct a file. PKCS#12 files (private key and certificate) must end in '.p12' or '.pfx'. Any other extension will be tra

Input File As:  Single Key/Cert File  Separate Key File and Cert File  
 Use as CA:  Yes  No

• File: C:\fakepath\jwscert.p12

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

Trusted Certificates and Private Keys

View Certificates and Private Keys > Import Certificate/Private Key

Back Next Finish Cancel

1 Select File 2 Password (if needed) 3 Select Entries 4 Confirm

Review and confirm selections for import.

Show Details	Alias	Type	Issued To
<input checked="" type="checkbox"/>	jwscert	Private Key and Certificate	CN=jwscert

Hide

Issued To: CN=jwscert  
 Issued By: CN=jwscert  
 Valid From: Oct 18, 2018 07:48 AM PDT  
 Key Algorithm: RSA  
 Serial Number: 11:A5:D7:A1:61:31:C7:61  
 Valid To: Oct 17, 2023 07:48 AM PDT  
 Version: 3  
 SHA-256 Fingerprint: 82:88:DF:CF:B8:13:17:E2:CF:92:89:EF:2B:2C:B7:47:AB:FE:8B:CB:6C:46:A7:99:C1:70:3F:9C:B6:91:43:42  
 SHA-1 Fingerprint: E1:7D:C5:55:8F:20:2F:26:9C:0E:6A:17:65:5B:8D:3E:33:35:3D:3B  
 MD5 Fingerprint: 02:71:08:29:6F:3B:6F:69:C1:9C:17:D5:FC:E1:F8:80

Back Next Finish Cancel

- 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

Create Authentication Scheme: JWT Auth Scheme

Authentication Schemes > Create Authentication Scheme: JWT Auth Scheme

• = Required

**General**

• Name: JWT Auth Scheme Description

**Scheme Common Setup**

• Authentication Scheme Type: JSON Web Token Template

• Protection Level: 5 [1-1,000,high]

Password Policies enabled for this Authentication Scheme

**Scheme Setup**

**JWT Token Authentication Attribute for Validation**

• User Lookup: sub

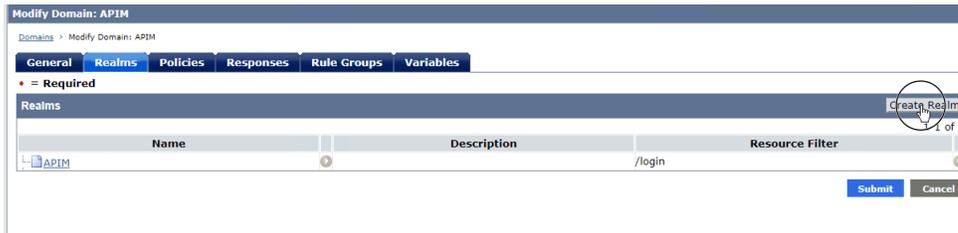
Certificate Alias List: jwscert

Use JOSE Header KID as Certificate Alias

HMAC Shared Key :

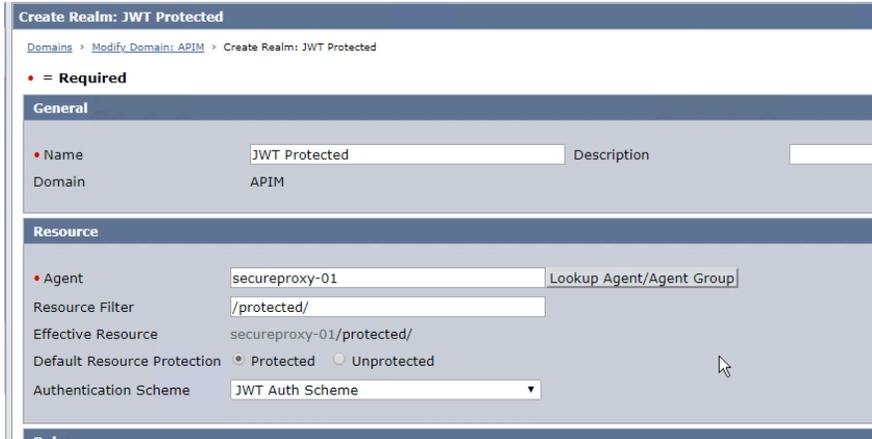
HMAC Confirm Shared Keys:

