

# Configure ISE 2.1 Guest Portal with PingFederate SAML SSO

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Flow Overview](#)

[Expected Flow for this Use Case](#)

[Configure](#)

[Step 1. Prepare ISE to Use an External SAML Identity Provider](#)

[Step 2. Configure the Guest portal to use an external Identity Provider](#)

[Step 3. Configure PingFederate to act as an Identity Provider for ISE Guest Portal](#)

[Step 4. Import IdP Metadata into ISE External SAML IdP Provider Profile](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) version 2.1 Single Sign On(SSO) capabilities for guest portal Security Assertion Markup Language (SAML).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine guest services.
- Basic knowledge about SAML SSO.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine version 2.1
- PingFederate 8.1.3.0 server from Ping Identity as SAML Identity Provider(IdP)

**The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.**

# Flow Overview

SAML is an XML-based standard for exchanging authentication and authorization data between security domains.

SAML specification defines three roles: the Principal ( Guest User), the Identity Provider [IdP] (IPing Federate server), and the Service Provider [SP] (ISE).

In a typical SAML SSO flow, the SP requests and obtains an identity assertion from the IdP. Based on this result, ISE can perform policy decisions as the IdP can include configurable attributes that ISE can use ( i.e. Group and email address associated to the AD object).

## Expected Flow for this Use Case

1. Wireless LAN Controller (WLC) or Access switch is configured for a typical Central Web Authentication (CWA) flow.

**Tip:** Find the configuration examples for CWA flows in the Related Information Section at the bottom of the article.

2. The client connects and the session gets authenticated against ISE. The Network Access Device(NAD) applies the redirect attributes value pairs (AVPs) returned by ISE(url-redirect-acl and url-redirect).

3. The client opens the browser, generates HTTP or HTTPS traffic, and gets redirected to ISE's Guest Portal.

4. Once in the portal the client will be able to enter previously assigned guest credentials (**Sponsor Created**) and self-provision a new guest account or use its AD credentials to log in (**Employee Login**) which will provide Single Sign On capabilities through SAML.

5. Once the user selects the option of "Employee Login" , the ISE verifies if there is an active assertion associated to this client's browser session against the IdP. If there are no active sessions, the IdP will enforce the user login. At this step the user will be prompted to enter AD credentials in the IdP portal directly.

6. The IdP authenticates the user via LDAP and it creates a new Assertion that will stay alive for a configurable time.

**Note:** Ping Federate by default applies a **Session Timeout** of 60 minutes (this means that if there are no SSO login requests from ISE in 60 minutes after initial authentication the session is deleted) and a **Session Max Timeout** of 480 minutes (even if the IdP has received constant SSO login requests from ISE for this user the session will expire in 8 hours).

As long as the Assertion session is still active, the Employee will experience SSO when he uses the Guest Portal. Once the session times out , a new User authentication will be enforced by the IdP.

# Configure

This section discusses the configuration steps to integrate ISE with Ping Federate and how to enable Browser SSO for the Guest Portal.

**Note:** Although various options and possibilities exist when you authenticate Guest users, not all combinations are described in this document. However, this example provides you with the information necessary to understand how to modify the example to the precise configuration you want to achieve.

## Step 1. Prepare ISE to Use an External SAML Identity Provider

1. On the Cisco ISE, choose **Administration > Identity Management > External Identity Sources > SAML Id Providers**.
2. Click **Add**.
3. Under **General** Tab, enter an **Id Provider Name**. Click **Save**. The rest of the configuration in this section depends on the metadata that needs to be imported from the IdP in later steps.

The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Identity Services Engine' and 'Administration'. The breadcrumb trail is 'Administration > External Identity Sources > SAML Id Providers'. The left sidebar shows a tree view of 'External Identity Sources' with 'SAML Id Providers' selected. The main content area shows the 'SAML Identity Provider' configuration page for 'PingFederate'. The 'General' tab is active, showing the 'Id Provider Name' field set to 'PingFederate' and the 'Description' field set to 'SAML SSO IdP'.

## Step 2. Configure the Guest portal to use an external Identity Provider

1. Choose **Work Centers > Guest Access > Configure > Guest Portals**.
2. Create a new portal and choose **Self-Registered Guest Portal**.

