

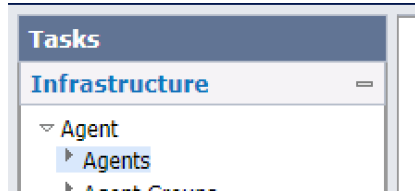
# CA SSO and CA APIM Integration Guide

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

## CA SSO configuration – Simple Integration with Basic Authentication

### 1. Create “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

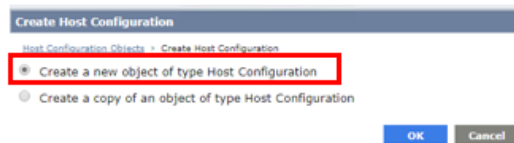
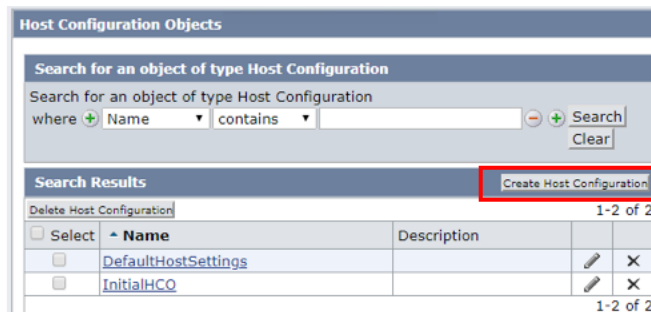
The screenshot shows the 'Create Agent' form. The 'Name' field is populated with 'agent.apim'. The 'Agent Type' is set to 'Web Agent'. The 'Submit' button is highlighted. Below the form, a table of existing agents is visible.

Select	Name	Description	Is 4x	Agent Type		
<input type="checkbox"/>	agent.apim			Web Agent		X
<input type="checkbox"/>	oneview-01			Web Agent		X
<input type="checkbox"/>	oneview-02			Web Agent		X
<input type="checkbox"/>	secureproxy-01			Web Agent		X
<input type="checkbox"/>	secureproxy-02			Web Agent		X

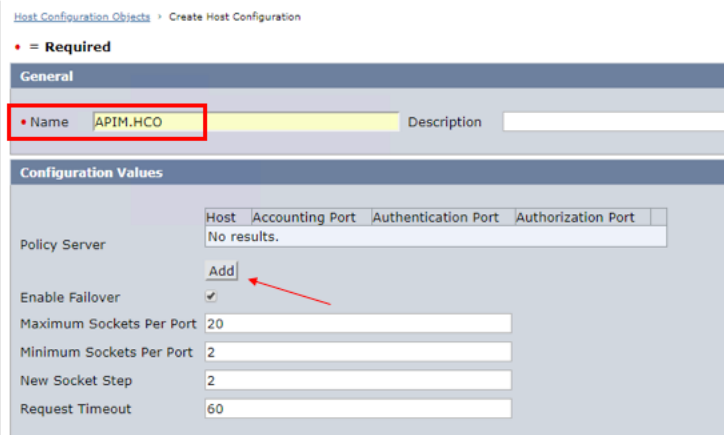
- Go to Infra Structure -> Hosts -> Host Configuration Object in CA SSO Admin UI



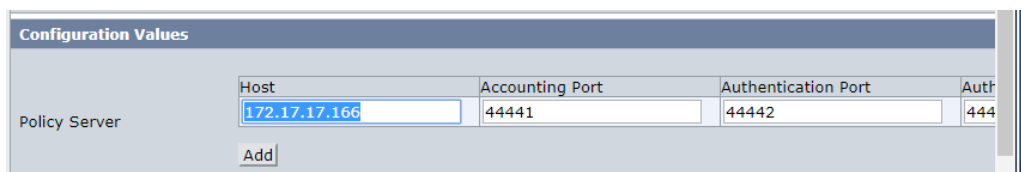
- Click "Create Host Configuration" button



