Cisco ISE 2.1 Guest Portal with SAML login option plus Sponsor Portal filtered pending accounts

Developers and Lab Proctors

This lab was created by Jason Kunst and Hsing-Tsu Lai, ISE Technical Marketing Engineers

Lab Overview

This lab is designed to help attendees understanding new and key features in Cisco Identity Services Engine (ISE) Release 2.1 around the integration of SAML SSO and Guest Credentials into a single portal. It expands on the capabilities of ISE 1.4 which allowed ISE web auth portals to integrate directly with Oracle Access Manager. ISE 2.1 supports more providers out of the box including SAML 2.0 standards. We will also show a new feature that allows filtering of Sponsor portal pending accounts list to only show the accounts that are destined for that sponsor.

In this environment we showcase how we are using PingFederate along with a single guest portal to allow guests and SAML SSO (ex: employees) to login to a single guest portal which also allowed a single Wireless LAN (SSID). Prior to this release guest and SAML SSO portals had to be separated and would require more than 1 Wireless LAN (SSID).

When working with SAML integration the following terms are used:

Identity Provider (IdP) – in this case its PingFederate

Service Provider (SP) – this is your ISE portal

These new providers are also supported for access to Sponsor, My Devices and Certificate Provisioning Portals.

Lab participants should be able to complete the lab within the allotted time of 1.5 hours.

It is recommended that you are familiar with the Guest and Sponsor capabilities before taking this lab as we will not be showing how those work.

Lab Exercises

This lab guide includes the following exercises:

- Lab Exercise 1.1: Configure ISE SAML IdP & Portal Basics
- Lab Exercise 1.2: Configure PingFederate IdP for ISE Guest Web Auth Portal
- Lab Exercise 1.3: Configure PingFederate IdP for ISE Sponsor Portal
- Lab Exercise 1.4: Finalize configuration of ISE IdP and Sponsor settings
- Lab Exercise 1.5: Guest Web Auth & Sponsor Portal Usage with SAML SSO features
- Lab Exercise 1.6: Review some common logs

Lab Exercise 1: ISE & PingFederate SAML Config

Lab Exercise 1.1: Configure ISE SAML IdP & Portal Basics

Exercise Description

In this exercise you will configure a SAML Identity Provider on ISE. This IdP will be used with your Guest and Sponsor Portals for single-sign on. This IdP will be used as the authentication provider used for a sub-portal which is mapped to on a Main Portal.

This gives you the capability of having a single portal (or entry point) into your network to handle both your guest and employee SSO logins. This single entry point can accommodate both types of users a single wireless lan (SSID) or wired network. Without this capability an administrator would have to configure 2 separate SSIDs to handle the different type of users. This is not a good user experience to have to worry about different open networks. On a wired network it wouldn't be possible to have a redirection that would handle both without this newly added feature.

Each ISE Portal that is using the IdP for SSO will be an SP. Here we are going to configure the Guest Portal using SSO and Sponsor Portal for Guest Access Management as a SP by pointing them to the PingFederate IdP.

The same configuration can be used with My Devices and Certificate Provisioning Portals. We won't be covering them in this lab.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Add PingFederate SAML IdP to ISE
- Create a Subportal for use with PingFederate SAML IdP
- Configure Main Guest Portal to use Sub-portal for SAML SSO

Exercise Steps

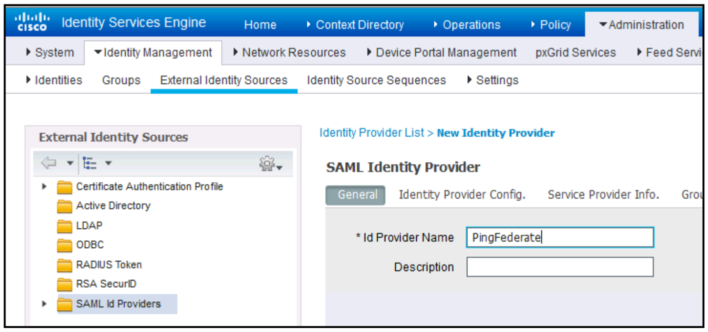
In the following steps you will setup PingFederate as a SAML IdP on ISE. In order to get the needed SAML Metadata from ISE you will have to do some basic setup and identification of the portals that are going to be used with the PingFederate solution.

Step 1 From the Admin PC, launch **Firefox** to go to https://ise.demo.local and login with **admin/ISEisC00L**

Step 2 Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers**

Step 3 Click **Add**

Step 4 Under General enter an **Id Provider Name**



* Id Provider Name: PingFederate

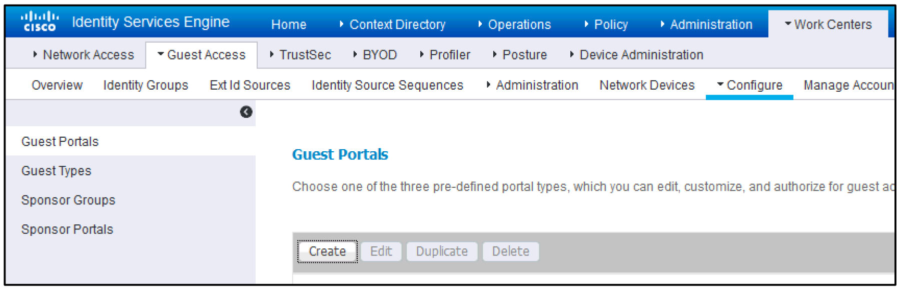
Description:

Step 5 Click **Submit**

In the following steps you will create a Guest Sub Portal that uses the PingFederate IDP for SAML SSO.

Step 6 Navigate to **Work Centers > Guest Access > Configure > Guest Portals**

Step 7 Click **create** and select **Self-Registered Guest Portal (it doesn't matter if this is Sponsored or self-registered portal as this portal will simply point to a SAML provider for login.**

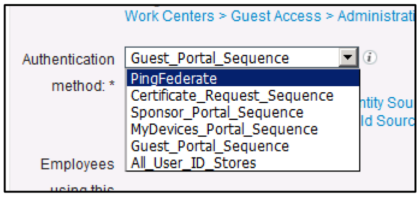


Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest ac

Step 8 Click **Continue**

Step 9 Name the portal – **MySubPortalForSSO**

Step 10 Expand **Portal Settings** and select **PingFederate**

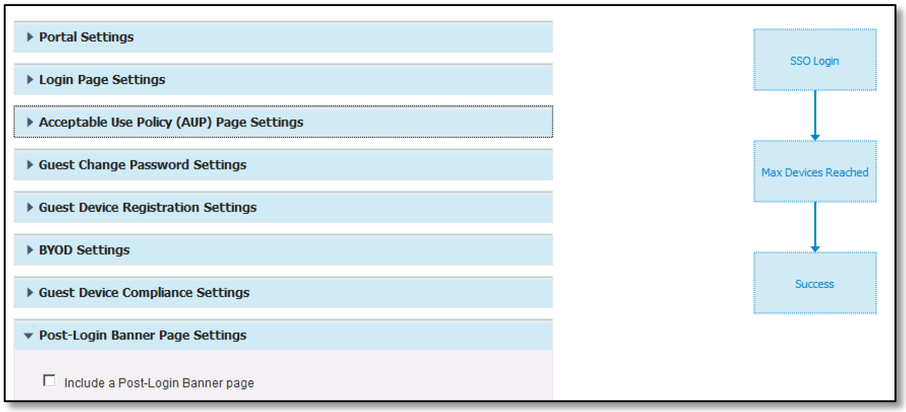


Authentication method: * Guest_Portal_Sequence

- PingFederate
- Certificate_Request_Sequence
- Sponsor_Portal_Sequence
- MyDevices_Portal_Sequence
- Guest_Portal_Sequence
- All_User_ID_Stores

Step 11 Expand **Acceptable Use Policy (AUP)** and **Post-Login Banner Page Settings** and uncheck the options

Notice the portal flow is going to use SSO for login. This is the portal that our main portal will redirect the user to for the SSO capabilities with PingFederate.



- Portal Settings
- Login Page Settings
- Acceptable Use Policy (AUP) Page Settings
- Guest Change Password Settings
- Guest Device Registration Settings
- BYOD Settings
- Guest Device Compliance Settings
- Post-Login Banner Page Settings

□ Include a Post-Login Banner page

Step 12 **Save** the portal

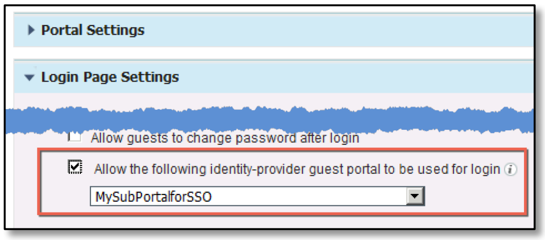
In the following steps you will map the Sub Portal used for SSO to a new Main Portal allow Guest Credential or SAML SSO portal access

Step 13 Click **Close** to bring back the list of Guest Portals (or Navigate back to **Guest Portals** listing)

Step 14 Click **Create** and choose the **Self-registered Guest Portal** and click **Continue.**

Step 15 Name the portal **MainPortal**

Step 16 Expand **Login Page Settings** and choose your Guest Sub Portal for SSO



- Portal Settings
- Login Page Settings

□ Allow guests to change password after login

☑ Allow the following identity-provider guest portal to be used for login

MySubPortalforSSO

Step 17 Expand **Self-Registration Page Settings**

Step 18 Set the guest account requirement for approval. This will allows us to work with the filtering guest accounts pending account approval.

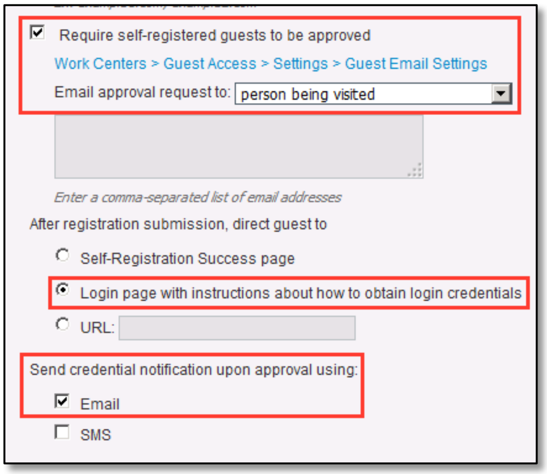
a. Check the box for **require self-registered guests to be approved**

b. In the pull down for Email approval request to: Select **person being visited** (which is your sponsor)

Note: The following 3 settings are not required to test this out but will be closer to the experience you would want a user to go through. We set the requirements to minimize the amount of pages the user must go through and to provide appropriate messaging for the desired flow

Step 19 Under After registration submission, direct guest to, choose the option: **Login page with instructions about how to obtain login credentials**

Step 20 Under Send credential notification upon approval using: Check the box for **Email**



☑ Require self-registered guests to be approved

Work Centers > Guest Access > Settings > Guest Email Settings

Email approval request to: person being visited

Enter a comma-separated list of email addresses

After registration submission, direct guest to

○ Self-Registration Success page

● Login page with instructions about how to obtain login credentials

○ URL:

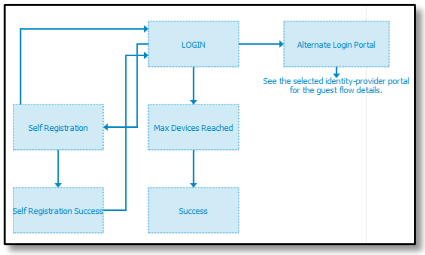
Send credential notification upon approval using:

☑ Email

□ SMS

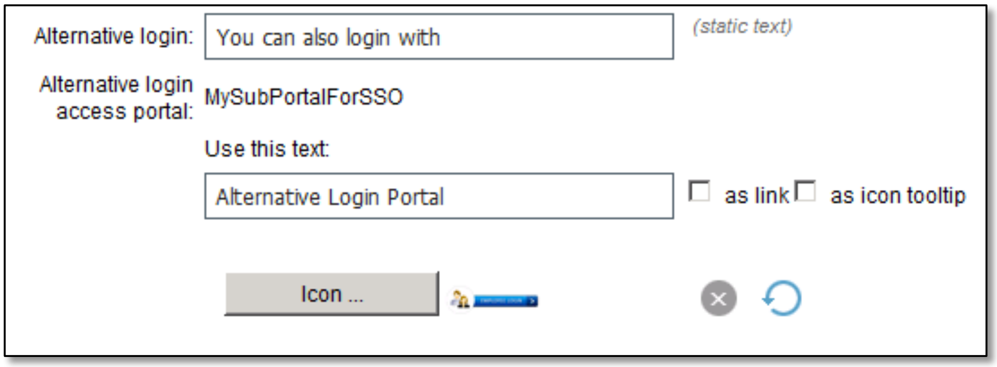
Step 21 Expand **Acceptable Use Policy (AUP)** and **Post-Login Banner Page Settings** and uncheck those options.

Notice the updated flow diagram showing the Main Portal linked to another portal for the SSO function.


LOGIN
Alternate Login Portal
See the selected identity-provider portal for the guest flow details.
Self Registration
Max Devices Reached
Self Registration Success
Success

Step 22 Navigate to **Portal Page Customization > Pages > Login**

Step 23 **Scroll down and notice the new option to customize the alternate login**



Alternative login: You can also login with *(static text)*

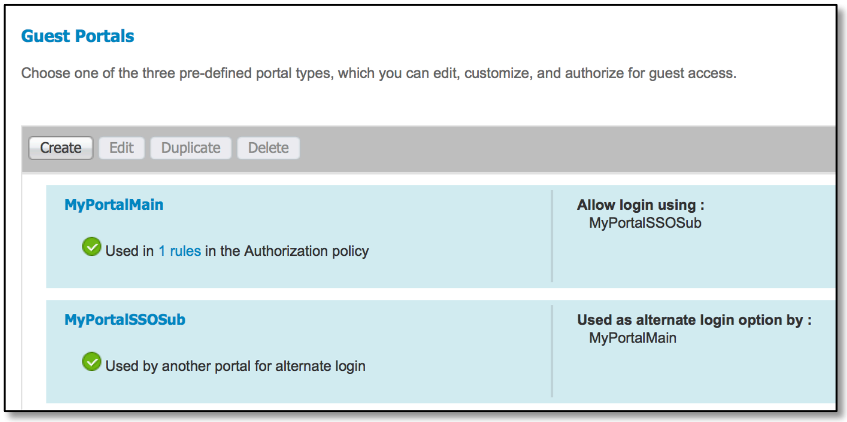
Alternative login access portal: MySubPortalForSSO

Use this text:

Alternative Login Portal □ as link □ as icon tooltip

Step 24 Click **Save**

Note: After you have configured your main portal (for guest that also uses the SSO sub-portal) and sub-portal (for SSO) you will see a similar portal message. In this lab we are not working with the Authorization Policies so what you have will look close (without the green checkboxes). All the testing for this was done with the portal test URLs. If order to work in your production environment you will need to make sure your authorization policies for CWA (guest credentialed portal) are setup to use the MyPortalMain


Guest Portals
Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.
Create
Edit
Duplicate
Delete

MyPortalMain

✓ Used in 1 rules in the Authorization policy

Allow login using :
MyPortalSSOSub

MyPortalSSOSub

✓ Used by another portal for alternate login

Used as alternate login option by :
MyPortalMain

Configure the Sponsor Portal to use an easy url (FQDN) for access and point it to the PingFederate IDP for SAML SSO.

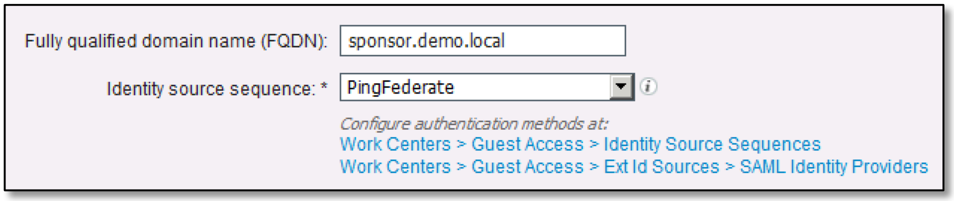
Step 25 Navigate to **Work Centers > Guest Access > Configure > Sponsor Portals**

Step 26 Click on **Sponsor Portal (default)**

Step 27 Expand **Portal Settings**

Step 28 Under the FQDN section enter: **sponsor.demo.local**

Step 29 Under Identity Source Sequence select **PingFederate.**

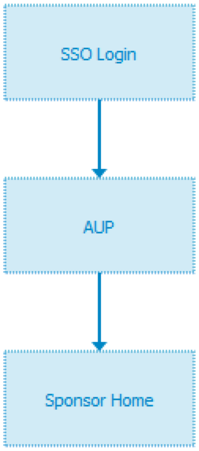


Fully qualified domain name (FQDN): sponsor.demo.local

Identity source sequence: * PingFederate

Configure authentication methods at:
Work Centers > Guest Access > Identity Source Sequences
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Note: Notice the flow the sponsor will go through is reflected in the built-in flow model



Step 30 Click **Save**

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 1.2: Configure PingFederate IdP for ISE Guest Web Auth Portal

Exercise Description

In this exercise you will go over the Ping Federated IdP configuration needed to work with ISE as an IdP for the Guest WebAuth Portal SP. You will export the needed SP information from ISE for the Guest WebAuth and Sponsor portals you configured before. You will also export the needed SAML XML files from the IdP to import onto ISE.