**Note:** This will not be the main portal that the user experience but a subportal that will interact with the IdP in order to verify session status. This portal is called SSOSubPortal.

3. Expand **Portal Settings** and choose **PingFederate** for **Authentication Method**.
4. From **Identity Source Sequence**, choose the External SAML IdP previously defined (PingFederate).

## Portals Settings and Customization

Portal Name: \*

SSOSubPortal

Description:

SubPortal that will connect to the SAML IdP

[Portal test URL](#)

Authentication  ⓘ  
method: \* *Configure authentication methods at:*

- Expand the **Acceptable Use Policy( AUP)** and **Post-Login Banner Page Settings** sections and disable both.

Portal flow is:



- Save the changes.
- Go back to Guest Portals and create a new one with the **Self-Registered Guest Portal** option.

**Note:** This will be the Primary portal visible to the client. The primary portal will use the SSOSubportal as an interface between ISE and the IdP. This portal is called PrimaryPortal.

Portal Name: \*

PrimaryPortal

Description:

Portal visible to the client during CWA flow.

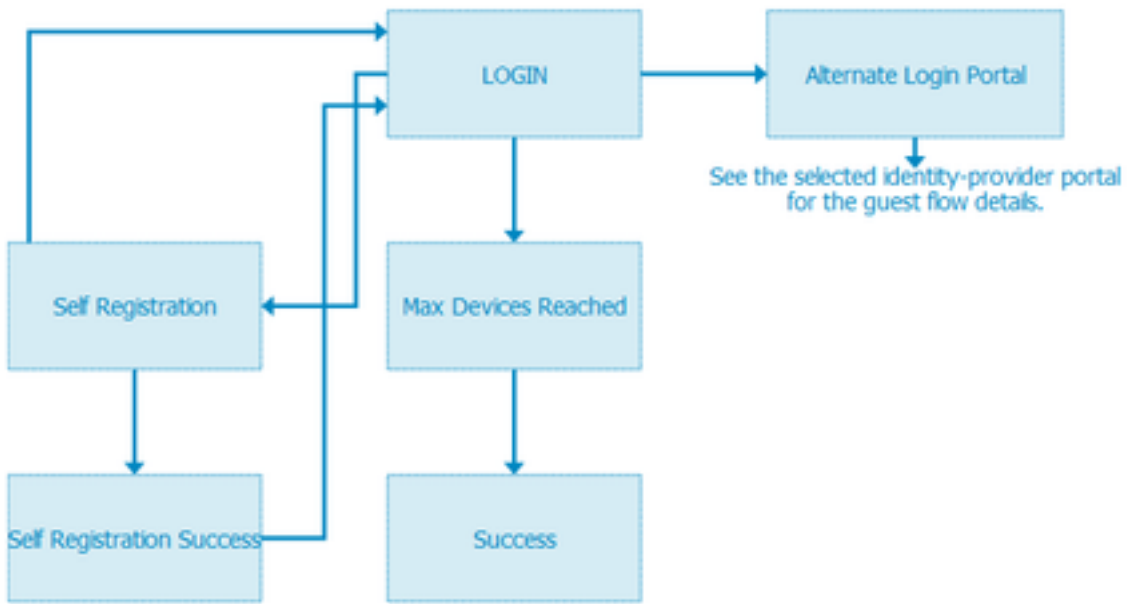
- Expand the **Login Page Settings** and choose the **SSOSubPortal** previously created under **“Allow the following identity-provider guest portal to be used for login”**.

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

- Expand the **Acceptable Use Policy AUP** and **Post-login Banner Page Settings** and uncheck them.

At this point the portal flow must look like this:

Guest Flow (Based on settings)



10. Choose **Portal Customization > Pages > Login**. You must now have the option to customize the **Alternative Login Options** (Icon, text, and so on).