- 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

**Search for an object of type Host Configuration**

Search for an object of type Host Configuration  
 where  Name  contains

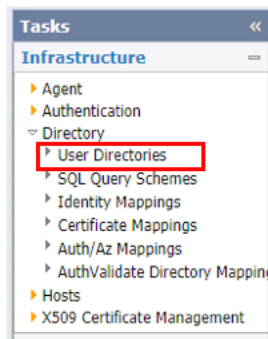
**Search Results**

Delete Host Configuration

Select	Name	Description
<input type="checkbox"/>	<a href="#">APIM.HCO</a>	
<input type="checkbox"/>	<a href="#">DefaultHostSettings</a>	
<input type="checkbox"/>	<a href="#">InitialHCO</a>	

## 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

**View User Directory: CA Directory**

User Directories > View User Directory: CA Directory > View User Directory: CA Directory

**General**

Name	Description
CA Directory	

**Directory Setup**

Namespace LDAP: sso:25389

Use authenticated user's security context ☐

Secure Connection ☐

**Administrator Credentials**

Require Credentials ☒

Username uid=superuser,ou=users,ou=northamerica,dc=ForwardInc,dc=ca

Password \*\*\*\*\*

Confirm Password \*\*\*\*\*

**LDAP Settings**

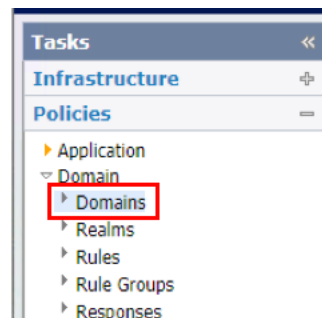
LDAP Search		LDAP User DN Lookup	
Root	dc=ForwardInc,dc=ca	Start	(uid=
Scope	One Level Sub-Tree	End	)
Max Time	30	Effective Lookup	(uid=ID-From-Login)
Max Results	0		
User Object			
User Class			

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

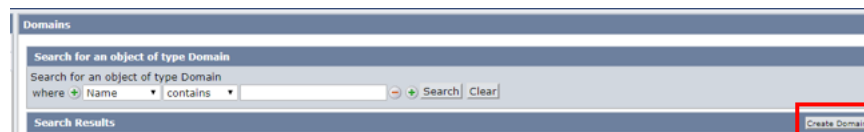
Users/Groups for CA Directory	
Search type	Attribute-value
Attribute	
Value	
Go	Reset
1-25 of 44 > >>	
Name	User Class
cn=AP AD,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP Analyst,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP HR,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP Insurance,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP Investments,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP Real Estate,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=AP Rep,ou=groups,ou=asiapacific,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E AD,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E Analyst,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E HR,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E Insurance,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E Investments,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E Real Estate,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=E Rep,ou=groups,ou=emea,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=IT,ou=groups,ou=northamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA AD,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA Analyst,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA HR,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA Insurance,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA Investments,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA Real Estate,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=LA Rep,ou=groups,ou=latinamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=Manager,ou=groups,ou=northamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=NA AD,ou=groups,ou=northamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
cn=NA Analyst,ou=groups,ou=northamerica,dc=ForwardInc,dc=ca	groupOfUniqueNames
1-25 of 44 > >>	

### 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

**Create Domain**

Domains > Create Domain

**General** Realms Policies Responses Rule Groups Variables

• = Required

**General**

• Name  Description

Global Policies Apply ☒

**User Directories**

Name	Description
No results.	