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



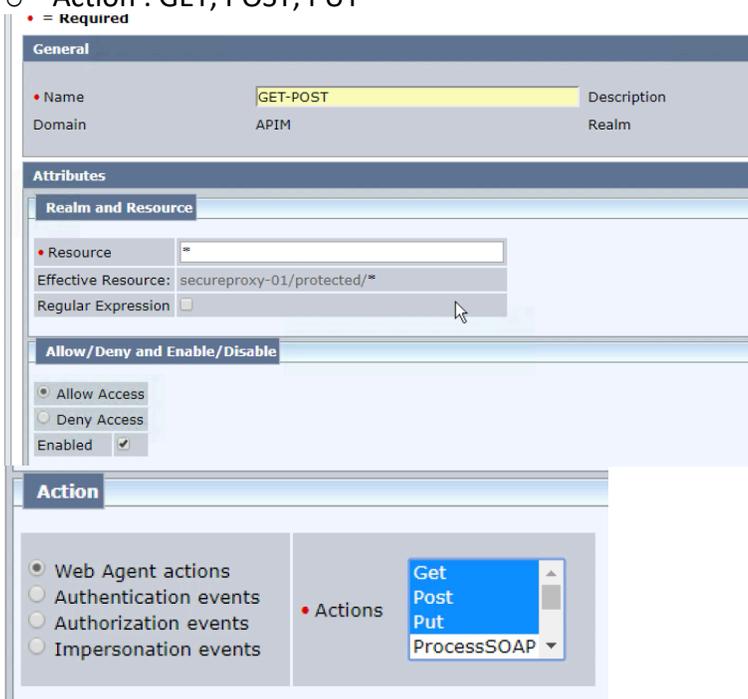
- Create new Realm

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



- Create Rule

- Name : GET-POST
- Resource : \*
- Action : GET, POST, PUT



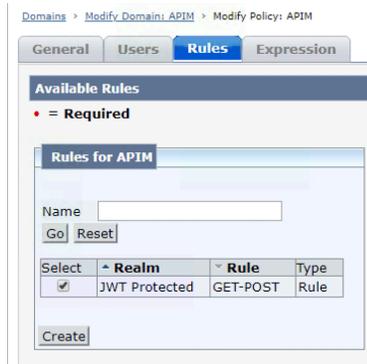
- Click "OK" button and Submit



- 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\*

ca Publish Web API Wizard

Steps

1. Service Information  
2. Access Control

Enter the name of the non-SOAP application you want to publish:

Service Name: Issue ID Token

Enter the HTTP URL that the Gateway should forward requests to:

Target URL:

Complete the Gateway URL that will receive service requests:

Gateway URL: http(s)://apim.forwardinc.ca:[port]/casso/idtoken\*

Specify the connection and routing information for the non-SOAP application.

Back Next Finish Cancel Help

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.)

ca Resolve External Dependencies Wizard

Steps

1. Unresolved CA Single Sign-On Configuration CASSO  
2. Unresolved provider CA SSO User DB

Policy contains assertions(s) referring to unknown CA Single Sign-On Configuration