Alternative login:  (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



**Note:** Notice that on the right side, under the portal preview, the additional login option is visible.

---

You can also login with



11. Click **Save**.

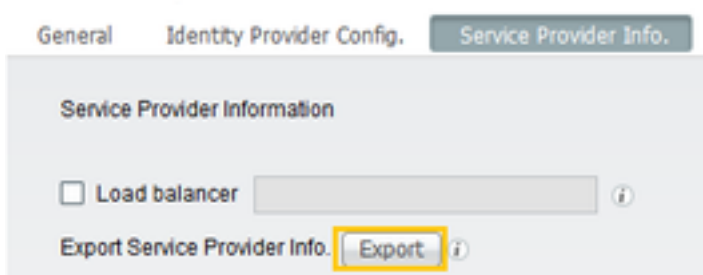
Now both portals appear under the Guest Portal List.

<b>PrimaryPortal</b> Portal visible to the client during CWA flow. ✓ Used in 1 rules in the Authorization policy	Allow login using : SSOSubPortal
<b>SSOSubPortal</b> SubPortal that will connect to the SAML IdP ✓ Used by another portal for alternate login	Used as alternate login option by : PrimaryPortal

### Step 3. Configure PingFederate to act as an Identity Provider for ISE Guest Portal

1. In ISE, choose **Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate** and click the **Service Provider Info.**
2. Under **Export Service Provider Info**, click **Export.**

#### SAML Identity Provider



3. Save and extract the zip file generated. The XML file contained here is used to create the profile in PingFederate in later steps.



**Note:** From this point on, this document covers the PingFederate configuration. This configuration is same for multiple solutions like Sponsor portal, MyDevices, and BYOD portals. (Those solutions are not covered in this article).

4. Open the PingFederate admin portal (typically <https://ip:9999/pingfederate/app> ).
5. Under the **IdP Configuration** tab > **SP Connections** section choose **Create New.**

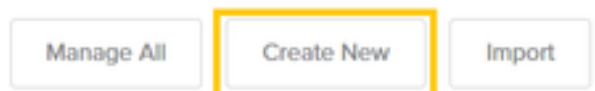
#### IdP Configuration

##### APPLICATION INTEGRATION

- Adapters
- Default URL
- Application Endpoints

##### AUTHENTICATION POLICIES

##### SP CONNECTIONS



6. Under **Connection Type**, click **Next.**

## SP Connection

Connection Type	Connection Options	Import Metadata
-----------------	--------------------	-----------------

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

CONNECTION TEMPLATE	No Template
<input checked="" type="checkbox"/> BROWSER SSO PROFILES	PROTOCOL SAML 2.0

7. Under **Connection Options**, click **Next**.

## SP Connection

Connection Type	Connection Options
-----------------	--------------------

Please select options that apply to this connection.

<input checked="" type="checkbox"/> BROWSER SSO
<input type="checkbox"/> IDP DISCOVERY
<input type="checkbox"/> ATTRIBUTE QUERY

8. Under **Import Metadata**, click the **File** radio button, click **Chose file** and choose the XML file previously exported from ISE.

## SP Connection

Connection Type	Connection Options	Import Metadata
-----------------	--------------------	-----------------

To populate many connection settings automatically, you can upload the metadata file. If you have the URL, select Enable Automatic Reloading.

METADATA	<input type="radio"/> NONE	<input checked="" type="radio"/> FILE
----------	----------------------------	---------------------------------------

No file selected

9. Under **Metadata Summary**, click **Next**.

10. On the General Info page, under Connection Name, enter a name ( such as ISEGuestWebAuth) and click **Next**.

PARTNER'S ENTITY ID  
(CONNECTION ID)

CONNECTION NAME

11. Under **Browser SSO**, click **Configure Browser SSO** and under **SAML Profiles** check the options and click **Next**.

## SP Connection | Browser SSO

SAML Profiles Assertion Lifetime Assertion Creation Protocol Settings Summary

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

Single Sign-On (SSO) Profiles

IDP-INITIATED SSO

SP-INITIATED SSO

Single Logout (SLO) Profiles

IDP-INITIATED SLO

SP-INITIATED SLO

12. On **Assertion lifetime** click **Next**.

13. On **Assertion Creation** click **Configure Assertion Creation**.

14. Under **Identity Mapping** choose **Standard** and click **Next**.

## SP Connection | Browser SSO | Assertion Creation

Identity Mapping Attribute Contract Authentication Source Mapping

Identity mapping is the process in which users authenticated by the IdP are associated to a local account. This process may affect the way that the SP will look up and associate the user to a specific local account.