Create **Add/Remove**

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

**Create Domain: APIM**

Domains > Create Domain: APIM

**General** Realms Policies Responses Rule Groups Variables

**Choose user directories**

• = Required

Available Members	Selected Members
CA Directory	
FederationWS/CustomUserStore	
SAML2FederationCustomUserStore	

OK Cancel

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

**Create Domain: APIM**

Domains > Create Domain: APIM

**General** **Realms** Policies Responses Rule Groups Variables

• = Required

**Realms** **Create Realm**

Name	Description	Resource Filter
0-0 of 0		

Submit Cancel

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

**Select an Agent**

• = Required

Filter  Go Reset

Select	Name	Type
<input checked="" type="radio"/>	agent.apim	Agent
<input type="radio"/>	oneview-01	Agent
<input type="radio"/>	oneview-02	Agent
<input type="radio"/>	secureproxy-01	Agent
<input type="radio"/>	secureproxy-02	Agent
<input type="radio"/>	FederationWebServicesAgentGroup	Agent Group
<input type="radio"/>	OneView	Agent Group
<input type="radio"/>	SecureProxyServer	Agent Group

Create Agent Create Agent Group

- Resource Filter: /login
- Authentication Scheme : Basic

**Create Realm: APIM**

Domains > Create Domain: APIM > Create Realm: APIM

• = Required

**General**

• Name  Description  
Domain

**Resource**

• Agent  Lookup Agent/Agent Group  
Resource Filter   
Effective Resource   
Default Resource Protection ☒ Protected ☐ Unprotected  
Authentication Scheme

**Rules**

- Rules section, click “Create” button

**Rules**

Name	Description	Resource	Actions	Enabled
No results.				

**Create**

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

**Create Rule**

Domains > Create Domain: APIM > Create Realm: APIM > Create Rule

• = Required

**General**

• Name  Description  
Domain  Realm

**Attributes**

**Realm and Resource**

• Resource   
Effective Resource:   
Regular Expression ☐

**Allow/Deny and Enable/Disable**

☒ Allow Access  
☐ Deny Access  
Enabled ☒

**Action**

☒ Web Agent actions  
☐ Authentication events  
☐ Authorization events  
☐ Impersonation events

• Actions

- Click “OK” button and exit rule setting

- Click “OK” button and exit Realm setting

The screenshot shows the 'Create Domain: APIM' interface with the 'Realms' tab selected. The 'Realms' section contains a table with columns 'Name', 'Description', and 'Resource Filter'. The table has one entry: 'APIM' with a description of '/login'. There is a 'Create Realm' button in the top right corner of the table. Below the table are 'Submit' and 'Cancel' buttons.

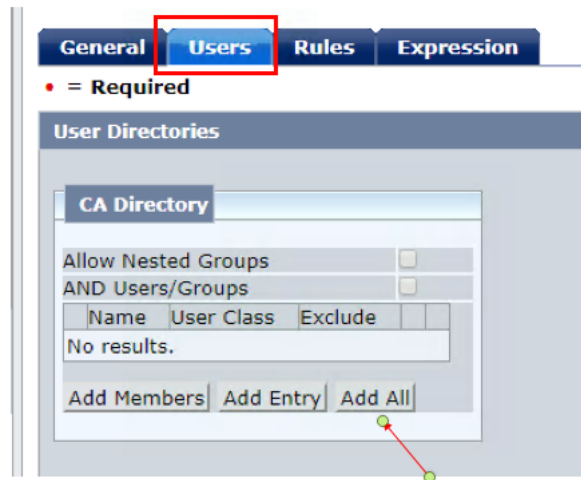
- Click Policies tab and click “Create” button

The screenshot shows the 'Create Domain: APIM' interface with the 'Policies' tab selected. The 'Policies' section contains a table with columns 'Name' and 'Description'. The table is empty, showing 'No results.' Below the table is a 'Create' button.

- In General tab, input name “APIM”

The screenshot shows the 'Create Policy' interface with the 'General' tab selected. The 'General' section contains a form with the following fields: 'Name' (input field with 'APIM'), 'Domain' (input field with 'APIM'), and 'Validate Identity' (checkbox). The 'Description' field is labeled 'Enabled'. Below the 'General' section is the 'Restrictions' section, which contains a 'Time' section with 'Set' and 'Clear' buttons and a text field 'No Time Restrictions apply'. Below the 'Time' section is an 'IP Address' section with a table containing columns 'IP Address', 'Subnet Mask', 'End of Range', and 'Host Name'. The table is empty, showing 'No results.' Below the table is an 'Add' button.