Exercise Objective

In this exercise, your goal is to complete the following tasks to setup PingFederate to work with the Guest WebAuth Portal:

- Export of the ISE SP information for the Guest Web Auth and Sponsor Portals
- Configuration of the ISE Guest WebAuth Portal on PingFederate as a Service Provider.

Exercise Steps

In these steps you will configure PingFederate as an IDP for ISE to use for SSO and the ISE Guest WebAuth Portal

On ISE we are getting the Metadata to import on the IdP (PingFederate). Each ISE Portal that is using SSO is going to be its own SP (Service Provider) and will need to be configured to use the IdP. Because of this, the XML file you export from ISE IdP settings will need to have each portal you want to use for SSO populated in it. The XML you export from ISE is imported into the IDP (Ping Federate). The IdP also has an XML file that is imported into ISE IdP config.

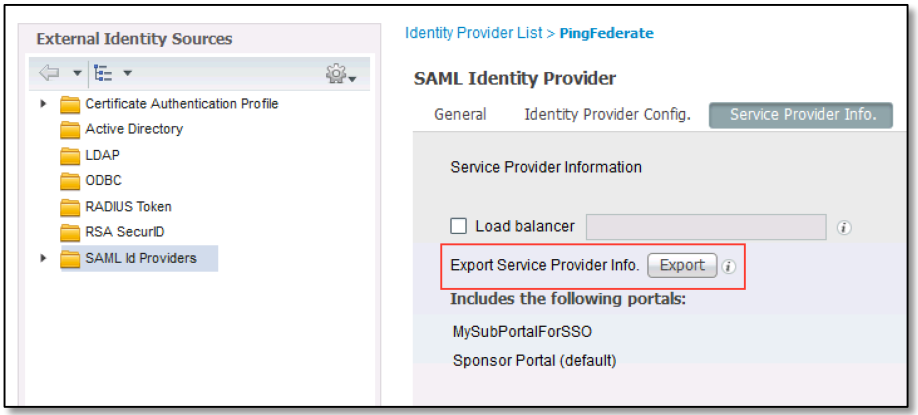
Step 1 From the Admin PC, launch **Firefox** to go to http://ise-1.demo.local

Step 2 Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**

Step 3 Click **Service Provider Info**

Note: There is an entry for each of the portals you have configured to use PingFederate as an IdP. Each of these portals is considered an SP. The information for each portal will be included in the XML Metadata that you will export to use on the IdP.

Step 4 Click **Export** and **Save** the .Zip file (PingFederate.Zip)

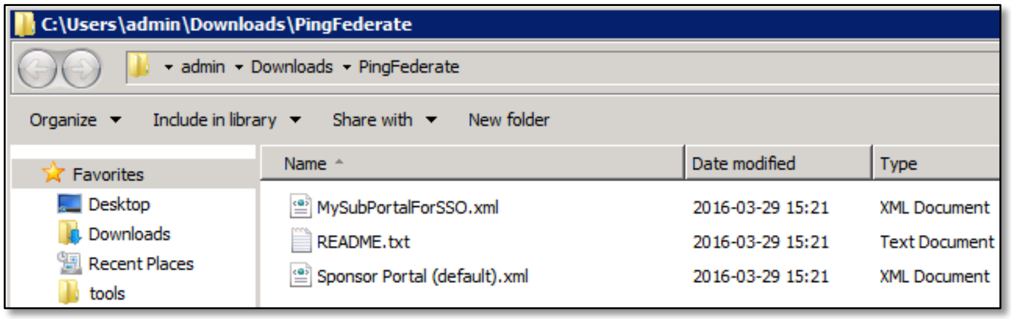

External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Identity Provider List > PingFederate
SAML Identity Provider
General
Identity Provider Config.
Service Provider Info.
Service Provider Information
Load balancer
Export Service Provider Info.
Export

Includes the following portals:

MySubPortalForSSO

Sponsor Portal (default)

Step 5 After the save of the Zip package you will need to extract it, navigate using File Explorer on the windows admin machine to the **download directory** and **extract all**. You will see 3 files. Each XML file is used for a different portal as the SP config on the SAML server.



Name	Date modified	Type
MySubPortalForSSO.xml	2016-03-29 15:21	XML Document
README.txt	2016-03-29 15:21	Text Document
Sponsor Portal (default).xml	2016-03-29 15:21	XML Document

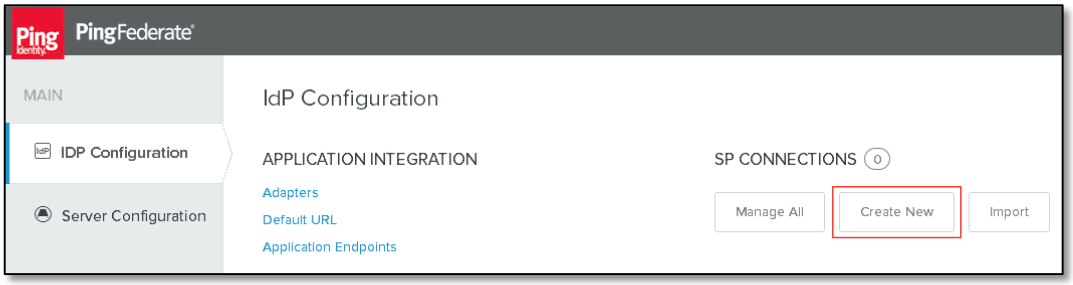
You will now configure the PingFederate IdP to use ISE SP Guest WebAuth Portal. The configuration is the same for My Devices and Certificate Provisioning Portals (which we are not covering).

Step 6 From the Admin PC, launch **Firefox** to go to https://pf.demo.local:9999/pingfederate/app and login with **admin/ISEisC00L**

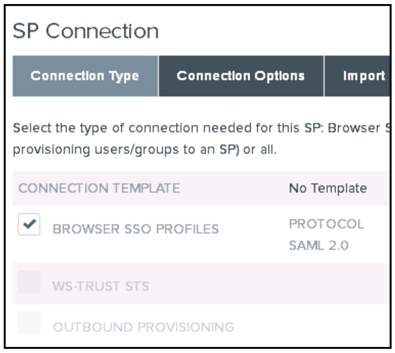
Step 7 Navigate to **IDP Configuration**

Step 8 Click **Create New**

Note: When going through these steps, don't let the page timeout, Ping doesn't like this and will cause you go to have to delete your config and start over as Ping doesn't save your settings well. You can try using Save Draft but I haven't had good luck with that.



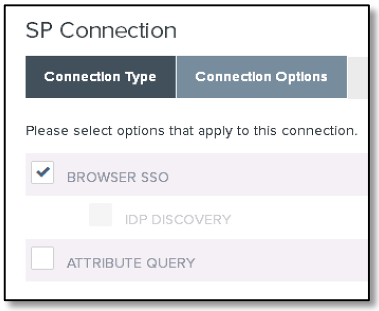
Step 9 Under Connection Type, Click **Next**



Select the type of connection needed for this SP: Browser S
provisioning users/groups to an SP) or all.

CONNECTION TEMPLATE	No Template
☑ BROWSER SSO PROFILES	PROTOCOL SAML 2.0
□ WS-TRUST STS	
□ OUTBOUND PROVISIONING	

Step 10 Under Connection Options, Click **Next**



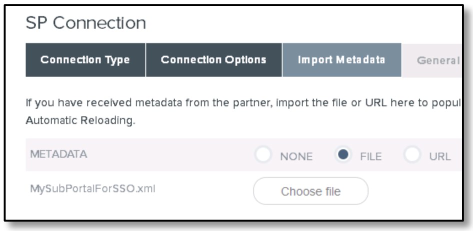
Please select options that apply to this connection.

☑ BROWSER SSO

□ IDP DISCOVERY

□ ATTRIBUTE QUERY

Step 11 Under Import Metadata, choose **File** and select the **MySubPortalForSSO.xml** this will be used to setup PingFederate for ISE SSO WebAuth Guest Portal as an SP, click **Next**



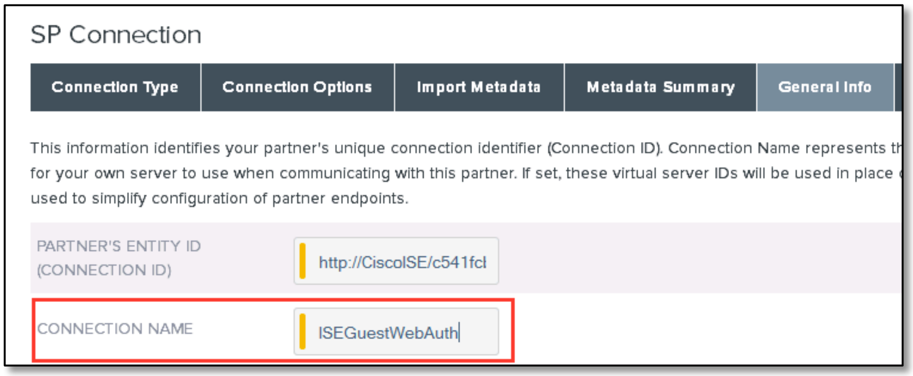
If you have received metadata from the partner, import the file or URL here to popul
Automatic Reloading.

METADATA ○ NONE ● FILE ○ URL

MySubPortalForSSO.xml

Step 12 On Metadata Summary page, click **Next**

Step 13 On the General info page, change the Connection Name to **ISEGuestWebAuth** and click **Next**



This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents th
for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place o
used to simplify configuration of partner endpoints.

PARTNER'S ENTITY ID (CONNECTION ID)	http://CiscoISE/c541fcl
CONNECTION NAME	ISEGuestWebAuth

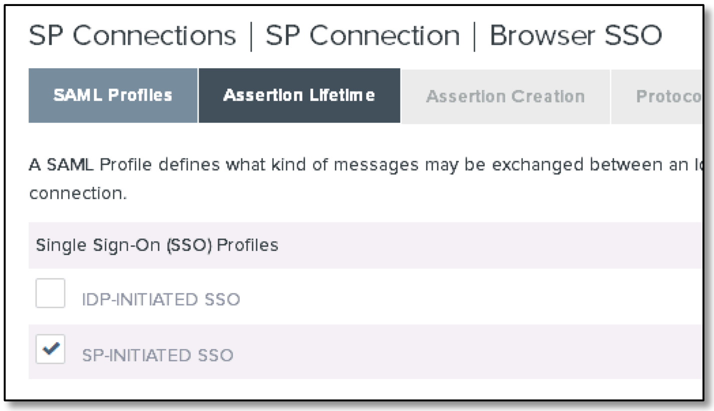
Step 14 Click **Configure Browser SSO**

Step 15 Under SAML Profiles check the following options:

a. Single Sign-On (SSO Profiles)

i. SP-INITIATED SSO

Note: Since the Guest Web Auth portal (SP) only initiates SSO to Ping that's the only check box we use here. For sponsor (and perhaps Certificate and My Devices) portal it would be different as these portals have sign out options.



SP Connections | SP Connection | Browser SSO

A SAML Profile defines what kind of messages may be exchanged between an Id connection.

Single Sign-On (SSO) Profiles

☐ IDP-INITIATED SSO

☑ SP-INITIATED SSO

Step 16 Click **Next**

Step 17 Under Assertion Lifetime click **Next**

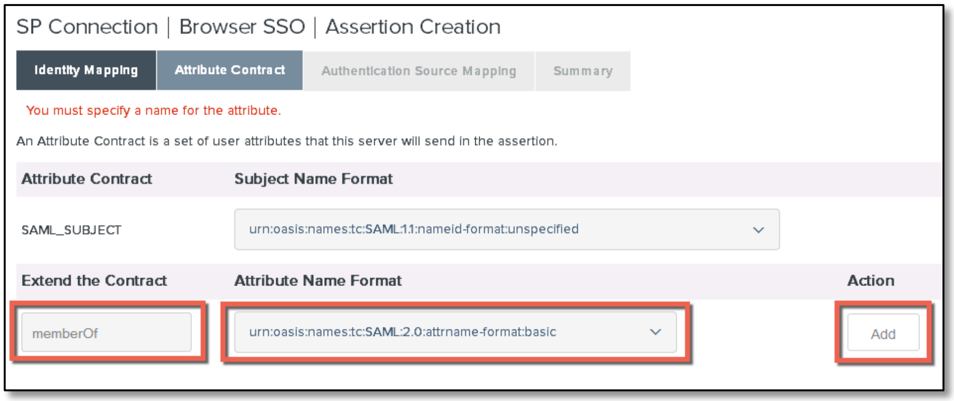
Step 18 Under Assertion Creation click **Configure Assertion Creation**

Step 19 Under Identity Mapping, click **Next**

Step 20 Under Attribute Contract > Extend the Contract

a. Enter **memberOf** with default Attribute Name Format and click **Add**

Note: This is needed to send back to ISE the group membership that can be used for the ISE authorization rules and differentiation of access depending on what user logged into the portal (Example: contractors vs employees). This is used where ISE will be needing user group information (Certificate Provisioning) and Sponsor Groups



SP Connection | Browser SSO | Assertion Creation

You must specify a name for the attribute.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

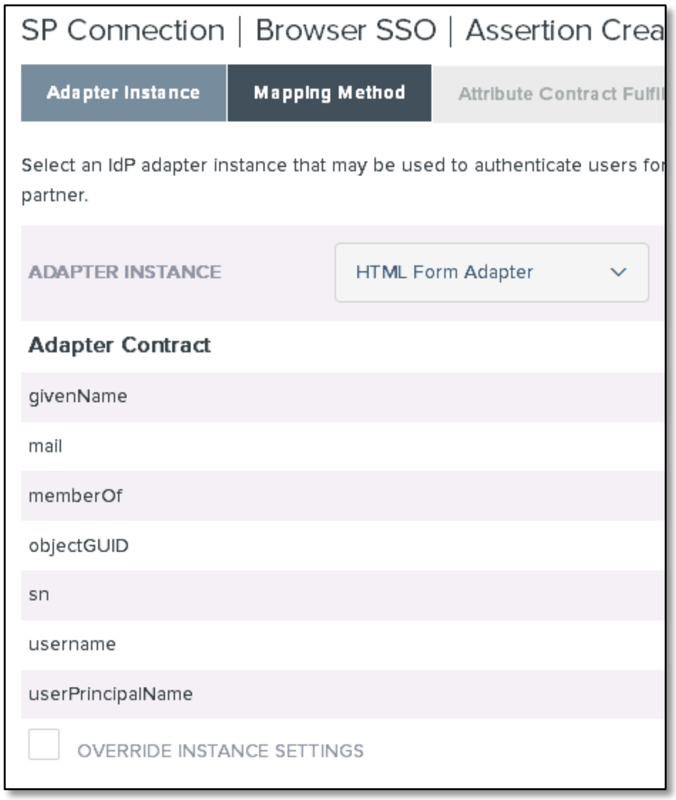
Attribute Contract	Subject Name Format	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	
Extend the Contract	**Attribute Name Format**	**Action**
memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

Step 21 Click **Add**

Step 22 Click **Next**

Step 23 Under Authentication Source Mapping, click **Map New Adapter Instance**

Step 24 Select **HTML Form Adapter**



SP Connection | Browser SSO | Assertion Crea

Select an IdP adapter instance that may be used to authenticate users fo partner.

