

# 使用PingFederate SAML SSO配置ISE 2.1訪客門戶

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[流量概覽](#)

[此使用案例的預期流程](#)

[設定](#)

[步驟1.準備ISE以使用外部SAML身份提供程式](#)

[步驟2.將訪客門戶配置為使用外部身份提供程式](#)

[步驟3.配置PingFederate以充當ISE訪客門戶的身份提供程式](#)

[步驟4.將IdP後設資料匯入ISE外部SAML IdP提供程式配置檔案](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔介紹如何為訪客門戶安全宣告標籤語言(SAML)配置思科身份服務引擎(ISE)版本2.1單點登入(SSO)功能。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 思科身分識別服務引擎訪客服務。
- 有關SAML SSO的基本知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.1
- 從Ping身份作為SAML身份提供程式(IdP)的PingFederate 8.1.3.0伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 流量概覽

SAML是基於XML的標準，用於在安全域之間交換身份驗證和授權資料。

SAML規範定義了三個角色：主體（訪客使用者）、身份提供程式[IdP]（IPing Federate伺服器）和服務提供程式[SP](ISE)。

在典型的SAML SSO流中，SP請求並從IdP獲取身份宣告。基於此結果，ISE可以執行策略決策，因為IdP可以包括ISE可以使用的可配置屬性（即與AD對象關聯的組和電子郵件地址）。

## 此使用案例的預期流程

1. 無線LAN控制器(WLC)或存取交換器設定為典型中央Web驗證(CWA)流程。

**提示：**在文章底部的「Related Information（相關資訊）」部分中查詢CWA流的配置示例。

2. 客戶端連線且會話通過ISE進行身份驗證。網路存取裝置(NAD)套用ISE（url-redirect-acl和url-redirect）返回的重新導向屬性值對(AVP)。

3. 客戶端開啟瀏覽器，生成HTTP或HTTPS流量，然後重定向到ISE的訪客門戶。

4. 一旦進入門戶，客戶端將能夠輸入先前分配的訪客憑證(發起人建立)並自行設定新的訪客帳戶或使用其AD憑證登入(員工登入)，這將通過SAML提供單點登入功能。

5. 使用者選擇「員工登入」選項後，ISE會根據IdP驗證是否存在與此客戶端瀏覽器會話關聯的活動斷言。如果沒有活動會話，IdP將強制使用者登入。在此步驟中，系統將提示使用者直接在IdP門戶中輸入AD憑證。

6. IdP通過LDAP對使用者進行身份驗證，並建立一個新的斷言，該斷言將在可配置的時間內保持活動狀態。

**注意：**預設情況下，Ping聯盟應用Session Timeout為60分鐘（這意味著如果在初始身份驗證後60分鐘內沒有來自ISE的SSO登入請求，會話將被刪除），Session Max Timeout為480分鐘（即使IdP已收到來自此使用者的ISE的常數SSO登入請求，會話將在8小時後過期）。

只要斷言會話仍處於活動狀態，員工在使用訪客門戶時將體驗SSO。一旦會話超時，IdP將強制實施新的使用者身份驗證。

## 設定

本節討論將ISE與Ping Federate整合的配置步驟，以及如何為訪客門戶啟用瀏覽器SSO。

**注意：**雖然對訪客使用者進行身份驗證時存在各種選項和可能性，但本文檔中並未介紹所有組合。但是，本示例將為您提供必要的資訊，以便瞭解如何將該示例修改為要實現的精確配置。

### 步驟1.準備ISE以使用外部SAML身份提供程式

1. 在Cisco ISE上，選擇Administration > Identity Management > External Identity Sources > SAML Id Provider。
2. 按一下「Add」。

3. 在**General**頁籤下，輸入**Id Provider Name**。按一下「**Save**」。本節中的其餘配置取決於後續步驟中需要從IdP匯入的後設資料。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. Under 'Administration', the 'External Identity Sources' menu item is selected. The main content area is divided into two panels. The left panel, titled 'External Identity Sources', shows a tree view with folders for 'Certificate Authentication Profile', 'Active Directory', 'LDAP', 'ODBC', 'RADIUS Token', 'RSA SecurID', and 'SAML Id Providers'. The right panel, titled 'Identity Provider List > PingFederate', shows the configuration for a 'SAML Identity Provider'. The 'General' tab is active, and the 'Id Provider Name' is set to 'PingFederate' and the 'Description' is 'SAML SSO IdP'.