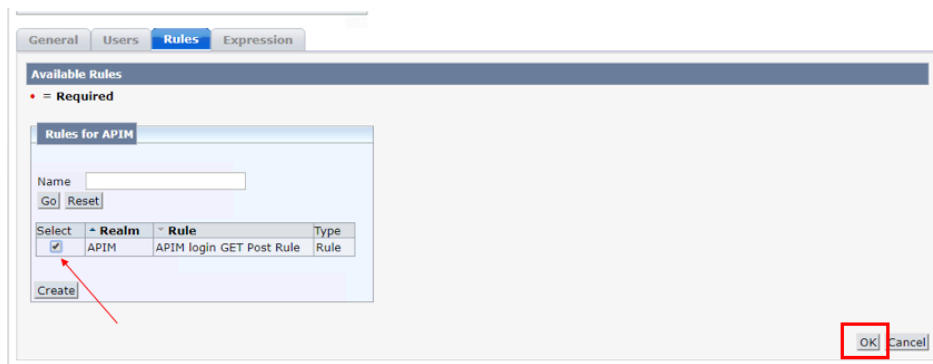
- In Users tab, click “Add All” button. (it means that every users in user DB can access the resource.)



- In Rules tab, 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

GeneralRealmsPoliciesResponsesRule GroupsVariables

• = Required

Policies

	Name	Description	
	APIM		

Create

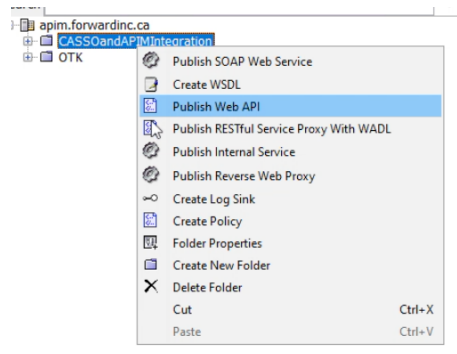
Submit

Cancel

# CA APIM configuration – Simple Integration with CA SSO SDK

## 1. Create New Web API for CA SSO Integration

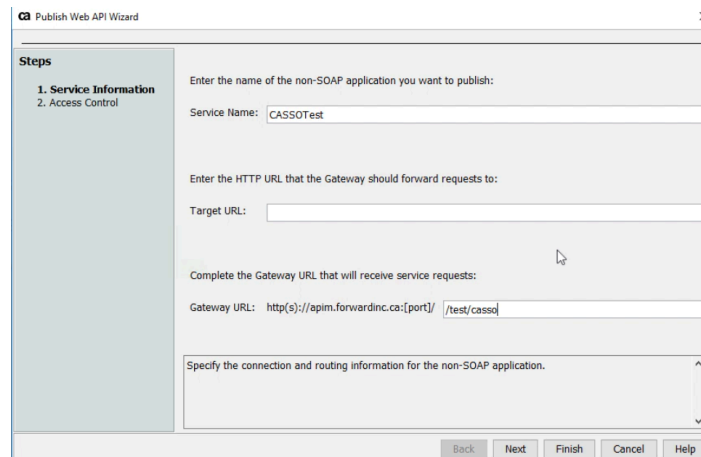
- Login into CA APIM Policy Manager and publish web API



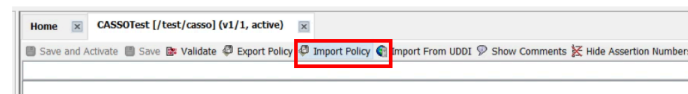
- Input Service information and click “Finish” button