ADAPTER INSTANCE: HTML Form Adapter

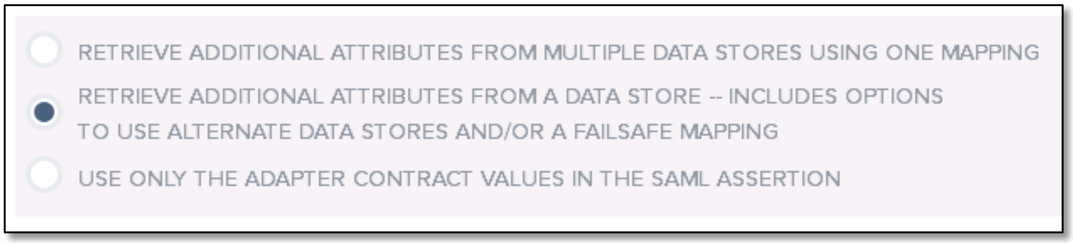
Adapter Contract

- givenName
- mail
- memberOf
- objectGUID
- sn
- username
- userPrincipalName

□ OVERRIDE INSTANCE SETTINGS

Step 25 Click **Next**

Step 26 Under Mapping Method choose the middle option at the bottom of the page



○ RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

● RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE -- INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

○ USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

Step 27 Click **Next**

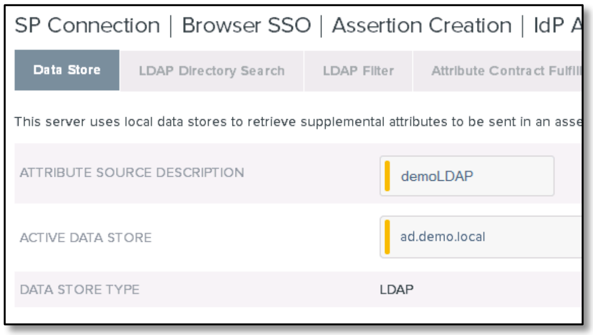
Step 28 Under Attribute Sources & User Lookup click **Add Attribute Source**

Step 29 Under Data Store enter the following:

a. Attribute Source Description: **demoLDAP**

b. Active Data Store: select **ad.demo.local**

Note: PingFederate is communicating with the AD/LDAP server environment in these flows. ISE does not communicate to AD directly.


SP Connection | Browser SSO | Assertion Creation | IdP A
Data Store
LDAP Directory Search
LDAP Filter
Attribute Contract Fulfil

This server uses local data stores to retrieve supplemental attributes to be sent in an asse

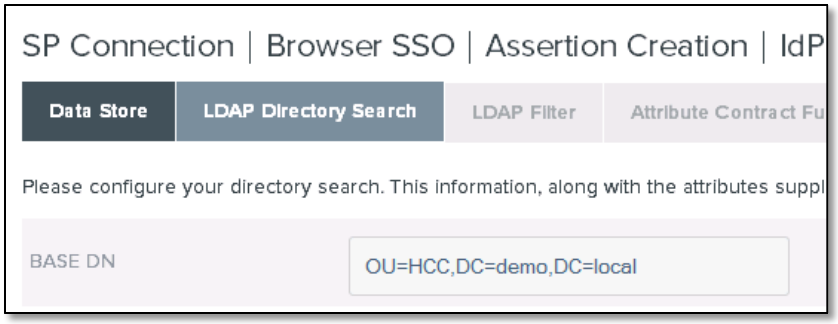
ATTRIBUTE SOURCE DESCRIPTION demoLDAP

ACTIVE DATA STORE ad.demo.local

DATA STORE TYPE LDAP

Step 30 Click **Next**

Step 31 Under LDAP Directory Search enter the Base DN as **OU=HCC,DC=demo,DC=local**

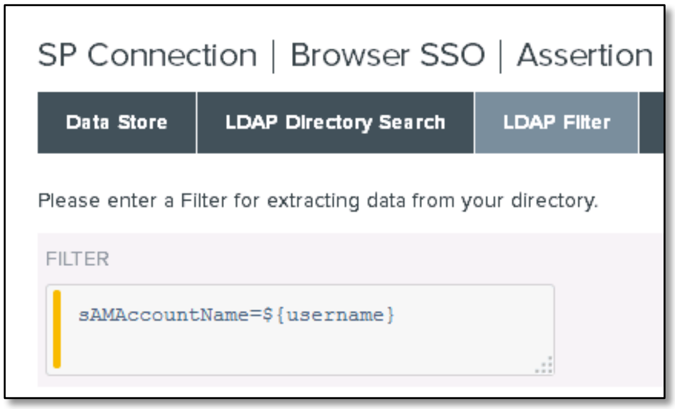


Please configure your directory search. This information, along with the attributes suppl

BASE DN OU=HCC,DC=demo,DC=local

Step 32 Click **Next**

Step 33 Under LDAP Filter, enter **sAMAccountName=${username}**



Please enter a Filter for extracting data from your directory.

FILTER

```
sAMAccountName=${username}
```

Step 34 Click **Next**

Step 35 Under **Attribute Contract Fulfillment**

a. Enter the following for Attribute Contract - SAML_SUBJECT:

   i. Source: **Adapter**

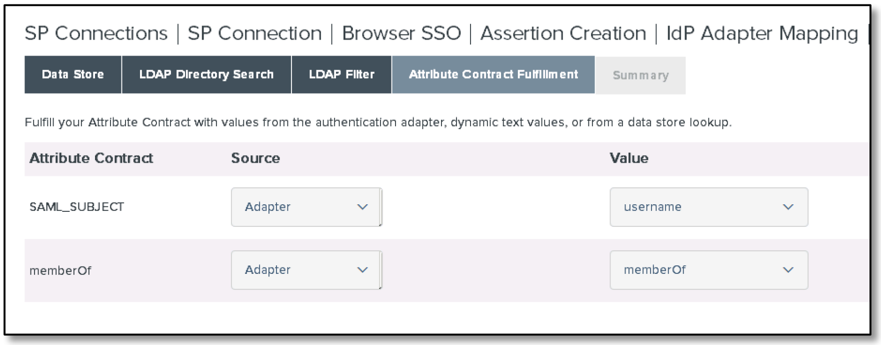
   ii. Value: **username**

b. Enter the following for Attribute Contract – memberOf:

   i. Source: **Adapter**

   ii. Value: **memberOf**

Note: Like the settings before, you will need the memberOf information to be able to use the solution. This is also needed for Sponsor, My Devices and Certificate Provisioning.



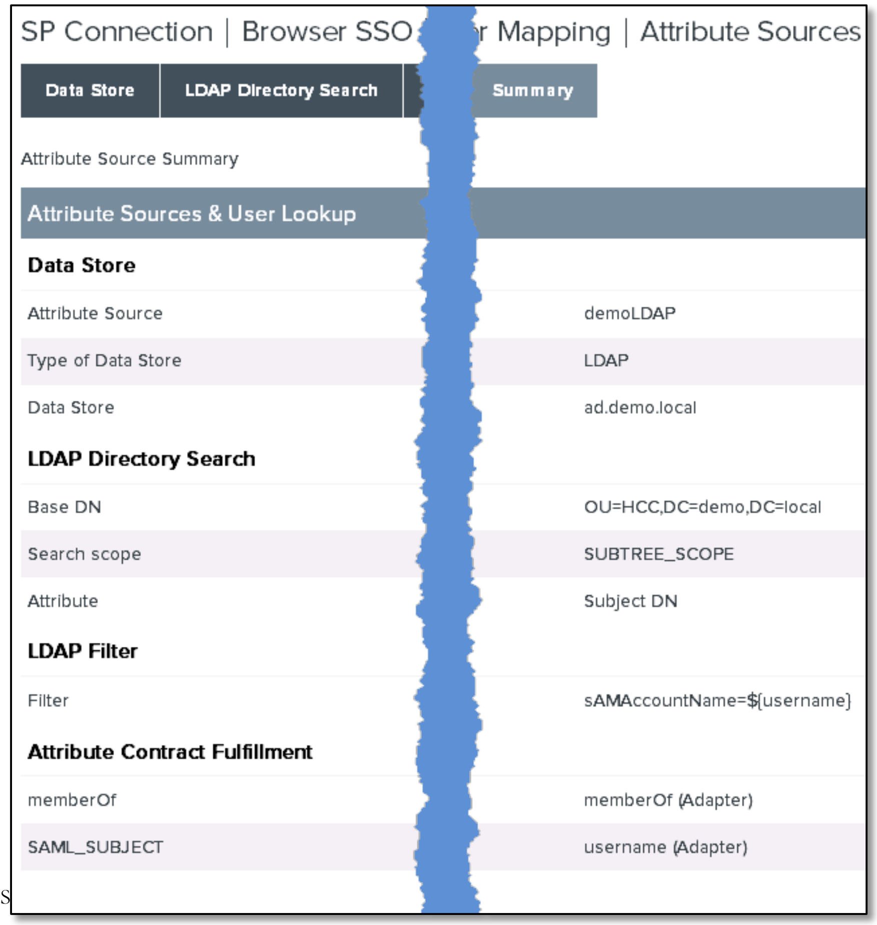
SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping |

Fulfill your Attribute Contract with values from the authentication adapter, dynamic text values, or from a data store lookup.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
memberOf	Adapter	memberOf

Step 36 Click **Next**

Step 37 Validate **Summary**



SP Connection | Browser SSO r Mapping | Attribute Sources

Attribute Source Summary

Attribute Sources & User Lookup

Data Store	
Attribute Source	demoLDAP
Type of Data Store	LDAP
Data Store	ad.demo.local
LDAP Directory Search	
Base DN	OU=HCC,DC=demo,DC=local
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
LDAP Filter	
Filter	sAMAccountName=${username}
Attribute Contract Fulfillment	
memberOf	memberOf (Adapter)
SAML_SUBJECT	username (Adapter)

Step 38 Click **Done.**

Step 39 Under Attribute Sources & User Lookup, click **Next**

Step 40 Under Failsafe Attribute Source, click **Next**

Step 41 Under Attribute Contract Fulfillment select the following:

a. For Attribute Contract: **SAML_SUBJECT**

   i. Source: **Adapter**

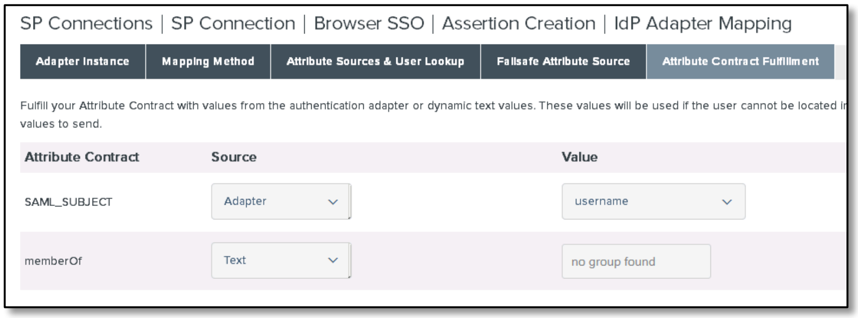
   ii. Value: **username**

b. For Attribute Contract: **memberOf**

   i. Source: **Text**

   ii. Value: **no group found**

Note: Like the settings before, you will need the memberOf information to be able to use the solution. This is also needed for Sponsor, My Devices and Certificate Provisioning

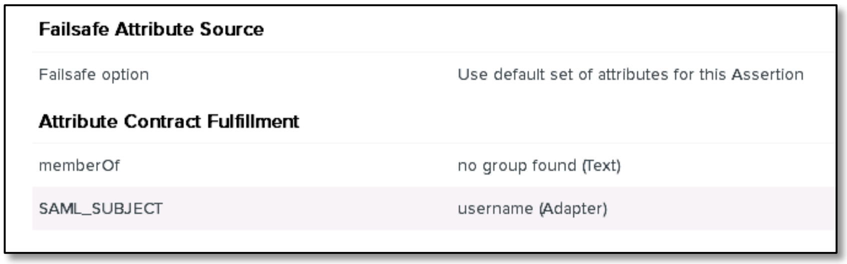

SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping
Adapter Instance
Mapping Method
Attribute Sources & User Lookup
Failsafe Attribute Source
Attribute Contract Fulfillment

Fulfill your Attribute Contract with values from the authentication adapter or dynamic text values. These values will be used if the user cannot be located i
values to send.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
memberOf	Text	no group found

Step 42 Click **Next**

Step 43 Validate **Summary (this is the info different from prior summary)**



Failsafe Attribute Source

Failsafe option	Use default set of attributes for this Assertion

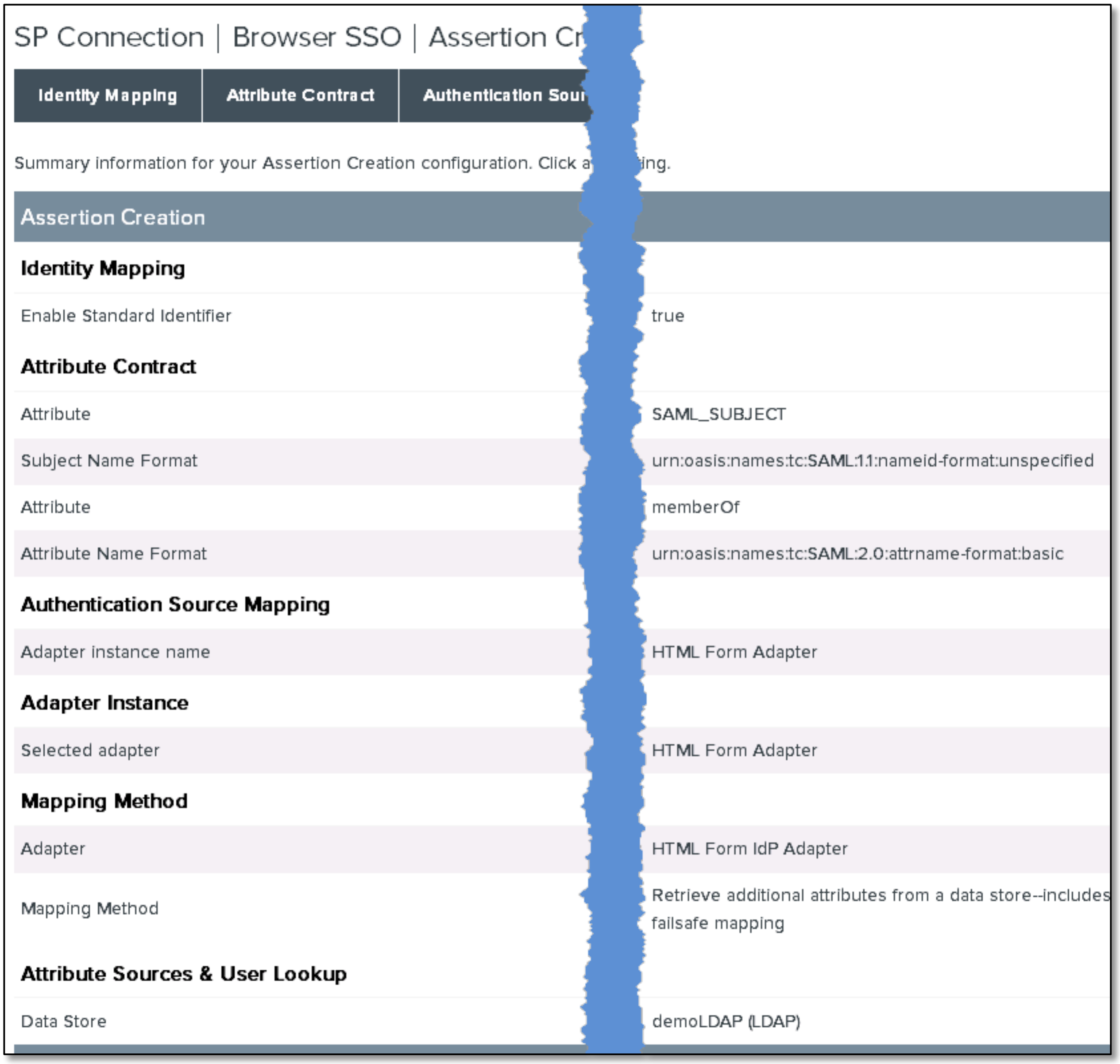
Attribute Contract Fulfillment

memberOf	no group found (Text)
SAML_SUBJECT	username (Adapter)

Step 44 Click **Done**

Step 45 Under Authentication Source Mapping, Click **Next**

Step 46 Validate **Summary (showing only the Assertion Creation section)**



SP Connection | Browser SSO | Assertion Cr

Summary information for your Assertion Creation configuration. Click a ing.