Missing CA Single Sign-On Details

Configuration Name CASSO

Hostname apim.forwardinc.ca

Action

Change assertions to use this CA Single Sign-On configuration

CASSO

Remove assertions that refer to the missing CA Single Sign-On configuration

Import erroneous assertions as-is

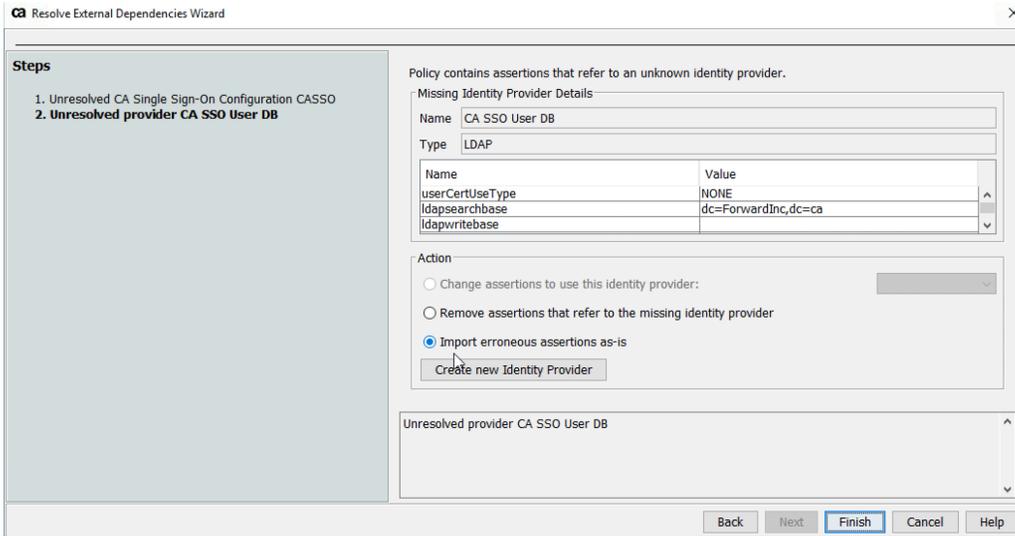
Create CA Single Sign-On Configuration

Unresolved CA Single Sign-On Configuration CASSO

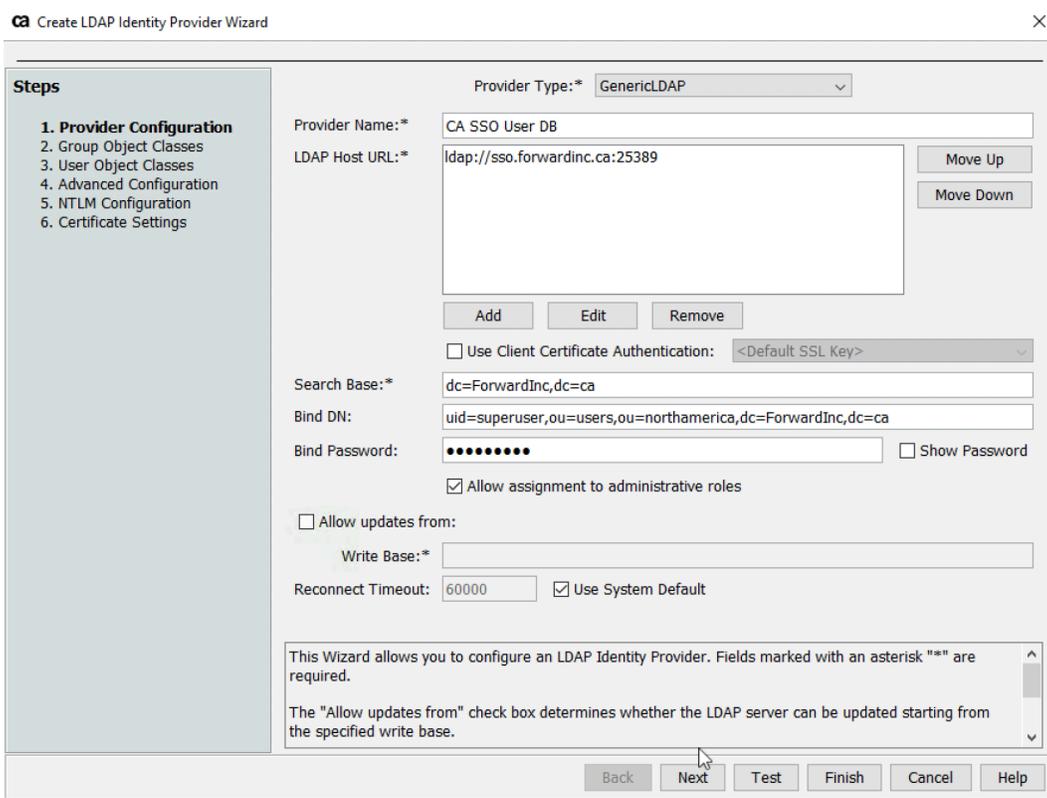
Back Next Finish Cancel Help

Then, click next

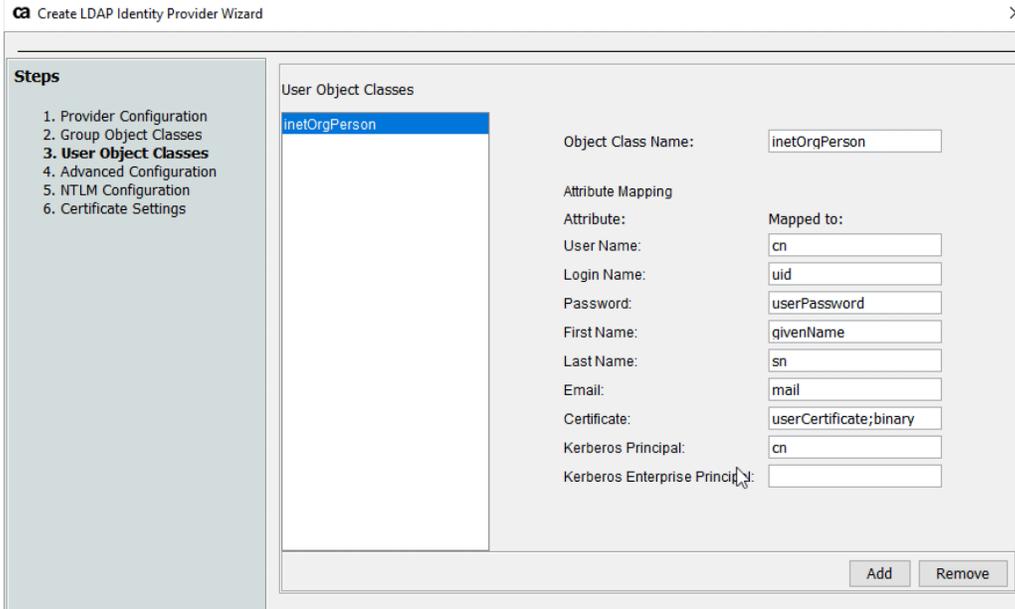
- In Wizard, select Import erroneous assertion as-is. “Create New Identity Provider”. It will connect CA SSO User Directory.