## 步驟2.將訪客門戶配置為使用外部身份提供程式

1. 選擇**Work Centers > Guest Access > Configure > Guest Portals**。
2. 建立新門戶並選擇**Self-Registered Guest Portal**。

**注意：**這不是使用者體驗的主要門戶，而是與IdP互動以驗證會話狀態的子門戶。此門戶稱為SSOSubPortal。

3. 展開**Portal Settings**，然後選擇**PingFederate**以進行身份驗證方法。
4. 在**身份源序列**中，選擇先前定義的外部SAML IdP(PingFederate)。

### Portals Settings and Customization

**Portal Name:** \* SSOSubPortal **Description:** SubPortal that will connect to the SAML IdP [Portal test URL](#)

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

5. 展開**Acceptable Use Policy(AUP)**和**Post-Login Banner Page Settings**部分，並禁用這兩部分。

門戶流為：



6.儲存更改。

7.返回訪客門戶，並使用**Self-Registered Guest Portal** 選項建立一個新門戶。

**注意：**這將是對客戶端可見的主門戶。主門戶將使用SSOSubportal作為ISE和IdP之間的介面。此門戶稱為PrimaryPortal。

<b>Portal Name: *</b>	<b>Description:</b>
PrimaryPortal	Portal visible to the client during CWA flow.

8. 展開**Login Page Settings**，然後選擇先前在「允許使用以下身份提供者訪客門戶進行登入」下建立的**SOSubPortal**。

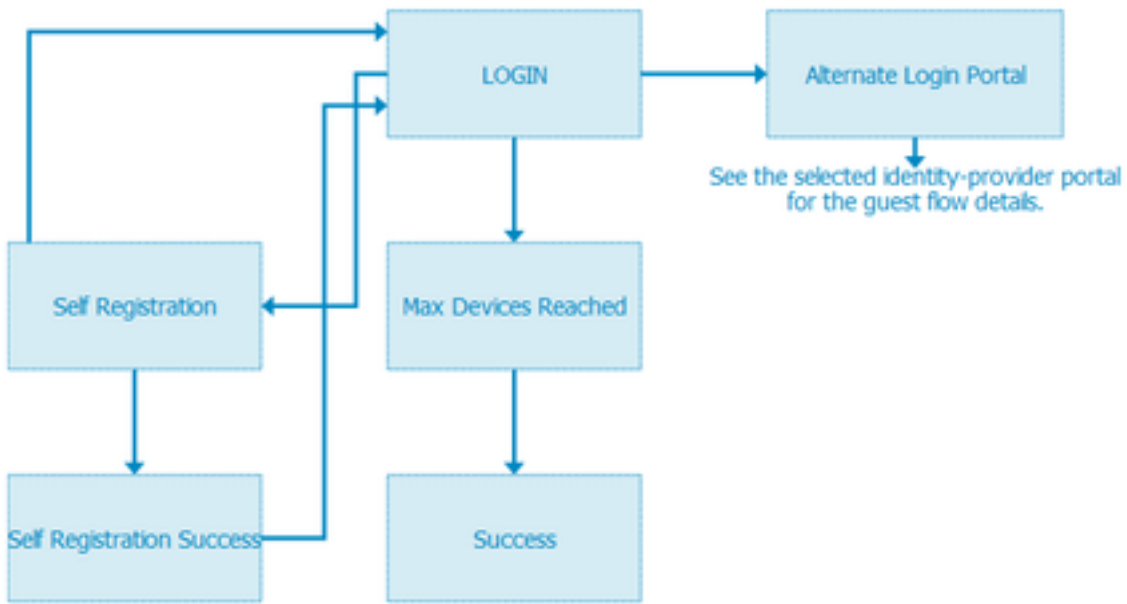
Allow the following identity-provider guest portal to be used for login ⓘ