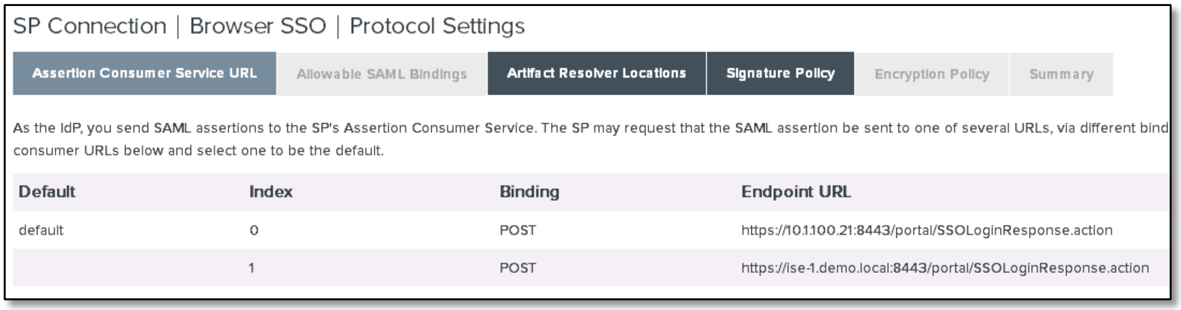
Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	memberOf
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	HTML Form Adapter
Adapter Instance	
Selected adapter	HTML Form Adapter
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Retrieve additional attributes from a data store--includes failsafe mapping
Attribute Sources & User Lookup	
Data Store	demoLDAP (LDAP)

Step 47 Click **Done**

Step 48 Under Assertion Creation, click **Next**

Step 49 Under Protocol Settings, click **Configure Protocol Settings**

Note: Under Assertion Consumer Service URL there should be 2 entries already populated. These are the referrer URLs that refer SSO events from ISE SP to the IdP. If they are not listed then you took too long and the system time out. Cancel out of this config, close browser tab, logout and log back into ping to start over.

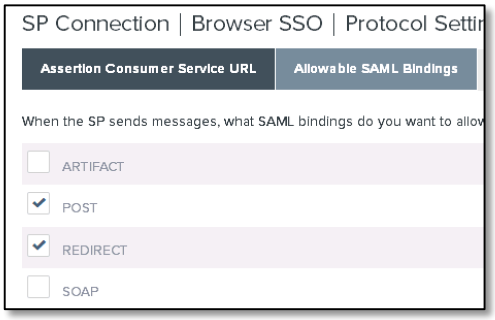

SP Connection | Browser SSO | Protocol Settings
Assertion Consumer Service URL
Allowable SAML Bindings
Artifact Resolver Locations
Signature Policy
Encryption Policy
Summary

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bind consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL
default	0	POST	https://10.1.100.21:8443/portal/SSOLoginResponse.action
	1	POST	https://ise-1.demo.local:8443/portal/SSOLoginResponse.action

Step 50 Click **Next**

Step 51 Under Allowable SAML Bindings, uncheck **ARTIFACT** and **SOAP**


SP Connection | Browser SSO | Protocol Setti
Assertion Consumer Service URL
Allowable SAML Bindings

When the SP sends messages, what SAML bindings do you want to allow

☐ ARTIFACT

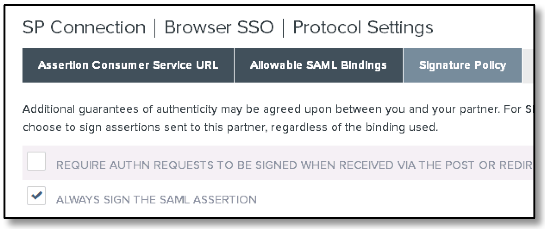
☑ POST

☑ REDIRECT

☐ SOAP

Step 52 Click **Next**

Step 53 Under Signature Policy click **Next**


SP Connection | Browser SSO | Protocol Settings
Assertion Consumer Service URL
Allowable SAML Bindings
Signature Policy

Additional guarantees of authenticity may be agreed upon between you and your partner. For S choose to sign assertions sent to this partner, regardless of the binding used.

☐ REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIR

☑ ALWAYS SIGN THE SAML ASSERTION

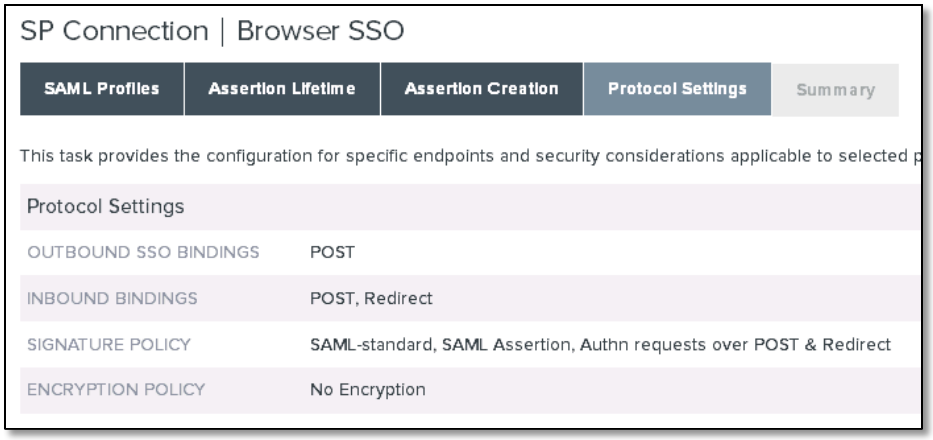
Step 54 Click **Next**

Step 55 Under Encryption Policy click **Next**

Step 56 Validate **Summary**

Step 57 Click **Done**

Step 58 Under Protocol Settings validate the settings



SP Connection | Browser SSO

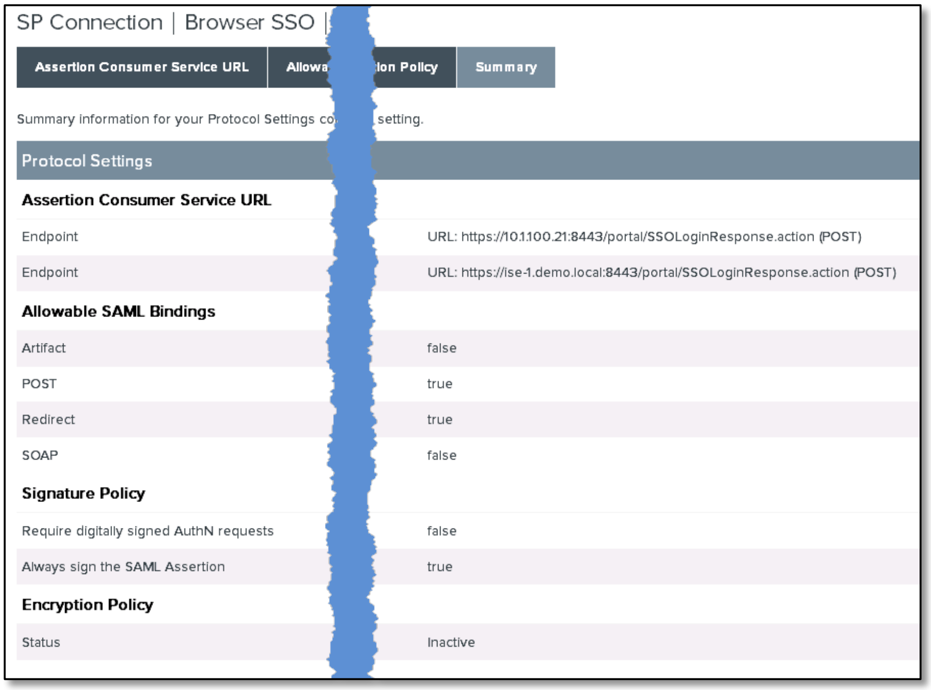
This task provides the configuration for specific endpoints and security considerations applicable to selected p

Protocol Settings

OUTBOUND SSO BINDINGS	POST
INBOUND BINDINGS	POST, Redirect
SIGNATURE POLICY	SAML-standard, SAML Assertion, Authn requests over POST & Redirect
ENCRYPTION POLICY	No Encryption

Step 59 Click **Next**

Step 60 Validate **Summary Page**



SP Connection | Browser SSO |

Summary information for your Protocol Settings co setting.

Protocol Settings

Assertion Consumer Service URL	
Endpoint	URL: https://10.1.100.21:8443/portal/SSOLoginResponse.action (POST)
Endpoint	URL: https://ise-1.demo.local:8443/portal/SSOLoginResponse.action (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always sign the SAML Assertion	true
Encryption Policy	
Status	Inactive

Step 61 Click **Done**

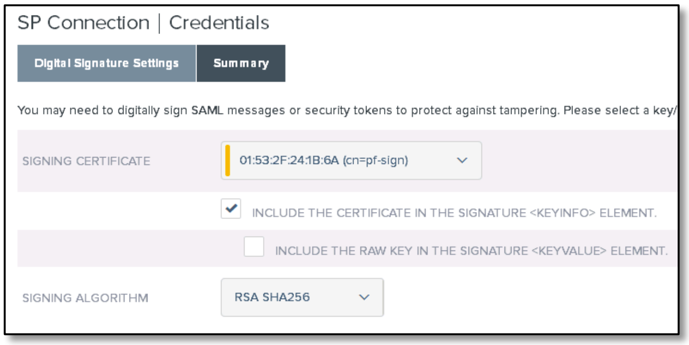
Step 62 Under Browser SSO click **Next**

Step 63 Under Credentials, click **Configure Credentials**

Step 64 Under Digital Signature Settings choose the following:

a. Choose Signing Certificate

b. Check **Include the certificate in the signature**



You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/

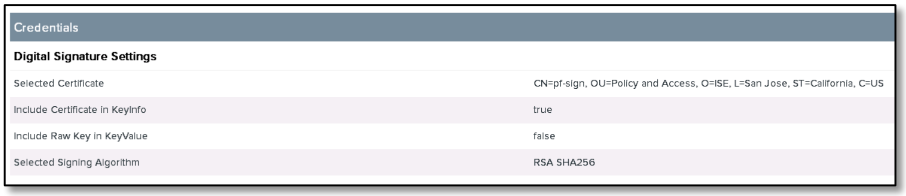
SIGNING CERTIFICATE: 01:53:2F:24:1B:6A (cn=pf-sign)

☑ INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

☐ INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM: RSA SHA256

Step 65 Click **Next** and Validate Summary

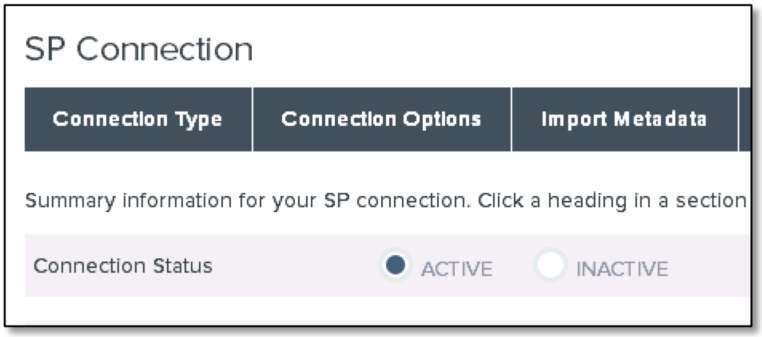


Credentials	
Digital Signature Settings	
Selected Certificate	CN=pf-sign, OU=Policy and Access, O=ISE, L=San Jose, ST=California, C=US
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	false
Selected Signing Algorithm	RSA SHA256

Step 66 Click **Done**

Step 67 Under Credentials Click **Next**

Step 68 Under Activation & Summary change Connection Status to **Active**



Summary information for your SP connection. Click a heading in a section

Connection Status ● ACTIVE ○ INACTIVE

Step 69 Scroll to the bottom and click **Save**

You have now completed configuration of the PingFederate IdP to use with the ISE SP Guest Web Auth Portal. The next exercise you will configure PingFederate for the ISE SP for the Sponsor Portal

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 1.3: Configure PingFederate IdP for ISE Sponsor Portal

Exercise Description

In this exercise you will go over the Ping Federated IdP configuration needed to work with ISE as an IdP. You will configure the necessary settings on PingFederate to work with the ISE Sponsor Portal SP.

Exercise Objective

In this exercise, your goal is to complete the following tasks to setup PingFederate to work with the Sponsor Portal:

- Configure PingFederate for the ISE Sponsor Portal SP

Exercise Steps

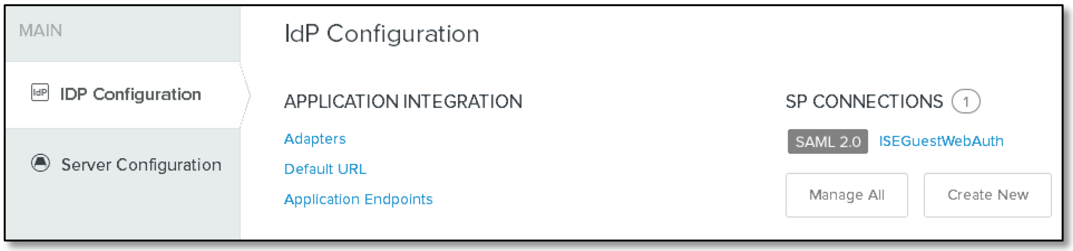
You will now configure the PingFederate IdP to use ISE SP Sponsor Portal.

Note: When going through these steps, don't let the page timeout, Ping doesn't like this and will cause you go to have to delete your config and start over as Ping doesn't save your settings well. You can try using Save Draft but I haven't had good luck with that.

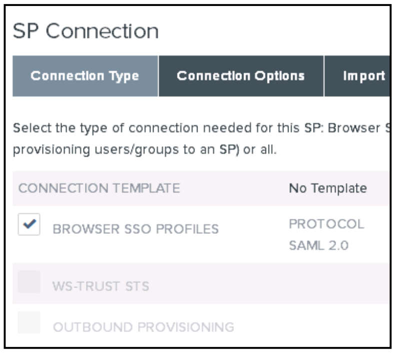
Step 1 From the Admin PC, launch **Firefox** to go to https://pf.demo.local:9999/pingfederate/app and login with **admin/ISEisC00L**

Step 2 Navigate to **IDP Configuration**

Step 3 Click **Create New**



Step 4 Under Connection Type, Click **Next**



SP Connection

Select the type of connection needed for this SP: Browser S
provisioning users/groups to an SP) or all.

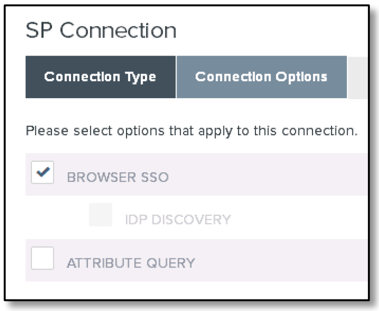
CONNECTION TEMPLATE No Template

☑ BROWSER SSO PROFILES PROTOCOL SAML 2.0

□ WS-TRUST STS

□ OUTBOUND PROVISIONING

Step 5 Under Connection Options, Click **Next**



SP Connection

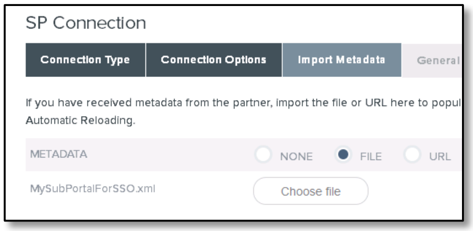
Please select options that apply to this connection.

☑ BROWSER SSO

□ IDP DISCOVERY

□ ATTRIBUTE QUERY

Step 6 Under Import Metadata, choose **File** and select the **Sponsor Portal (default).xml** this will be used to setup PingFederate for ISE SSO WebAuth Guest Portal as an SP, click **Next**



SP Connection

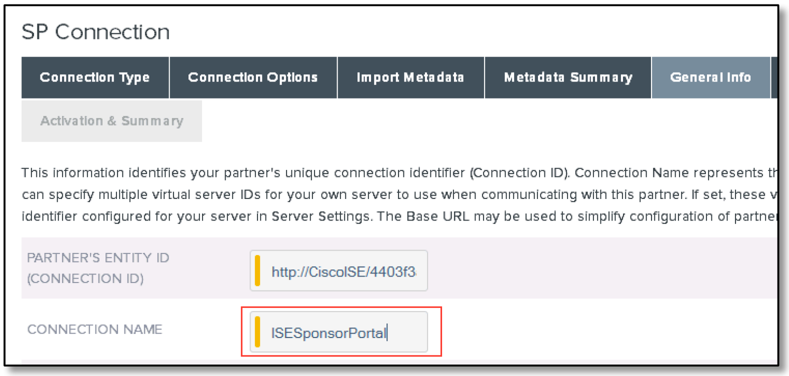
If you have received metadata from the partner, import the file or URL here to popul
Automatic Reloading.