STANDARD: Send the SP a known attribute value as the name identifier. The

15. On **Attribute Contract** > **Extend Contract** enter the attributes **mail** and **memberOf** and click **add**. Click **Next**.

## SP Connection | Browser SSO | Assertion Creation

Identity Mapping Attribute Contract Authentication Source Mapping Summary

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

Attribute Contract	Subject Name Format	
SAML_SUBJECT	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>	
Extend the Contract	Attribute Name Format	Action
mail	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit</a>   <a href="#">Delete</a>
memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit</a>   <a href="#">Delete</a>



Configuration of this option allows the Identity Provider to pass the **MemberOf** and **Email** attributes provided by Active Directory to ISE, which ISE can use later as a condition during policy decision.

16. Under **Authentication Source Mapping** click **Map New Adapter Instance**.

17. On **Adapter Instance** choose **HTML Form Adapter**. Click **Next**

SP Connection | Browser SSO | Assertion Creation

Adapter Instance | Mapping Method | Attribute Contract Full

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

ADAPTER INSTANCE | HTML Form Adapter

Adapter Contract

givenName

mail

memberOf

objectGUID

sn

username

userPrincipalName

OVERRIDE INSTANCE SETTINGS

18. Under **Mapping methods** choose the second option down and click **Next**.

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

19. On **Attribute Sources & User Lookup** click **Add Attribute Source** box.

20. Under **Data Store** enter a description, and choose LDAP connection instance from **Active Data Store** and define what type of Directory Service this is. If there are no **Data Stores** configured yet click **Manage Data Stores** in order to add the new instance.

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

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
------------	-----------------------	-------------	--------------------------------	---------

This server uses local data stores to retrieve supplemental attributes to be sent in an assertion. Specify an Attribute Source

ATTRIBUTE SOURCE DESCRIPTION	[Redacted]et
ACTIVE DATA STORE	[Redacted]et
DATA STORE TYPE	LDAP

[Manage Data Stores](#)

21. Under **LDAP Directory Search** define the **Base DN** for LDAP user Lookup in the domain and click **Next**.

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

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
------------	-----------------------	-------------	--------------------------------	---------

Please configure your directory search. This information, along with the attributes supplied in the contract, will be used

BASE DN	CN=Users,DC=[Redacted],DC=net
SEARCH SCOPE	Subtree

**Note:** This is important as it will define the base DN during the LDAP user lookup. An incorrectly defined Base DN will result in Object Not found in LDAP schema.

22. Under **LDAP Filter** add the string **sAMAccountName=\${username}** and click **Next**.

# SP Connection | Browser SSO | Assertior

**Data Store** | **LDAP Directory Search** | **LDAP Filter**

Please enter a Filter for extracting data from your directory.

FILTER

23. Under **Attribute Contract Fulfillment** choose the given options and click **Next**.

# SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attribute

**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

24. Verify the configuration at the summary section and click **Done**.

25. Back in **Attribute Sources & User lookup** click **Next**.

26. Under **Failsafe Attribute Source** click **Next**.

27. Under **Attribute Contract Fulfillment** choose these options and click **Next**.

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

28. Verify the configuration in Summary Section and click **Done**.
29. Back on **Authentication Source Mapping** click **Next**.
30. Once configuration has been verified under **Summary** page click **Done**.
31. Back on **Assertion Creation** click **Next**.
32. Under **Protocol Settings** , click **Configure Protocol Settings**. At this point there must be two entries already populated. Click **Next**.

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL	Allowable SAML Bindings	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 bindings. Please provide the possible

Default	Index	Binding	Endpoint URL
default	0	POST	https://14.36.157.210:8443/portal/SSOLoginResponse.action
	1	POST	https://orise21a.rtpaaa.net:8443/portal/SSOLoginResponse.action

33. Under SLO Service URLs click **Next**.
34. On Allowable SAML Bindings, uncheck the options ARTIFACT and SOAP and click **Next**.