- It shows “Create LDAP Identity Provider Wizard” and input correct Bind Password. (CA demo123). Using “Test” button, please verify the connection. Depending on the environment, LDAP Host file and other information can be changed.

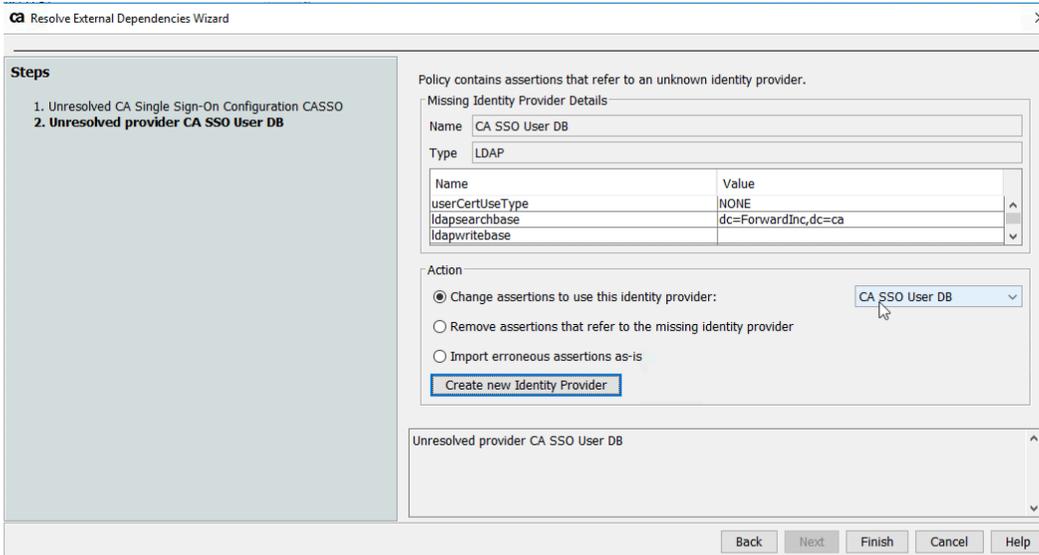


- Then, click “Next” continually. In User Object classes screen, please verify the Login Name. In CA LDAP, default Login Name should be “uid”. When you are using other user directory, it can be different.



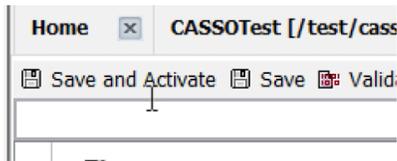
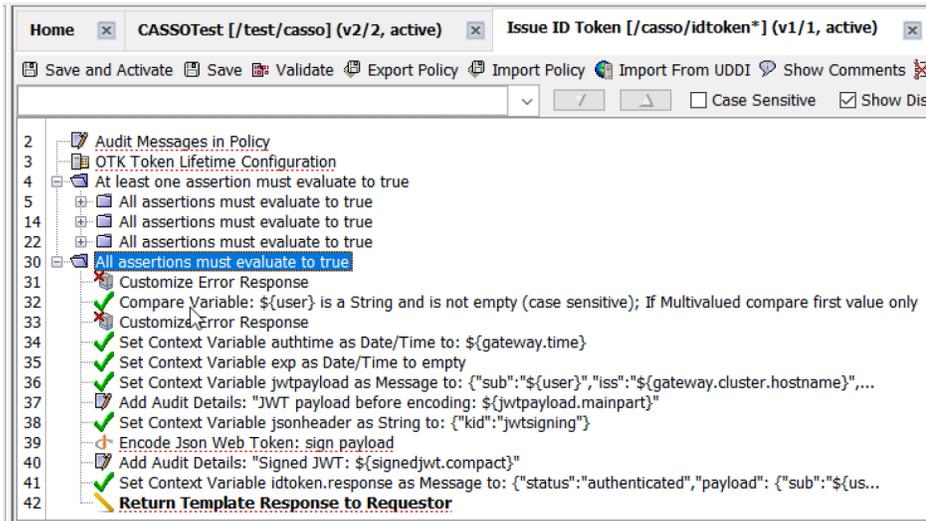
Then, click Finish button.