METADATA ○ NONE ● FILE ○ URL

MySubPortalForSSO.xml

Step 7 Under Metadata Summary, click **next.**

Step 8 On the General info page, change the Connection Name to **ISESponsorPortal** and click **Next**



SP Connection

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents th
can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these v
identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partne

PARTNER'S ENTITY ID (CONNECTION ID): http://CiscoISE/4403f3

CONNECTION NAME: ISESponsorPortal

Step 9 Click **Configure Browser SSO**

Step 10 Under SAML Profiles check the following options:

a. Single Sign-On (SSO Profiles)

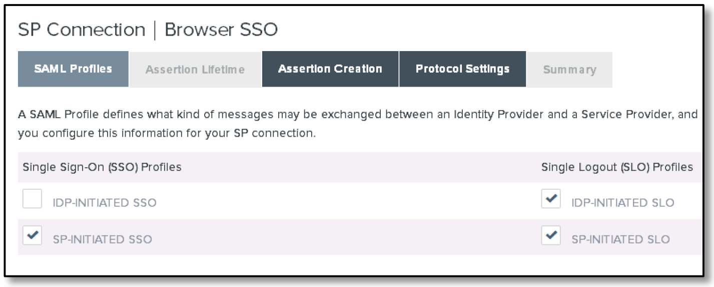
i. SP-INITIATED SSO

b. Single Logout (SLO) Profiles

i. IDP-INITIATED SLO

ii. SP-INITAITED SLO

Note: When you did this for the guest portal you only selected the first option (SP-INITIATED SSO). That's because the capabilities of the guest portal only allows SSO from the ISE SP. The guest portal also doesn't have logout capability. With the Sponsor portal it can initiate a logout. The same can be done from the IDP side of things. My Devices and Certificate Provisioning Portals can use this as well (if configured in the environment)



SP Connection | Browser SSO

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
□ IDP-INITIATED SSO	☑ IDP-INITIATED SLO
☑ SP-INITIATED SSO	☑ SP-INITIATED SLO

Step 11 Click **Next**

Step 12 Under Assertion Lifetime click **Next**

Step 13 Under Assertion Creation click **Configure Assertion Creation**

Step 14 Under Identity Mapping, click **Next**

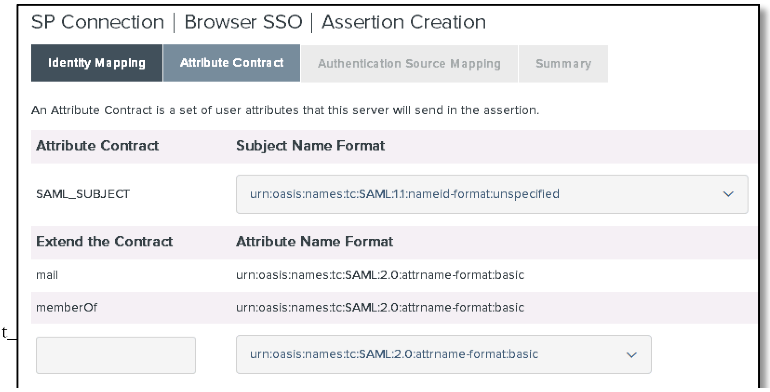
Step 15 Under Attribute Contract > Extend the Contract

a. Enter **memberOf** with default Attribute Name Format and click **Add (DON'T MISS IT!)**

Note: This is needed to send back to the ISE Sponsor Portal the group member info. This is used to configure Sponsor group mappings. This can also be used with the Certificate Provisioning Portal

b. Enter **mail** with default Attribute Name Format and click **Add (DON'T MISS IT!)**

Note: This is needed to send back to the ISE Sponsor Portal the email address information, which is used for filtering of the Pending Approvals list for self-registered guests



SP Connection | Browser SSO | Assertion Creation

An Attribute Contract is a set of user attributes that this server will send in the assertion.

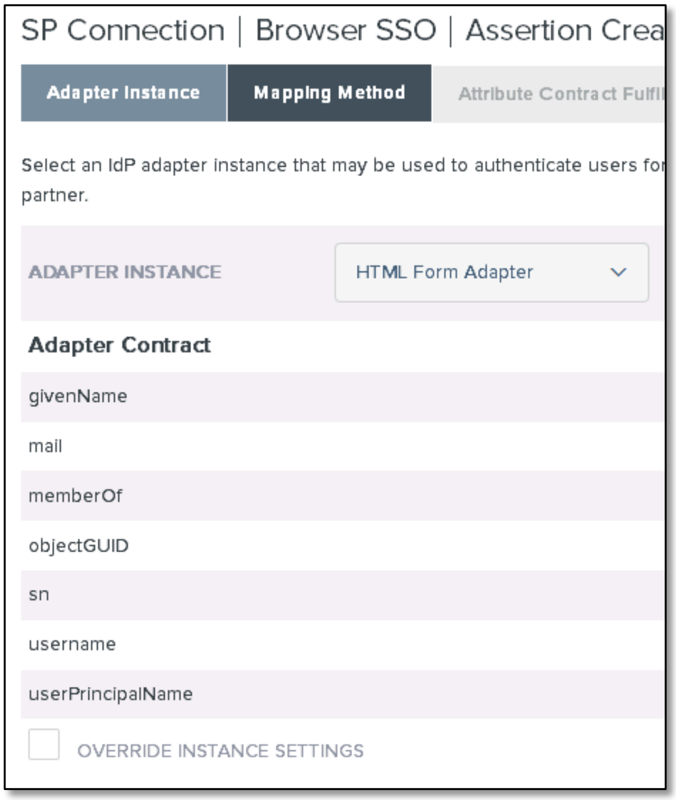
Attribute Contract	Subject Name Format
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Extend the Contract	Attribute Name Format
mail	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic

Step 16 Click **Next**

Step 17 Under Authentication Source Mapping, click **Map New Adapter Instance**

Step 18 Select **HTML Form Adapter**



SP Connection | Browser SSO | Assertion Crea

Select an IdP adapter instance that may be used to authenticate users fo
partner.

ADAPTER INSTANCE: HTML Form Adapter

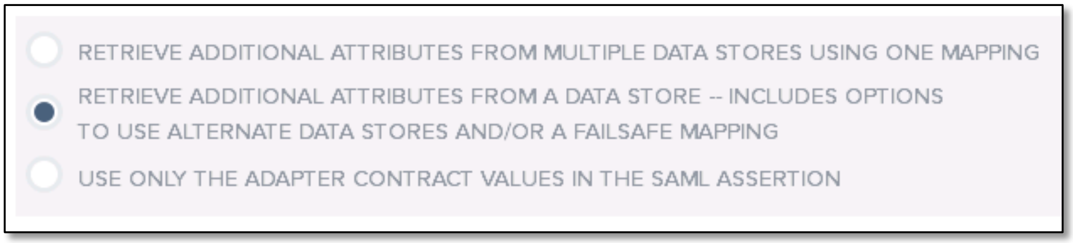
Adapter Contract

- givenName
- mail
- memberOf
- objectGUID
- sn
- username
- userPrincipalName

□ OVERRIDE INSTANCE SETTINGS

Step 19 Click **Next**

Step 20 Under Mapping Method choose the middle option at the bottom of the page



○ RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

● RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE -- INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

○ USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

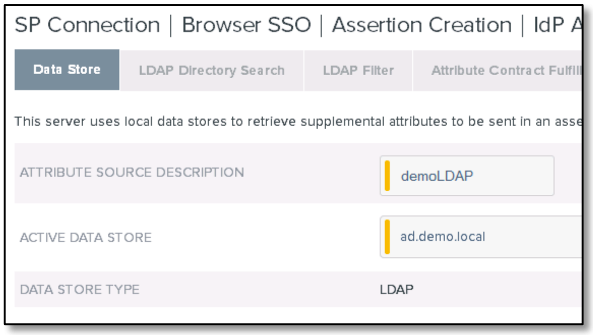
Step 21 Click **Next**

Step 22 Under Attribute Sources & User Lookup click **Add Attribute Source**

Step 23 Under Data Store enter the following:

a. Attribute Source Description: **demoLDAP**

b. Active Data Store: select **ad.demo.local**


SP Connection | Browser SSO | Assertion Creation | IdP A

This server uses local data stores to retrieve supplemental attributes to be sent in an asse

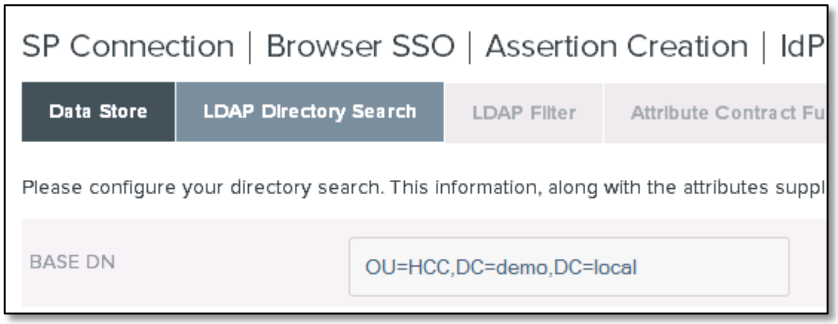
ATTRIBUTE SOURCE DESCRIPTION demoLDAP

ACTIVE DATA STORE ad.demo.local

DATA STORE TYPE LDAP

Step 24 Click **Next**

Step 25 Under LDAP Directory Search enter the Base DN as **OU=HCC,DC=demo,DC=local**

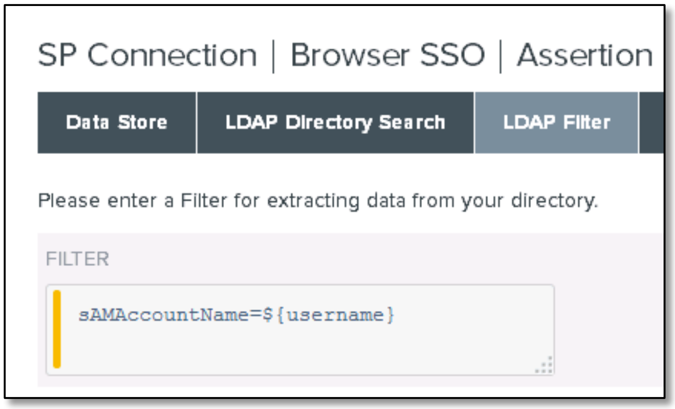

SP Connection | Browser SSO | Assertion Creation | IdP

Please configure your directory search. This information, along with the attributes suppl

BASE DN OU=HCC,DC=demo,DC=local

Step 26 Click **Next**

Step 27 Under LDAP Filter, enter **sAMAccountName=${username}**


SP Connection | Browser SSO | Assertion

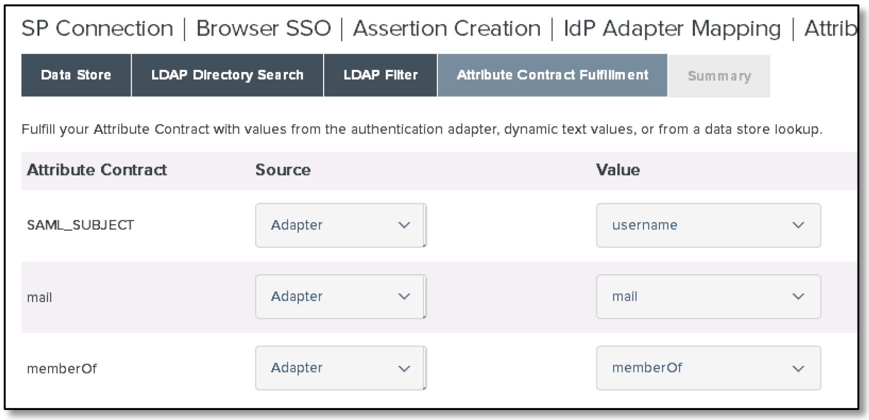
Please enter a Filter for extracting data from your directory.

FILTER

sAMAccountName=${username}

Step 28 Click **Next**

Step 29 Under **Attribute Contract Fulfillment choose the following options:**

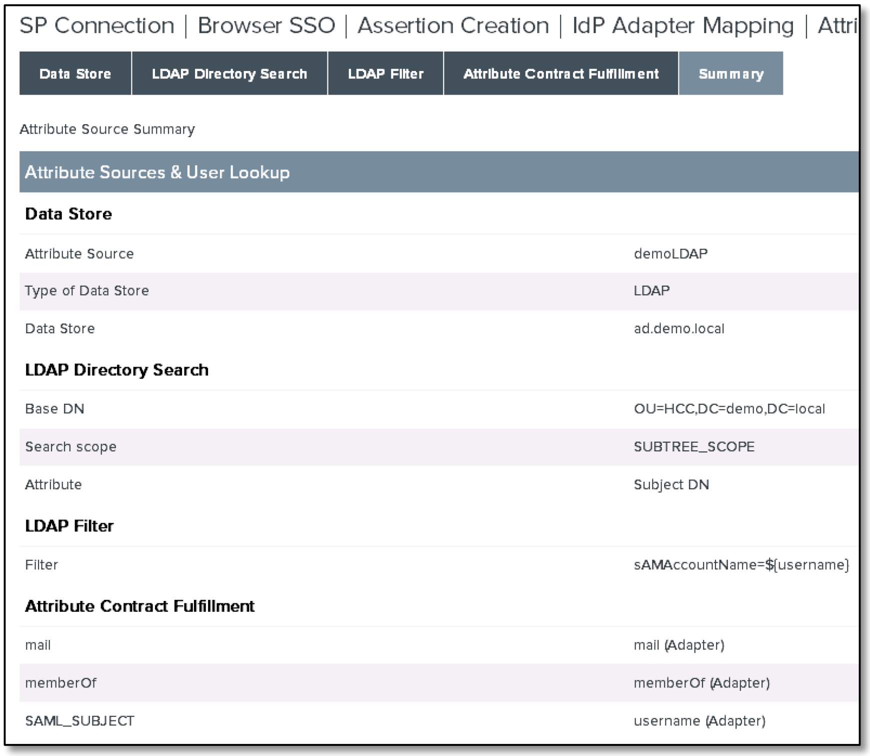

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attrib
Data Store
LDAP Directory Search
LDAP Filter
Attribute Contract Fulfillment
Summary

Fulfill your Attribute Contract with values from the authentication adapter, dynamic text values, or from a data store lookup.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
mail	Adapter	mail
memberOf	Adapter	memberOf

Step 30 Click **Next**

Step 31 Validate **Summary**


SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attri
Data Store
LDAP Directory Search
LDAP Filter
Attribute Contract Fulfillment
Summary

Attribute Source Summary

Attribute Sources & User Lookup	
Data Store	
Attribute Source	demoLDAP
Type of Data Store	LDAP
Data Store	ad.demo.local
LDAP Directory Search	
Base DN	OU=HCC,DC=demo,DC=local
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
LDAP Filter	
Filter	sAMAccountName=${username}
Attribute Contract Fulfillment	
mail	mail (Adapter)
memberOf	memberOf (Adapter)
SAML_SUBJECT	username (Adapter)

Step 32 Click **Done.**

Step 33 Under Attribute Sources & User Lookup, click **Next**

Step 34 Under Failsafe Attribute Source, click **Next**

Step 35 Under Attribute Contract Fulfillment select the following:

a. For Attribute Contract: **SAML_SUBJECT**

  i. Source: **Adapter**

    ii. Value: **username**

b. For Attribute Contract: **mail**

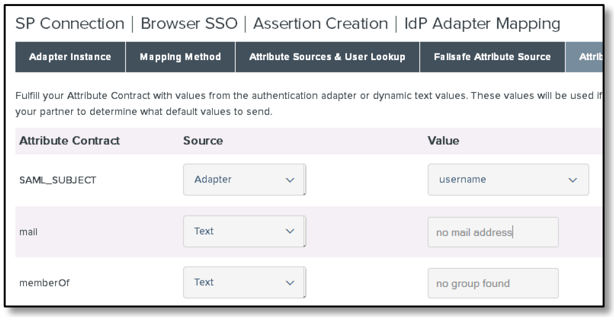
    i. Source: **Text**

    ii. Value: **no mail address**

c. For Attribute Contract: **memberOf**

    i. Source: **Text**

    ii. Value: no group found

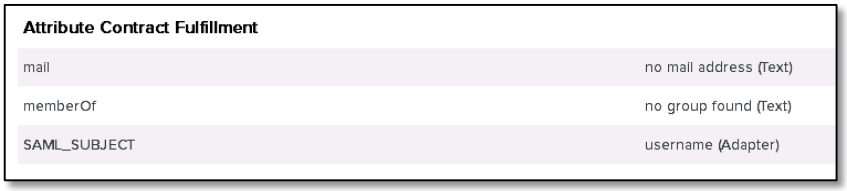

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping
Adapter Instance
Mapping Method
Attribute Sources & User Lookup
Failsafe Attribute Source
Attrib