Assertion Consumer Service URL	SLO Service URLs	Allowable SAML Bindings
--------------------------------	------------------	-------------------------

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

ARTIFACT

POST

REDIRECT

SOAP

35. Under Signature Policy click **Next**.
36. Under Encryption Policy click **Next**.
37. Review the configuration in the Summary page and click **Done**.
38. Back on Browser SSO > Protocol settings click **Next**, validate the configuration, and click **Done**.
39. The browser SSO tab appears. Click **Next**.

## SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials
-----------------	--------------------	--------------	--------------	-------------	-------------

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources a configuration.

### BROWSER SSO CONFIGURATION

Configure Browser SSO

40. Under **Credentials** click **Configure Credentials** and choose the signing certificate to be used during IdP to ISE communication and check the option **Include the certificate in the signature**. Then click **Next**.

## SP Connection | Credentials

Digital Signature Settings	Signature Verification Settings	Summary
----------------------------	---------------------------------	---------

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

SIGNING CERTIFICATE

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

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

SIGNING ALGORITHM

**Note:** If there are no certificates configured click **Manage Certificates** and follow the prompts in order to generate a **Self-signed certificate** to be used to sign IdP to ISE communications.

41. Validate the configuration under the summary page and click **Done**.

42. Back on the **Credentials** tab click **Next**.

43. Under **Activation & Summary** choose **Connection Status ACTIVE**, validate the rest of the configuration, and click **Done**.

## SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status  ACTIVE  INACTIVE

## Step 4. Import IdP Metadata into ISE External SAML IdP Provider Profile

1. Under the PingFederate management console, choose **Server Configuration > Administrative Functions > Metadata Export**. If the server has been configured for multiple roles( IdP and SP), choose the option **I am the Identity Provider(IdP)**. Click **Next**.
2. Under **Metadata** mode select “**Select Information to Include In Metadata Manually**”. Click **Next** .

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. Under **Protocol** click **Next**.

4. On **Attribute Contract** click **Next**.

5. Under **Signing Key** choose the certificate previously configured on the connection profile. Click **Next**.

### Export Metadata

Metadata Role	Metadata Mode	Protocol	Attribute Contract	Signing Key
---------------	---------------	----------	--------------------	-------------

The metadata may contain a public key that this system uses for digital signatures. If you wish to include

#### DIGITAL SIGNATURE KEYS/CERTS

01:55:31:36:ED:D8 (cn=[REDACTED].147.1) ▼

6. Under **Metadata Signing** choose the signing certificate and check **Include this certificate's public key in the key info element**. Click **Next**.

SIGNING CERTIFICATE

INCLUDE THIS CERTIFICATE'S PUBLIC KEY CERTIFICATE IN THE <KEYINFO> ELEMENT.

SIGNING ALGORITHM

7. Under **XML encryption certificate** click **Next**.

**Note:** The option to enforce encryption here is up to the Network Admin.

8. Under **Summary** section click **Export**. Save the Metadata file generated and then click **Done**.

Export Metadata

Metadata Role   Metadata Mode   Protocol   Attribute Contract   Signing Key   Metadata Signing   XML Encryption Certificate   Export & Summary

Click the Export button to export this metadata to the file system.

Export Metadata	
<b>Metadata Role</b>	
Metadata role	Identity Provider
<b>Metadata Mode</b>	
Metadata mode	Select information manually
Use the secondary port for SOAP channel	false
<b>Protocol</b>	
Protocol	SAML 2.0
<b>Attribute Contract</b>	
Attribute	None defined
<b>Signing Key</b>	
Signing Key	CN=14.36.1471, OU=TAC, O=Cisco, L=RTP, C=US
<b>Metadata Signing</b>	
Signing Certificate	CN=14.36.1471, OU=TAC, O=Cisco, L=RTP, C=US
Include Certificate in KeyInfo	false
Include Raw Key in KeyValue	false
Selected Signing Algorithm	RSA SHA256
<b>XML Encryption Certificate</b>	
Encryption Keys/Certs	NONE

Export

Cancel   Previous   Done


9. Under ISE, choose to **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**.

10. Click **Identity Provider Config > Browse** and proceed to import the metadata saved from PingFederate Metadata Export operation.