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



Then, click “Finish” button.

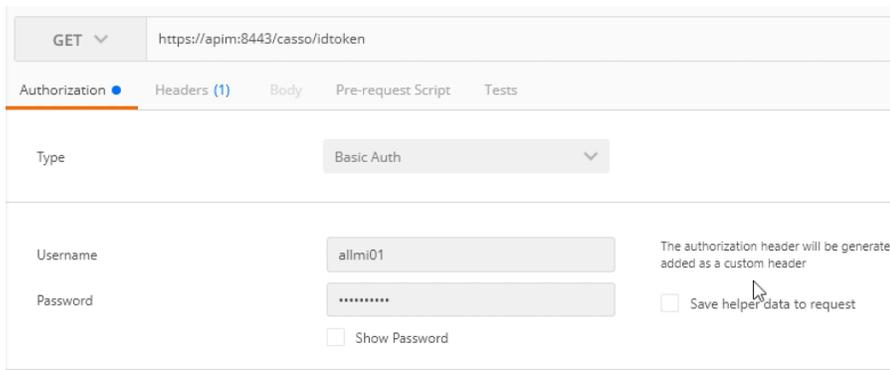
- Then, you can see the imported policies in UI. Click “Save and Activate” icon in UI.



- 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

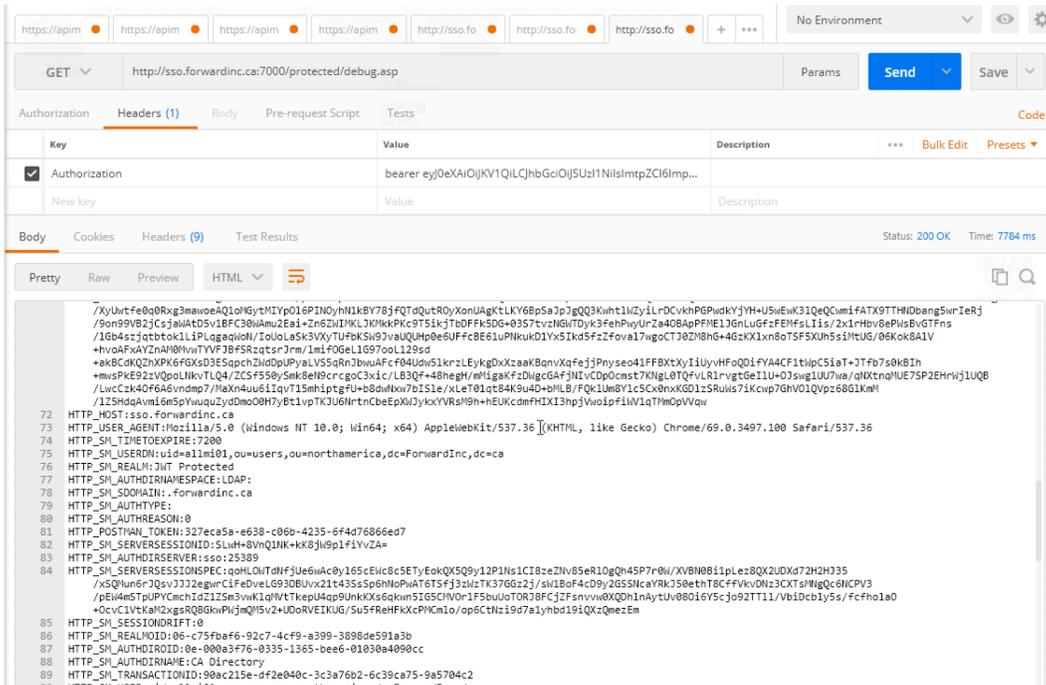
- Download PostMan (REST API Client) and execute it.
- In Postman, input the following information.
  - Method: GET
  - URL : **https:// <API GW FQDN>:8443/casso/idtoken**
  - User name: allmi01
  - Password: P@ssword01



Then, click “Send” button.

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





- After 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.