Fulfill your Attribute Contract with values from the authentication adapter or dynamic text values. These values will be used if your partner to determine what default values to send.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
mail	Text	no mail address
memberOf	Text	no group found

Step 36 Click **Next**

Step 37 Validate **Summary (this is the info different form prior summary)**



Attribute Contract Fulfillment

mail	no mail address (Text)
memberOf	no group found (Text)
SAML_SUBJECT	username (Adapter)

Step 38 Click **Done**

Step 39 Under Authentication Source Mapping, Click **Next**

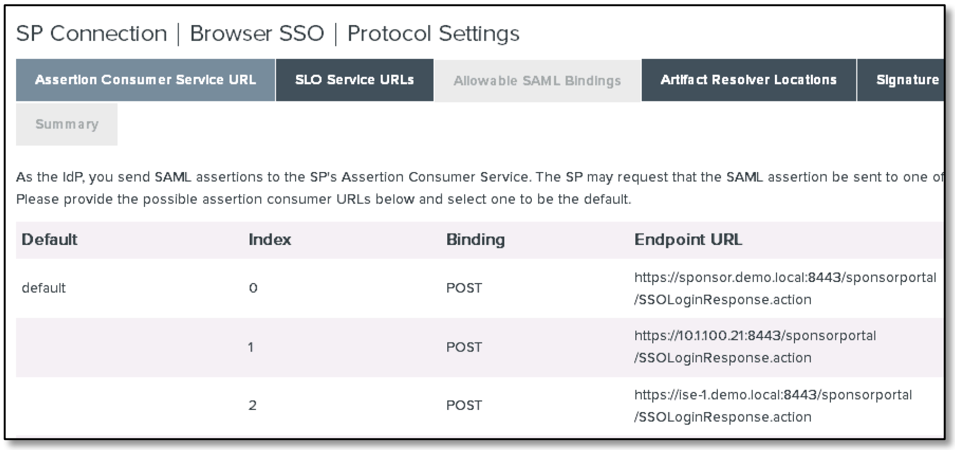
Step 40 Validate **Summary**

Step 41 Click **Done**

Step 42 Under Assertion Creation, click **Next**

Step 43 Under Protocol Settings, click **Configure Protocol Settings.**

Note: Under Assertion Consumer Service URL there should be 3 entries already populated. These are the referrer URLs that refer SSO events from ISE SP to the IdP. Notice the sponsor.demo.local (this is the Easy URL FQDN you configured under the Sponsor Portal Settings (if this is missing then you will need to go back to the step for that and add it back in, then change the portal to use the Sponsor sequence, save it, go back into the portal settings and change it back to use Ping, save it and then re-export the Metadata for ISE as this URL is contained in that file. If you are missing all 3 then cancel out of this config, close the browser tab, logout and log back into ping to start over.

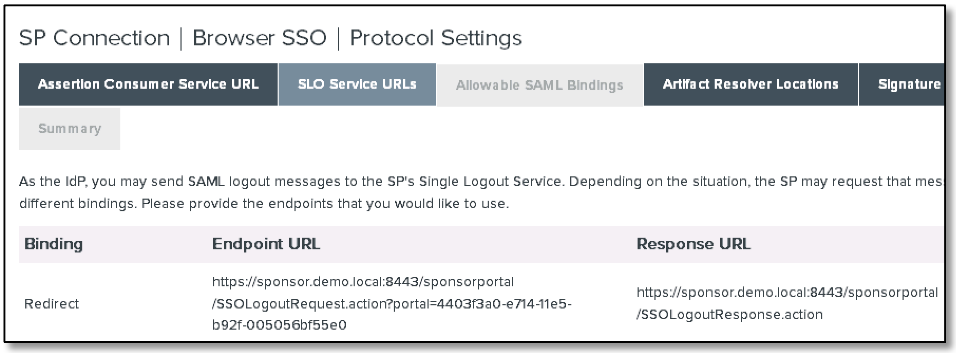

SP Connection | Browser SSO | Protocol Settings
Assertion Consumer Service URL
SLO Service URLs
Allowable SAML Bindings
Artifact Resolver Locations
Signature
Summary

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of
Please provide the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL
default	0	POST	https://sponsor.demo.local:8443/sponsorportal/SSOLoginResponse.action
	1	POST	https://10.1.100.21:8443/sponsorportal/SSOLoginResponse.action
	2	POST	https://ise-1.demo.local:8443/sponsorportal/SSOLoginResponse.action

Step 44 Click **Next**

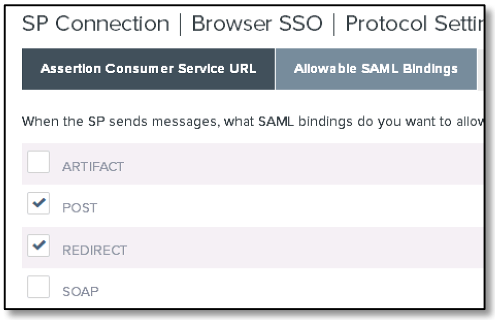
Step 45 Under **SLO Service URLs** you will see 1 redirect, this is used for logout on the Sponsor Portal, click **Next**


SP Connection | Browser SSO | Protocol Settings
Assertion Consumer Service URL
SLO Service URLs
Allowable SAML Bindings
Artifact Resolver Locations
Signature
Summary

As the IdP, you may send SAML logout messages to the SP's Single Logout Service. Depending on the situation, the SP may request that mes
different bindings. Please provide the endpoints that you would like to use.

Binding	Endpoint URL	Response URL
Redirect	https://sponsor.demo.local:8443/sponsorportal/SSOLogoutRequest.action?portal=4403f3a0-e714-11e5-b92f-005056bf55e0	https://sponsor.demo.local:8443/sponsorportal/SSOLogoutResponse.action

Step 46 Under Allowable SAML Bindings, uncheck **ARTIFACT** and **SOAP**


SP Connection | Browser SSO | Protocol Setti
Assertion Consumer Service URL
Allowable SAML Bindings

When the SP sends messages, what SAML bindings do you want to allow

□ ARTIFACT

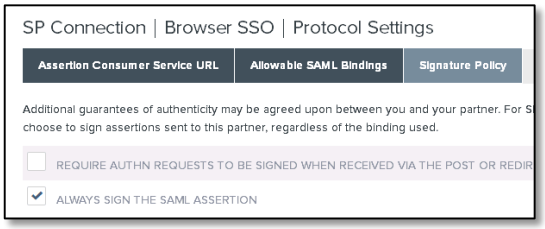
☑ POST

☑ REDIRECT

□ SOAP

Step 47 Click **Next**

Step 48 Under Signature Policy click **Next**


SP Connection | Browser SSO | Protocol Settings

Additional guarantees of authenticity may be agreed upon between you and your partner. For S choose to sign assertions sent to this partner, regardless of the binding used.

□ REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIR

☑ ALWAYS SIGN THE SAML ASSERTION

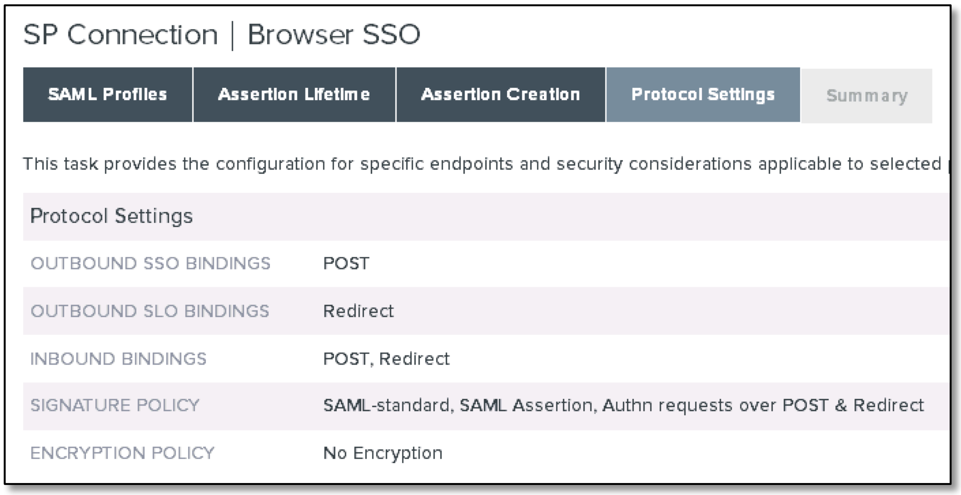
Step 49 Click **Next**

Step 50 Under Encryption Policy click **Next**

Step 51 Validate **Summary**

Step 52 Click **Done**

Step 53 Under Protocol Settings **validate the settings** and click **Next**


SP Connection | Browser SSO

This task provides the configuration for specific endpoints and security considerations applicable to selected

Protocol Settings

OUTBOUND SSO BINDINGS	POST
OUTBOUND SLO BINDINGS	Redirect
INBOUND BINDINGS	POST, Redirect
SIGNATURE POLICY	SAML-standard, SAML Assertion, Authn requests over POST & Redirect
ENCRYPTION POLICY	No Encryption

Step 54 Validate **Summary Page** and click **Done**

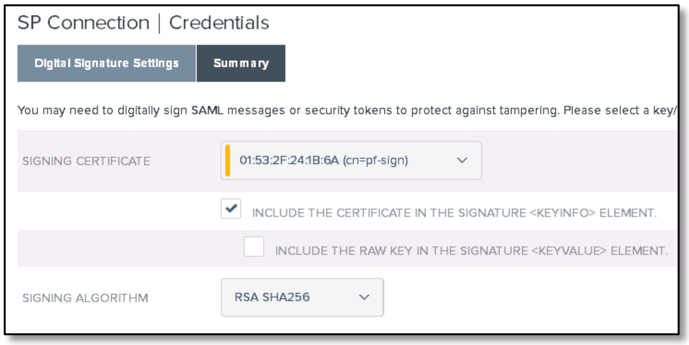
Step 55 Under Browser SSO click **Next**

Step 56 Under Credentials, click **Configure Credentials**

Step 57 Under Digital Signature Settings choose the following:

a. Choose Signing Certificate

b. Check **Include the certificate in the signature**



You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/

SIGNING CERTIFICATE 01:53:2F:24:1B:6A (cn=pf-sign)

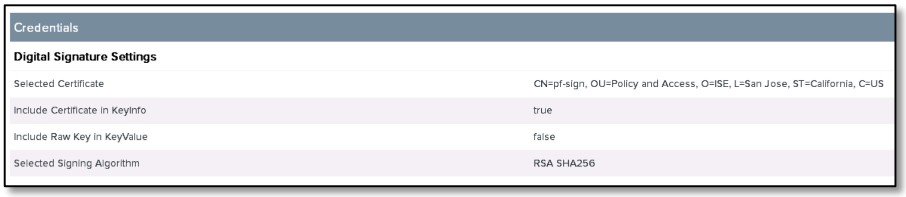
☑ INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

□ INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM RSA SHA256

Step 58 Click **Next**

Step 59 Validate Summary and click **Next**

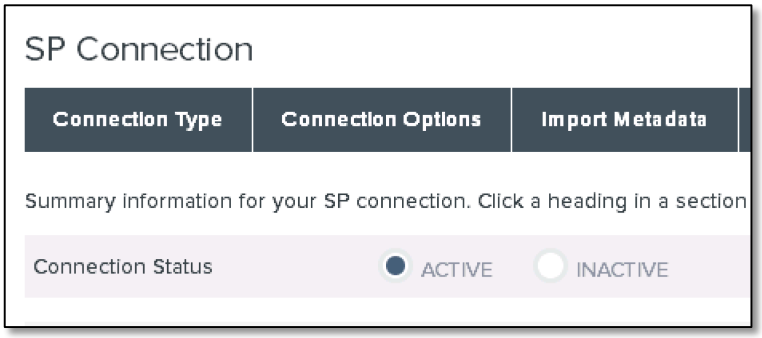


Credentials	
Digital Signature Settings	
Selected Certificate	CN=pf-sign, OU=Policy and Access, O=ISE, L=San Jose, ST=California, C=US
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	false
Selected Signing Algorithm	RSA SHA256

Step 60 Click **Done**

Step 61 Under Credentials Click **Next**

Step 62 Under Activation & Summary change Connection Status to **Active**



Summary information for your SP connection. Click a heading in a section

Connection Status ● ACTIVE ○ INACTIVE

Step 63 Scroll to the bottom and click **Save**

You have now completed configuration of the PingFederate IdP to use with the ISE SP Sponsor Portal.

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 1.3: Configure PingFederate IdP for ISE Sponsor Portal

Lab Exercise 1.4: Finalize configuration of ISE IdP and Sponsor settings

Exercise Description

In this exercise you will export the MetaData information from the Guest Webauth & Sponsor Portal SP configurations. Import the IdP information into ISE to work with the portals. Finalize the ISE IdP configuration for ISE and configure the sponsor portal for the IdP Groups.

Exercise Objective

In this exercise, your goal is to complete the following tasks to setup PingFederate to work ISE.

- Export metadata information from Ping
- Import metadata info into ISE for the portals
- Finalize the ISE IdP configuration for PingFederate
- Configure ISE sponsor portal for IdP Group Mappings.

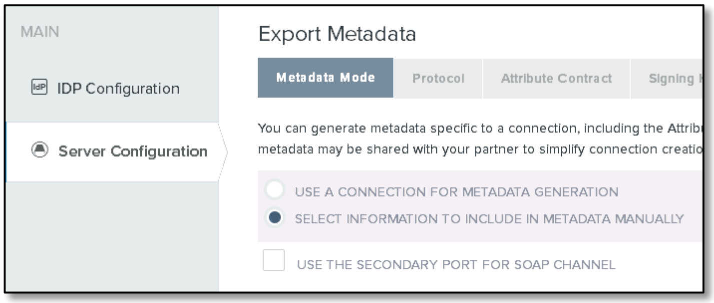
Exercise Steps

You will now export the Metadata information for the Guest Web Auth and Sponsor Portal SP configurations from Ping IdP to import onto ISE.

Step 1 From the Admin PC, launch **Firefox** to go to https://pf.demo.local:9999/pingfederate/app and login with **admin/ISEisC00L**

Step 2 On PingFederate, Navigate to **Server Configuration > Administrative Functions > Metadata Export**

Step 3 Under Metadata Mode, use **Select Information to include in metadata manually**



You can generate metadata specific to a connection, including the Attrib metadata may be shared with your partner to simplify connection creatio

○ USE A CONNECTION FOR METADATA GENERATION

● SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

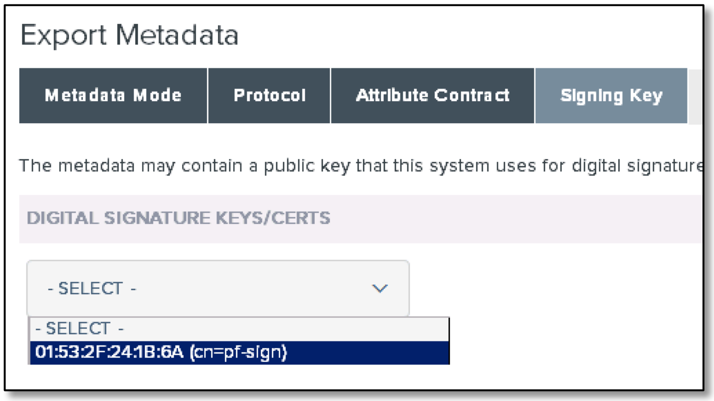
□ USE THE SECONDARY PORT FOR SOAP CHANNEL

Step 4 Click **Next**

Step 5 Under Protocol, click **Next**

Step 6 Under Attribute Contract, click **Next**

Step 7 Under **Signing Key,** select from the pull down



Export Metadata

The metadata may contain a public key that this system uses for digital signature

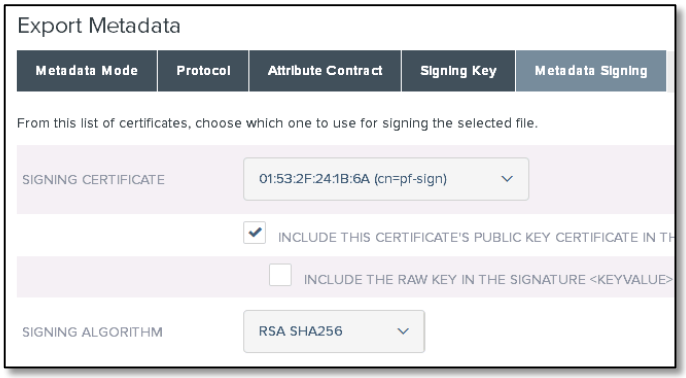
DIGITAL SIGNATURE KEYS/CERTS

- SELECT -

- SELECT -
01:53:2F:24:1B:6A (cn=pf-sign)

Step 8 Click **Next**

Step 9 Under Metadata Signing, select the **Signing Certificate** and **Include this Certificate Public Key**



Export Metadata

From this list of certificates, choose which one to use for signing the selected file.