## SAML Identity Provider

General   **Identity Provider Config.**   Service Provider I

### Identity Provider Configuration

Import Identity Provider Config File  

Provider Id	PingFederate
Single Sign On URL	https://[redacted].147.1:9031
Single Sign Out URL (Post)	https://[redacted].147.1:9031

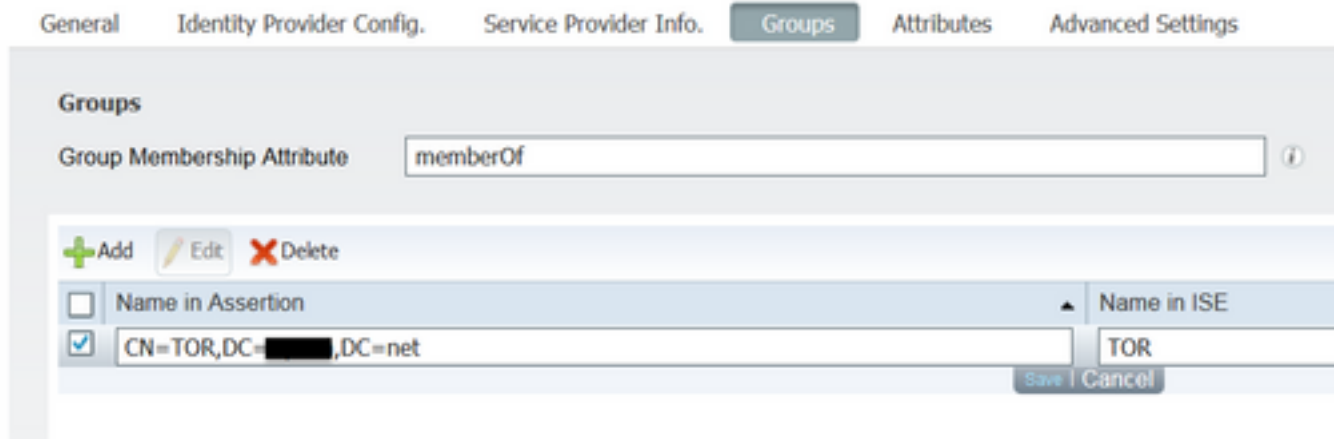
### Signing Certificates

Subject	CN=[redacted].147.1, OU=[redacted], O=Cisco, L=RTP, C=US
---------	--

11. Choose **Groups** Tab, under **Group Membership Attribute** add **memberOf** and then click **Add**

Under the **Name in Assertion** add the Distinguished Name that the **IdP** must return when **memberOf** attribute is retrieved form LDAP authentication. In this case the group configured is linked to the sponsor group of TOR and the DN for this group is as follows:

### SAML Identity Provider



The screenshot shows the 'SAML Identity Provider' configuration interface with the 'Groups' tab selected. The 'Group Membership Attribute' is set to 'memberOf'. Below this, there are buttons for '+Add', 'Edit', and 'Delete'. A table lists the groups:

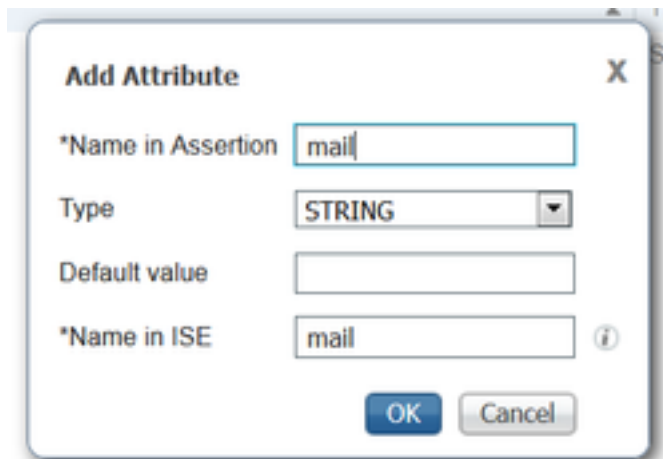
<input type="checkbox"/>	Name in Assertion	Name in ISE
<input checked="" type="checkbox"/>	CN=TOR,DC=██████,DC=net	TOR

Buttons for 'Save' and 'Cancel' are visible at the bottom right of the table.