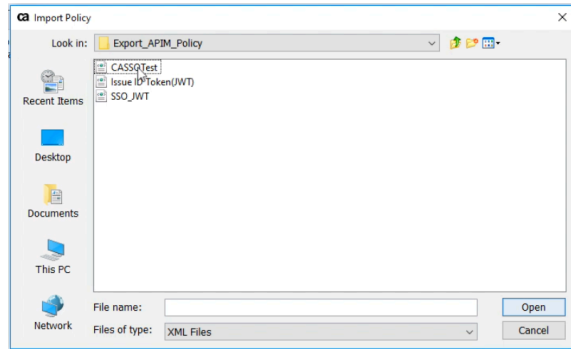
Service Name : CASSOTest

Gateway URL: /test/casso

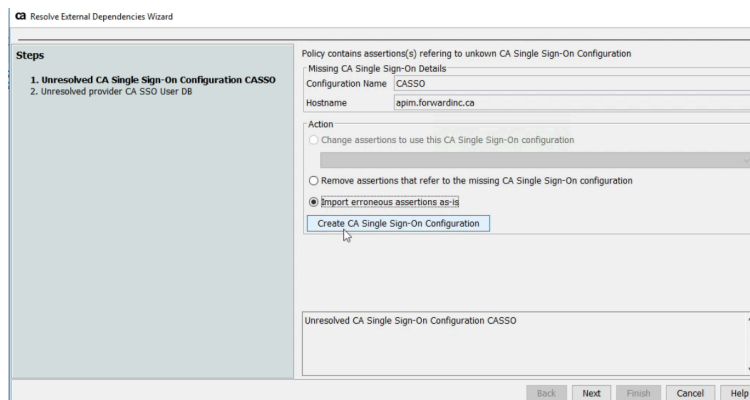


- Import “CASSOTest” policy, which is download from the site. (CASSOTest.xml)

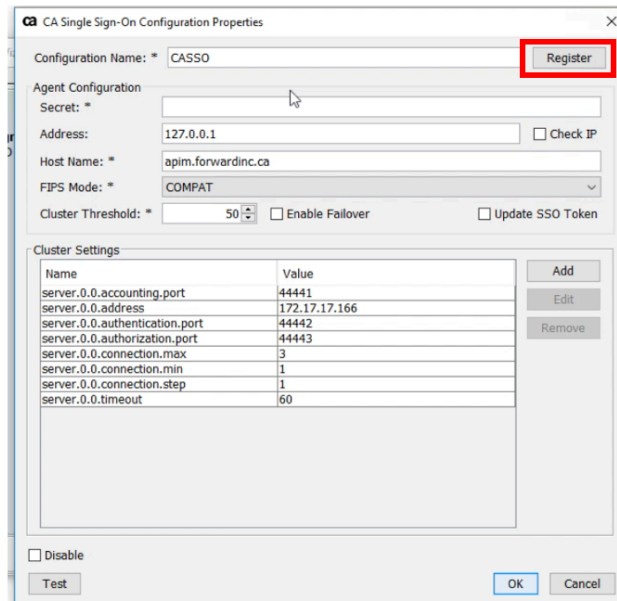




- Pop up “Resolve External Dependency Wizard” windows and select “Import erroneous assertion as-is”. Then, click “Create CA Single Sign-On Configuration”.



- 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

CA Single Sign-On Registration Properties

CA Single Sign-On Registration Parameters

Address: \* 172.17.17.166

Host Name: \* apim.forwardinc.ca

Host Configuration: \* APIM.HCO

FIPS Mode: \* COMPAT

User Name: \* siteminder

Password: \* SiteMinderPassword

Manage passwords

OK Cancel

Policy Server IP Address or Hostname

Trust Host name ( Any name can be used)

Host configuration Object name, which is defined in CA SSO Admin UI

FIPS mode (please check Policy Server FIPS mode.)