SIGNING CERTIFICATE 01:53:2F:24:1B:6A (cn=pf-sign)

☑ INCLUDE THIS CERTIFICATE'S PUBLIC KEY CERTIFICATE IN TH

☐ INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE>

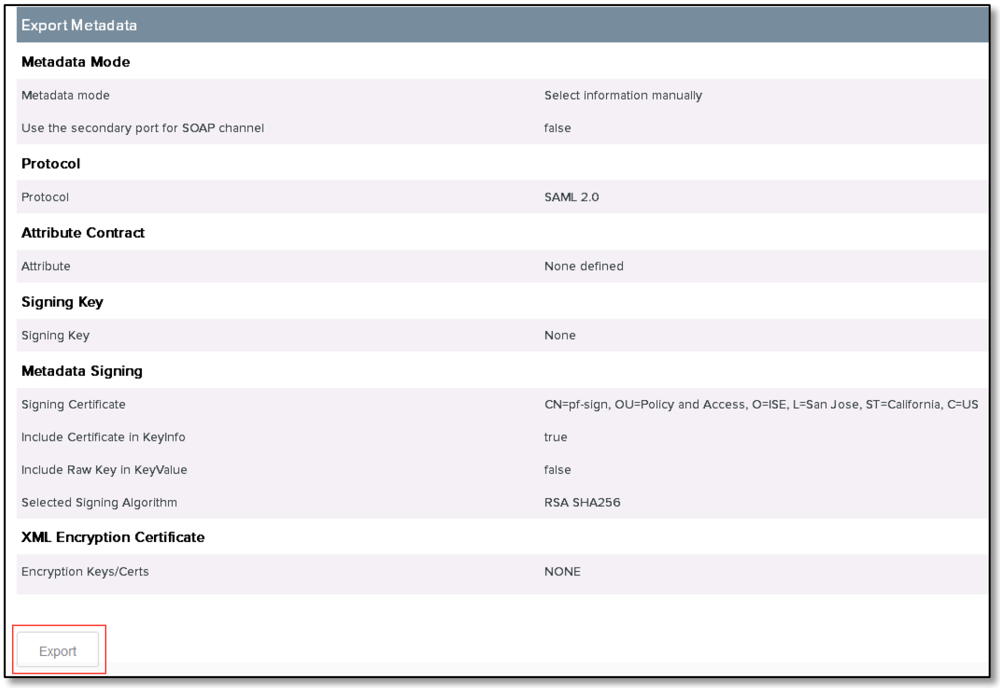
SIGNING ALGORITHM RSA SHA256

Step 10 Click **Next**

Step 11 Under **XML Encryption Certificate**, click **Next**

Step 12 Validate the **Summary Page**

Step 13 Click **Export** and save off the **Metadata.xml file**



Export Metadata

Metadata Mode

Metadata mode	Select information manually
Use the secondary port for SOAP channel	false

Protocol

Protocol	SAML 2.0

Attribute Contract

Attribute	None defined

Signing Key

Signing Key	None

Metadata Signing

Signing Certificate	CN=pf-sign, OU=Policy and Access, O=ISE, L=San Jose, ST=California, C=US
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	false
Selected Signing Algorithm	RSA SHA256

XML Encryption Certificate

Encryption Keys/Certs	NONE

Step 14 Click **Done**

Now that you have completed export of the metadata information on the IdP you will now import this information onto ISE and finalize the ISE IdP entry for PingFederate.

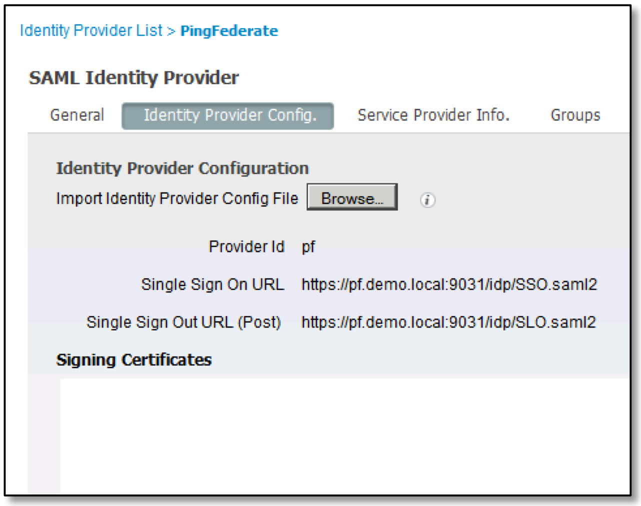
Step 15 Use **Firefox** to go to https://ise.demo.local and login with **admin/ISEisC00L**

Step 16 Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**

Step 17 Import the **IdP Metadata File**

a. Select **Identity Provider Config**

b. Click **Browse** and choose the **metadata.xml file you exported from Ping**



Identity Provider Configuration

Import Identity Provider Config File

Provider Id pf

Single Sign On URL https://pf.demo.local:9031/idp/SSO.saml2

Single Sign Out URL (Post) https://pf.demo.local:9031/idp/SLO.saml2

Signing Certificates

Step 18 Select the **Groups** tab, here you will configured the groups to use from Ping

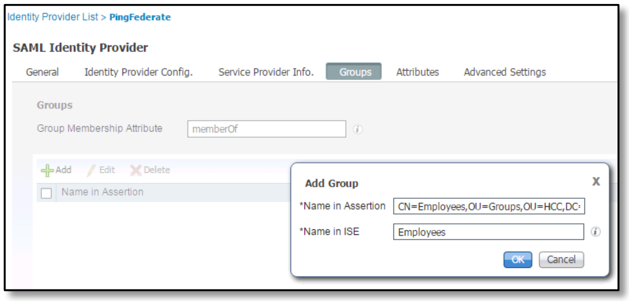
a. Enter Group Membership Attribute: **memberOf**

b. Click **Add**

   i. Name in Assertion: (value coming from SAML IdP) **CN=Employees,OU=Groups,OU=HCC,DC=demo,DC=local**

   ii. Name in ISE: **Employees**

c. Click **OK**



Groups

Group Membership Attribute: memberOf

*Name in Assertion: CN=Employees,OU=Groups,OU=HCC,DC·

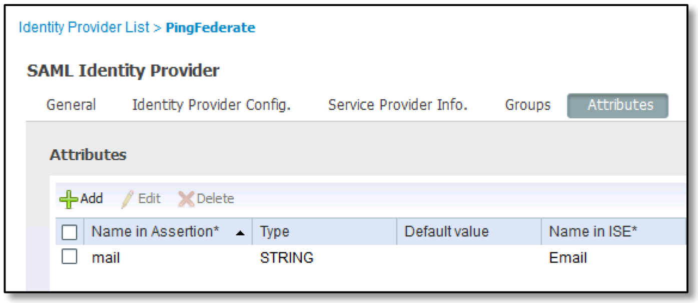
*Name in ISE: Employees

Step 19 Select the **Attributes** tab, here you will enter the info needed to receive email attribute from Ping users to use with the Sponsor Portal pending accounts filtered list.

a. Click **Add**

b. Enter Name in Assertion: **mail**, the other field for Name in ISE will fill automatically

c. Click **OK**



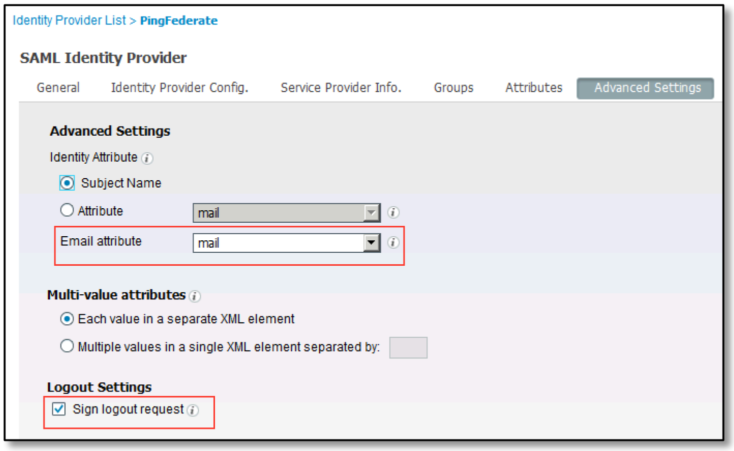
Attributes

□	Name in Assertion* ▲	Type	Default value	Name in ISE*
□	mail	STRING		Email

Step 20 Select the **Advanced Settings** Tab, this is where we map the email attribute and choose the Logout Settings

a. Under Identity Attribute choose Email attribute: **mail**

b. For Logout Settings check the box for **Sign logout request**



Identity Provider List > PingFederate

SAML Identity Provider

Advanced Settings

Identity Attribute

● Subject Name

○ Attribute mail

Email attribute mail

Multi-value attributes

● Each value in a separate XML element

○ Multiple values in a single XML element separated by:

Logout Settings

☑ Sign logout request

Step 21 Click **Save**

You have now completed configuration of the PingFederate IDP on ISE. Next you will configure your Sponsor Group settings for user groups and to filter your list of Pending accounts to only those destined to the specific sponsor.

Step 22 Navigate to **Work Centers > Guest Access > Configure > Sponsor Groups > ALL_ACCOUNTS**

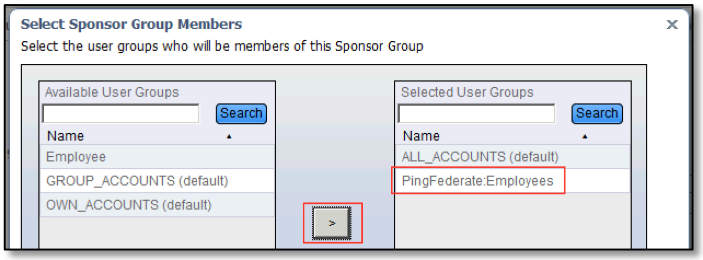
Step 23 Configure your Sponsor Group to work with the PingFederate Employee Groups

a. Click on **Members…**

b. From the Available User Groups, Select the **PingFederate:Employees**

c. Click the arrow to move the group to the Selected User Groups

d. Click **OK**



Select Sponsor Group Members

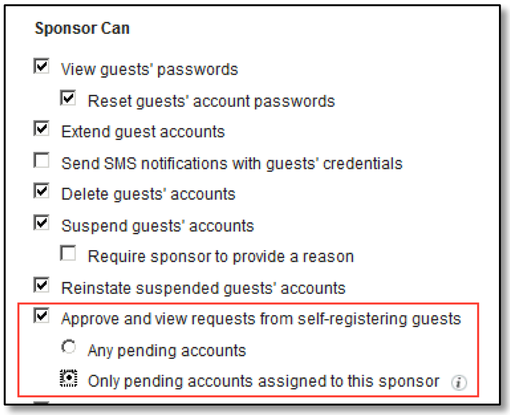
Select the user groups who will be members of this Sponsor Group

Available User Groups
Name
Employee
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Selected User Groups
Name
ALL_ACCOUNTS (default)
PingFederate:Employees

Next will configure the sponsor group to only see those self-registered guest pending accounts that are designated for them (the guest enters the sponsors email address under person being visited).

Step 24 Under the section for **Sponsor Can > Approve and view requests from self-registering guests** section check the box for **Only pending accounts assigned to this sponsor**



Sponsor Can

☑ View guests' passwords

☑ Reset guests' account passwords

☑ Extend guest accounts

□ Send SMS notifications with guests' credentials

☑ Delete guests' accounts

☑ Suspend guests' accounts

□ Require sponsor to provide a reason

☑ Reinstate suspended guests' accounts

☑ Approve and view requests from self-registering guests

○ Any pending accounts

● Only pending accounts assigned to this sponsor

Step 25 Click **Save** under the Sponsor Group

You have now finished setting up the ISE IdP and Sponsor Group settings. In the next exercise you will use the Guest and Sponsor Portals to see how they work the configured features.

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 1.5: Guest Web Auth & Sponsor Portal Usage with SAML SSO features

Exercise Description

Now that you have configured PingFederate and ISE for the settings needed to use SAML SSO with the ISE Guest Web Auth and Sponsor Portals. Plus configured the necessary settings in the sponsor portal and groups. You are ready to try out the SSO portal access and see the filtered pending accounts. In this exercise you will access the Guest Web Auth and Sponsor Portals using SSO, generate some self-registered guest accounts that require approval and then access the sponsor portal to see how the filtering options works.

In these tests we will be using the test portal URL for the guest portal as its not required to use a real client connection through a Network Access Device. This saves time and complexity on setup. If you're interested in trying real clients in guest flow this can be done in our general guest lab or through cisco dCloud.

Exercise Objective

In this exercise, your goal is to complete the following tasks to learn how the new portal and sponsor group options work.

- Access the Guest and Sponsor Portals using SAML
- Create self-registered accounts requiring approval
- Validate the pending approval filtering

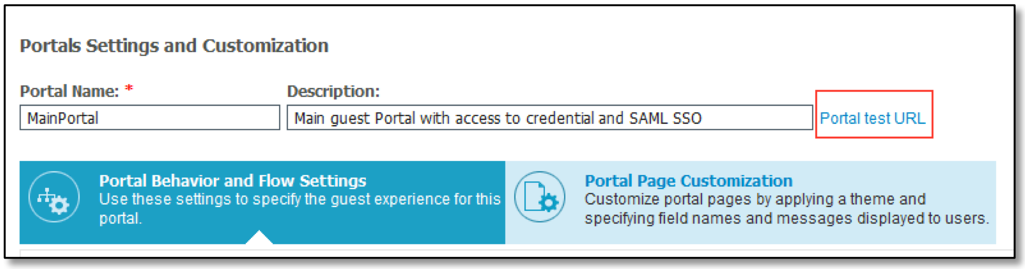
Exercise Steps

Access the guest portal using PingFederate SAML SSO.

Step 1 From the Admin PC, launch **Firefox** to go to https://ise-1.demo.local and login with **admin/ISEisC00L**

Step 2 Access the Guest Portal and test

a. Navigate to **Work Centers > Guest Access > Configure > Guest Portals**
b. Choose the **Main Portal** you created.
c. At the top of the screen click on the **Portal Test URL**



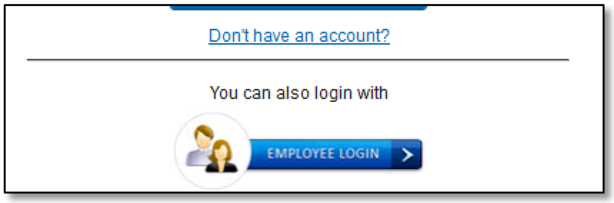
Portals Settings and Customization

Portal Name: * MainPortal

Description: Main guest Portal with access to credential and SAML SSO

Portal test URL
Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.
Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Note: A new browser window will launch. This portal gives you the option to login to the normal credentialed portal (with guest, internal or external users (AD/LDAP). It also includes a new option available at the bottom of the page, this button for Employee Login is linked to the additional portal you created that uses PingFederate as an authentication method.