Once you add the DN and “Name in ISE” description click **OK**.

12. Choose **Attributes** tab and click **Add**.

At this step, add the attribute “mail” that is contained in the SAML token passed from the IdP that based on Ping’s query over LDAP, it must contain the email attribute for that object.



The 'Add Attribute' dialog box is shown with the following fields:

- \*Name in Assertion: mail
- Type: STRING
- Default value: (empty)
- \*Name in ISE: mail

Buttons for 'OK' and 'Cancel' are at the bottom.

**Note:** Steps 11 and 12 ensure that ISE receives the AD object Email and MemberOf attributes through the IdP login action.

## Verify

1. Launch the Guest Portal using the Portal Test URL or by following the CWA flow. The user will have the options to enter guest credentials, create their own account, and Employee Login.



## Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)

You can also login with



2. Click **Employee Login**. Since there are no Active Sessions the user will be redirected to the IdP login portal.

A screenshot of a web page titled "Sign On". The page has a dark grey header with the text "Sign On". Below the header, there is a message: "Please sign on and we'll send you right along." followed by two input fields labeled "USERNAME" and "PASSWORD". At the bottom of the form is a blue button labeled "Sign On".

3. Enter AD credentials and click **Sign On**.

4. IdP logon screen will redirect the user to the Guest Portal Success Page.



**Success**

You now have Internet access through this network.

5. At this point, every time the user comes back to the Guest Portal and choose “**Employee Login**” they will be allowed in the network as long as the Session is still active in the IdP.

## Troubleshoot

Any SAML authentication issue will be logged under ise-psc.log. There is a dedicated component (SAML) under **Administration > Logging > Debug log Configuration > Select the node in question > Set SAML component to debug level.**

You can access ISE through CLI and enter the command **show logging application ise-psc.log tail** and monitor the SAML events, or you can download ise-psc.log for further analysis under **Operations > Troubleshoot > Download Logs > Select the ISE node > Debug Logs tab > click ise-psc.log** to download the logs.

```
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAMLUtils::isOracle() - checking whether IDP URL  
indicates that its OAM. IDP URL: https://10.36.147.1:9031/idp/sso.saml2  
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SPProviderId for PingFederate is: http://CiscoISE  
/5b4c0780-2da2-11e6-a5e2-005056a15f11  
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- ResponseValidationContext:  
    IDP URI: PingFederate  
    SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11  
    Assertion Consumer URL: https://10.36.157.210:8443/portal/SSOLoginResponse.action  
    Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-  
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8  
b99-2ef6b76c1d4b_SEMI_DELIMITER10.36.157.210  
    Client Address: 10.0.25.62  
    Load Balancer: null  
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.BaseSignatureValidator -:::- Determine the signing certificate  
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.BaseSignatureValidator -:::- Validate signature to SAML standard  
with cert:CN=10.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352  
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
org.opensaml.xml.signature.SignatureValidator -:::- Creating XMLSignature object  
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
org.opensaml.xml.signature.SignatureValidator -:::- Validating signature with signature  
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.SAMLSignatureValidator -:::- Assertion signature validated  
succesfully  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
```

```
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.AssertionValidator -:::- Assertion issuer succesfully validated  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.AssertionValidator -:::- Subject succesfully validated  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.AssertionValidator -:::- Conditions succesfully validated  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for guest  
IDPResponse  
:  
    IdP ID: PingFederate  
    Subject: guest  
    SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success  
    SAML Success:true  
    SAML Status Message:null  
    SAML email:guest@example  
    SAML Exception:null  
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - about to call  
authenticateSAMLUser messageCode:null subject:guest  
2016-06-27 16:15:39,375 DEBUG [http-bio-10.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED
```

## Related Information

- [Central Web Authentication with Cisco WLC and ISE configuration example.](#)
- [Central Web Authentication with a Switch and Identity Services Engine Configuration Example.](#)
- [Release Notes for Cisco Identity Services Engine, Release 2.1](#)
- [Cisco Identity Services Engine Administrator Guide, Release 2.1](#)