CA SSO Admin User Name

CA SSO Admin Password

CA Single Sign-On Registration Properties

CA Single Sign-On Registration Parameters

Address: \* 172.17.17.166

Host Name: \* apim.forwardinc.ca

Host Configuration: \* APIM.HCO

FIPS Mode: \* COMPAT

User Name: \* siteminder

Password: \* SiteMinderPassword

Manage passwords

OK Cancel

Registering...

Cancel

CA Single Sign-On Configuration Properties

Configuration Name: \* CASSO

Register

Agent Configuration

Secret: \*

Address: 127.0.0.1

Check IP

Host Name: \* apim.forwardinc.ca

FIPS Mode: \* COMPAT

Cluster Threshold: \* 50

Enable Failover

Update SSO Token

Cluster Settings

Name	Value
server.0.0.accounting.port	44441
server.0.0.address	172.17.17.166
server.0.0.authentication.port	44442
server.0.0.authorization.port	44443
server.0.0.connection.max	3
server.0.0.connection.min	1
server.0.0.connection.step	1
server.0.0.timeout	60

Add

Edit

Remove

Disable

Test

OK Cancel

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

Resolve External Dependencies Wizard

Steps

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

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

Missing CA Single Sign-On Details

Configuration Name CASSO

Hostname apim.forwardinc.ca

Action

☒ Change assertion to use this CA Single Sign-On configuration

CASSO

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

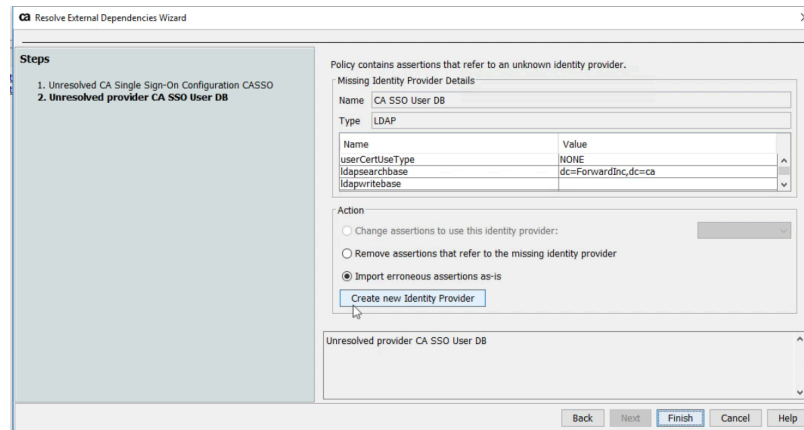
☐ Import erroneous assertions as-is

Create CA Single Sign-On Configuration

Unresolved CA Single Sign-On Configuration CASSO

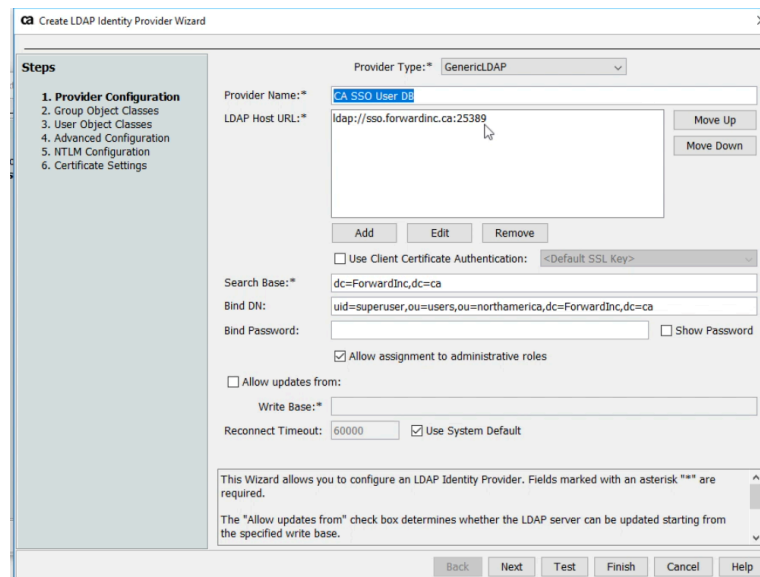
Back Next Finish Cancel Help

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



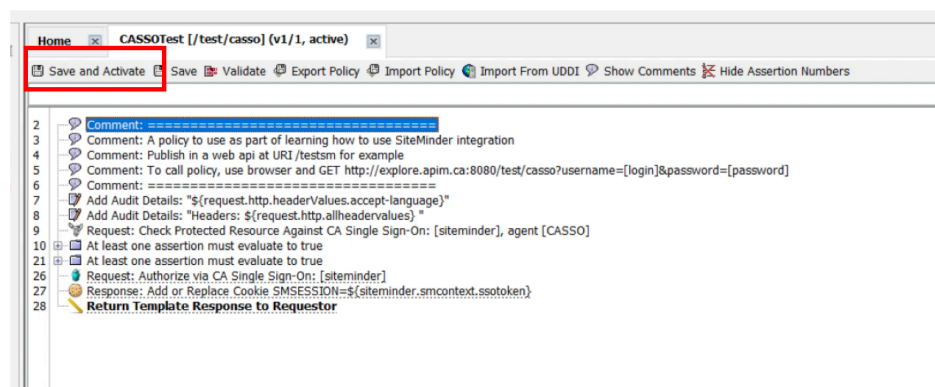
- **Change LDAP Identity Provider Wizard based on user directory in CA SSO. You can find the in detail connection information from CA SSO User Directory.**

*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.**

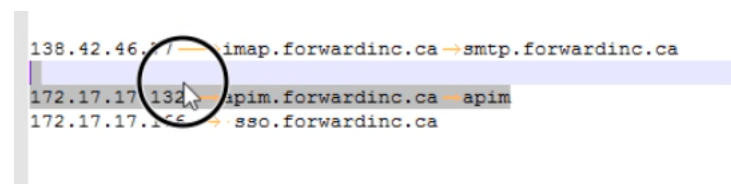
- When it shows imported assertions in the UI, please click “Save and Activate” icon.



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>.

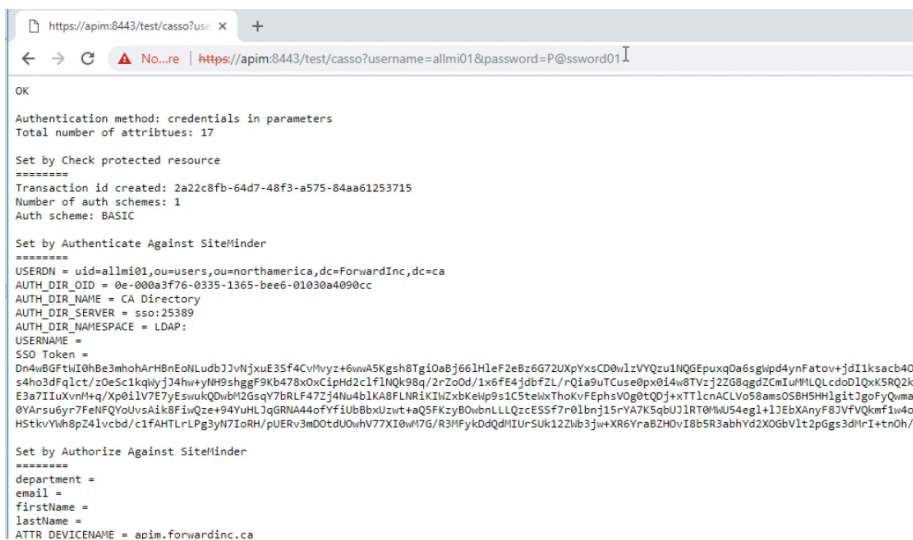


It shows kind of warning message with guide.

## 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 smsession cookie is saved in the browser.