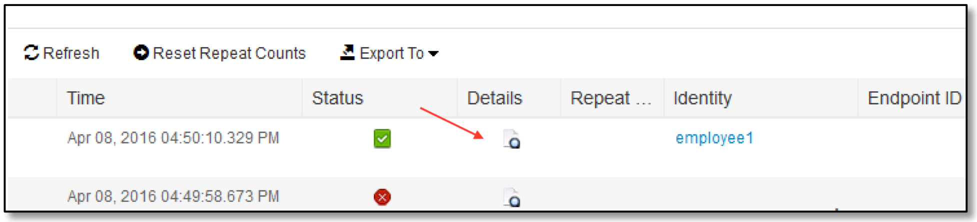
Don't have an account?

You can also login with

d. Click on the **employee login button** and you're redirected to a PingFederate portal, login with **employee1/ISEisC00L.**

e. Close the browser window and try the process again. You'll notice this time that you don't need to enter the credentials, you go directly to the success screen. This SSO token will now carry over to other ISE portals that the user is allowed access to with this authentication method.

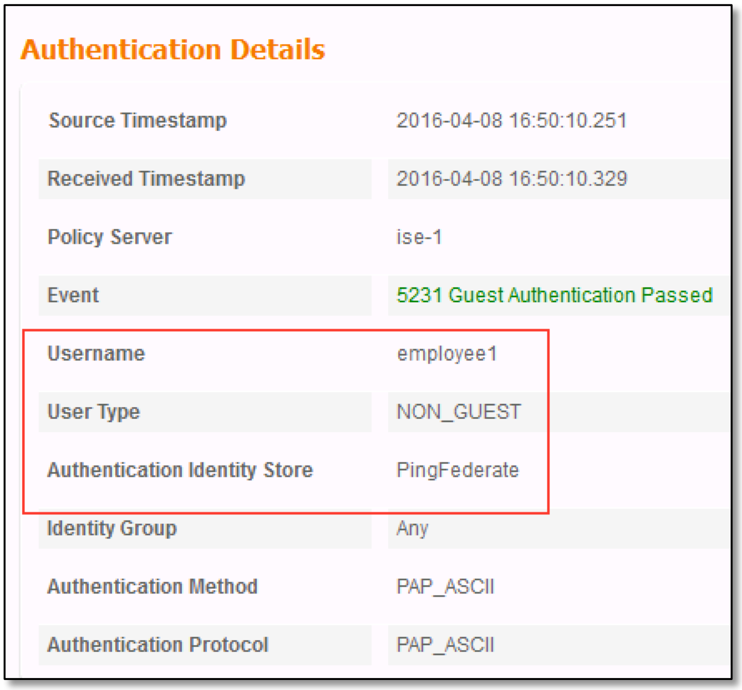
Step 3 Navigate to **Operations > RADIUS Live Log**



Time	Status	Details	Repeat ...	Identity	Endpoint ID
Apr 08, 2016 04:50:10.329 PM	✓	🔍		employee1	
Apr 08, 2016 04:49:58.673 PM	✗	🔍			

Note: Although we are not working with real client devices you can still see a RADIUS live log of your login to the portal. It missing information such as IP and MAC Address because there is no real client or authentication on a NAD.

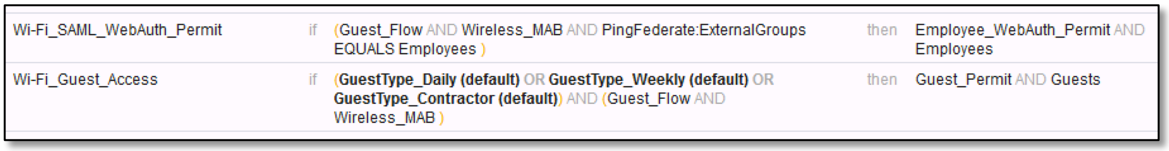
Step 4 Click on employee1 **details** and notice that the user is a NON_GUEST type of account coming from PingFederate



Authentication Details

Source Timestamp	2016-04-08 16:50:10.251
Received Timestamp	2016-04-08 16:50:10.329
Policy Server	ise-1
Event	5231 Guest Authentication Passed
Username	employee1
User Type	NON_GUEST
Authentication Identity Store	PingFederate
Identity Group	Any
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII

For your reference: An authorization policy that could used to differentiate access depending on the type of user hitting the Web Auth Portal. Notice how the PingFederated ID source can be chosen under other conditions.



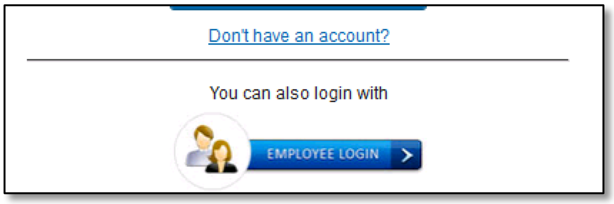
Wi-Fi_SAML_WebAuth_Permit	if	(Guest_Flow AND Wireless_MAB AND PingFederate:ExternalGroups EQUALS Employees)	then	Employee_WebAuth_Permit AND Employees
Wi-Fi_Guest_Access	if	(**GuestType_Daily (default)** OR **GuestType_Weekly (default)** OR **GuestType_Contractor (default)**) AND (Guest_Flow AND Wireless_MAB)	then	Guest_Permit AND Guests

You have completed a SAML SSO login.

Step 5 Now lets create some self-registered guest accounts to use with our filtered list of Sponsor Portal Pending Accounts

a. Access the **Main Portal** using the test URL again.

b. Click on the **Don't have an account** link



c. Enter in the minimum to make an account

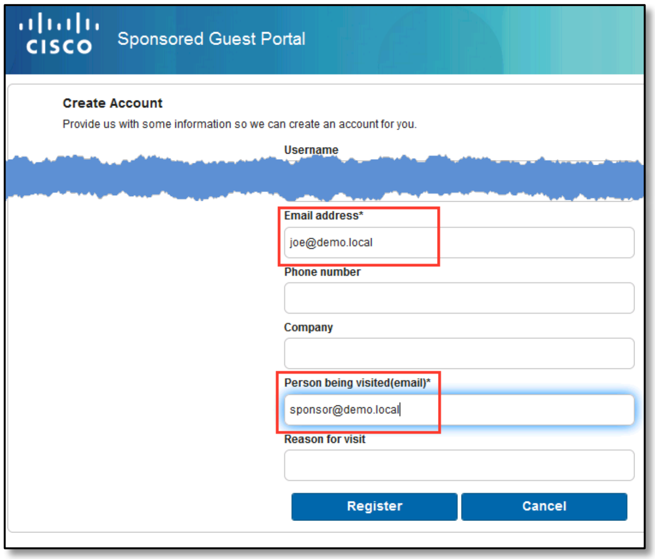
i. Guest email address: joe@demo.local

ii. Person being visited: sponsor@demo.local

iii. Click **Register**

.

d. Repeat above this time using the following values



Create Account

Provide us with some information so we can create an account for you.

Username

Email address*: joe@demo.local

Phone number

Company

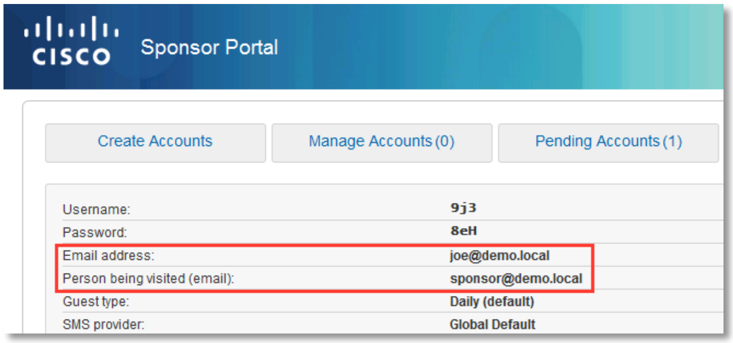
Person being visited(email)*: sponsor@demo.local

Reason for visit

i. Click **Don't have an account** again
ii. Guest email address: rob@demo.local
iii. Person being visited: sponsor1@demo.local
iv. Click **Register**

Step 6 Lets now discover the options available for the Sponsor Portal around SAML login, logout and filtering of the guest pending accounts.

a. Navigate to http://sponsor.demo.local (there is a bookmark for this under ise).
b. You are presented with a SAML login (if you didn't login with the guest portal from before). Login with **sponsor/ISEisC00L**
c. Navigate to **Pending Accounts (1),** notice there is a request from joe@demo.local (the one for rob is not listed)
d. Click on the username to see the details. Notice the person being visited is sponsor@demo.local



Username:	9j3
Password:	8eH
Email address:	joe@demo.local
Person being visited (email):	sponsor@demo.local
Guest type:	Daily (default)
SMS provider:	Global Default

e. Signout of the Sponsor Portal in the upper right by clicking on the **Welcome Sponsor**

This performed a SLO (Single Logout) of the SAML portal through ISE

f. Login as **sponsor1/ISEisC00L**
g. Click on **Pending Accounts (1)**

h. Click on the username to get details for the account. Notice this time the account is for **rob** who is visiting **sponsor1**

The ability to filter the list of pending accounts depending on the Sponsor (person being visited) email address is limited to configurations where you are integrating with SAML provider that provides the email address or internal sponsor accounts on ISE. In ISE 2.1 it is not supported to retrieve this attribute for filtering from direct integration with AD/LDAP. This support should be added in ISE 2.2

You have now completed working with the new features of SAML portals with ISE 2.1.

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 1.6: Log information for troubleshooting and debugging

Exercise Description

In this exercise will look at some of the logs available to you to help in troubleshooting and debugging issues with SAML Portals specifically around some of the issues seen here in this lab.

Exercise Objective

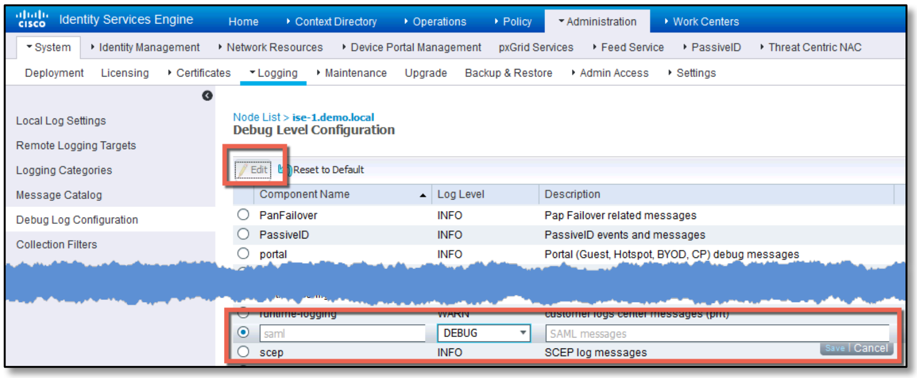
In this exercise, your goal is to learn about some of the different issues seen when troubleshooting Guest SAML Portal and Sponsor filtered pending accounts list.

- Access the ISE CLI
- Validate the good messages and possible bad messages

Exercise Steps

Step 1 Navigate to Operations > RADIUS Live Log
Step 2 Set ISE to debug on SAML

a. On ISE, **Navigate to Administration > System > Logging > Debug Log Configuration > ise-1**
b. Find the Component Name: **saml**
c. Select the **radial**
d. Click **Edit** at the top of the page to change it



Node List > ise-1.demo.local
Debug Level Configuration

	Component Name	Log Level	Description
○	PanFailover	INFO	Pap Failover related messages
○	PassiveID	INFO	PassiveID events and messages
○	portal	INFO	Portal (Guest, Hotspot, BYOD, CP) debug messages
○	runtime-logging	WARN	customer logs center messages (prrt)
●	saml	DEBUG	SAML messages
○	scep	INFO	SCEP log messages

e. Click **Save**

Step 3 Login to the ISE CLI

a. Using Putty SSH open ISE
b. Login as **admin/ISEisC00L**

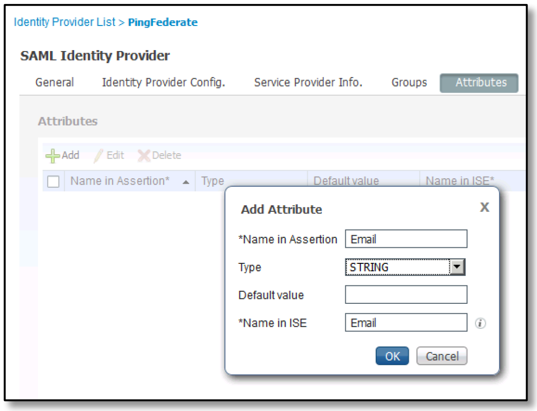
Step 4 Type **show logging application ise-psc.log**
Step 5 Hit **Enter**
Step 6 Search for sponsor@demo.local using /sponsor@demo.local

Issue1: Not receiving filtered list of pending accounts

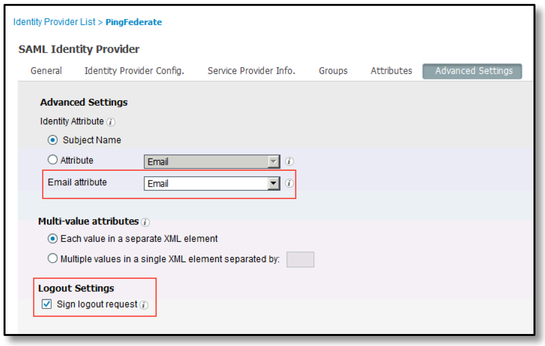
This log shows that it is receiving an attribute of ‘mail’ but its not configured on ISE. This was seen when I had the following screens configured as Email when PingFederate was sending it as ‘mail’

I found this by searching for the e-mail address of my sponsor as they weren't receiving a list of filtered pending accounts

```
2016-04-06 02:58:18,587 DEBUG  [http-bio-10.1.100.21-8443-exec-10][] cpm.saml.framework.impl.SAMLAttributesParser -::::-
[parseAttributes] Delimeter not configured, Attribute=<mail> add value=<sponsor@demo.local>
```



*Name in Assertion: Email
Type: STRING
Default value:
*Name in ISE: Email



Advanced Settings

Identity Attribute

● Subject Name

○ Attribute: Email

Email attribute: Email

Multi-value attributes

● Each value in a separate XML element

○ Multiple values in a single XML element separated by:

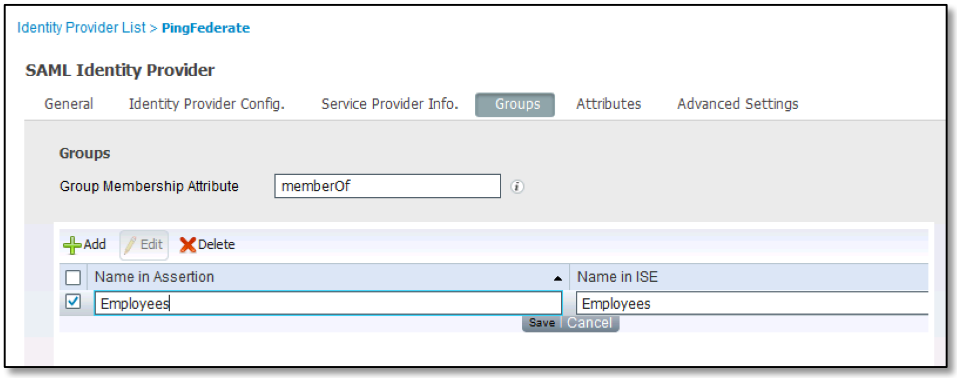
Logout Settings

☑ Sign logout request

Issue2: Unable to login to the Sponsor Portal

This issue was seen when the group mapping was not configured correctly. ISE was receiving memberOf value CN=Employees,OU=Groups,OU=HCC,DC=demo,DC=local but it was configured on ISE as Employees, the value should be CN=Employees,OU=Groups,OU=HCC,DC=demo,DC=local

```
 2016-04-06 02:58:18,587 DEBUG  [http-bio-10.1.100.21-8443-exec-10][] cpm.saml.framework.impl.SAMLAttributesParser -::::-
[parseAttributes] Found attribute name : memberOf
 2016-04-06 02:58:18,587 DEBUG  [http-bio-10.1.100.21-8443-exec-10][] cpm.saml.framework.impl.SAMLAttributesParser -::::-
[parseAttributes] Delimeter not configured, Attribute=<m
 emberOf> add value=<CN=Employees,OU=Groups,OU=HCC,DC=demo,DC=local>
```



Groups

Group Membership Attribute: memberOf

☐	Name in Assertion	Name in ISE
☑	Employees	Employees

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.