SSOSubPortal

9.展開**Acceptable Use Policy AUP**和**Post-login Banner Page Settings**並取消選中。

此時，入口流必須如下所示：

## Guest Flow (Based on settings)



10.選擇Portal Customization > Pages > Login。現在，您必須具有自定義可選登入選項（圖示、文本等）的選項。


Alternative login:  (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



注意：請注意，在右側，門戶預覽下會顯示其他登入選項。

---

You can also login with



11.按一下Save。

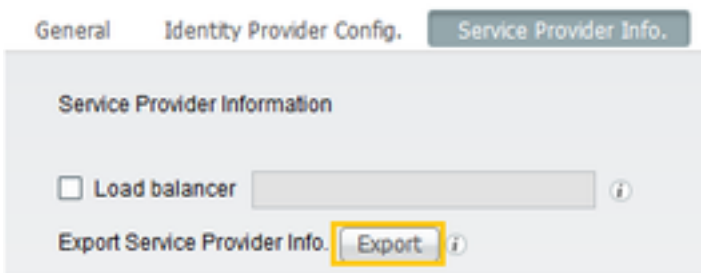
現在，兩個門戶都會顯示在Guest Portal List下。

<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

### 步驟3.配置PingFederate以充當ISE訪客門戶的身份提供程式

1. 在ISE中，選擇Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate，然後點選Service Provider Info。
2. 在Export Service Provider Info下，按一下Export。

#### SAML Identity Provider



3. 儲存並解壓產生的zip檔案。此處包含的XML檔案用於在後續步驟中的PingFederate中建立配置檔案。

 SSOSubPortal.xml

註：從現在起，本文檔將介紹PingFederate配置。對於發起人門戶、MyDevices和BYOD門戶等多個解決方案，此配置是相同的。（本文未涵蓋這些解決方案）。

4. 開啟PingFederate管理員門戶(通常為<https://ip:9999/pingfederate/app>)。
5. 在「IdP配置」選項卡>「SP連接」部分下，選擇新建。

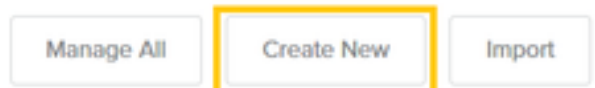
#### IdP Configuration

##### APPLICATION INTEGRATION

Adapters  
 Default URL  
 Application Endpoints

##### AUTHENTICATION POLICIES

##### SP CONNECTIONS



6. 在Connection Type下，單擊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.在Connection Options下，單擊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.在Import Metadata下，按一下File單選按鈕，按一下Selected file並選擇以前從ISE匯出的XML檔案。

## 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.在後設資料摘要下，按一下下一步。

10.在「一般資訊」頁面的「連線名稱」下，輸入名稱（例如ISEGuestWebAuth），然後按一下下一步。

PARTNER'S ENTITY ID  
(CONNECTION ID)

http://CiscoISE/5b4c

CONNECTION NAME

ISEGuestWebAuth

11. 在**瀏覽器SSO**下，按一下**配置瀏覽器SSO**，在**SAML配置檔案**下選中選項並按一下**下一步**。

## 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 messages are processed. This information is used to configure the SP connection.

Single Sign-On (SSO) Profiles

Single Logout (SLO) Profiles

IDP-INITIATED SSO

IDP-INITIATED SLO

SP-INITIATED SSO

SP-INITIATED SLO

12. 在**Assertion lifetime**上按一下**Next**。

13. 在**Assertion Creation**中，按一下**Configure Assertion Creation**。

14. 在**身份對映**下，選擇**標準**，然後按一下**下一步**。

## 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 with local users. 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. 在「**屬性合約**」>「**擴展合約**」中，輸入屬性**mail**和**memberOf**，然後按一下**add**。按「**Next**」( **下一步** )。

## 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

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

Edit | Delete

memberOf

urn:oasis:names:tc:SAML:2.0:attrname-format:basic

Edit | Delete

通過配置此選項，身份提供程式可以將Active Directory提供的**MemberOf**和**Email**屬性傳遞到



ISE，ISE以後可以在策略決策期間將此屬性用作條件。

16.在Authentication Source Mapping下，按一下Map New Adapter Instance。

17.在「介面卡例項」上選擇「HTML表單介面卡」。按一下下一步

SP Connection | Browser SSO | Assertion Cre

Adapter Instance | Mapping Method | Attribute Contract Full

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

ADAPTER INSTANCE | HTML Form Adapter

**Adapter Contract**

givenName

mail

memberOf

objectGUID

sn

username

userPrincipalName

OVERRIDE INSTANCE SETTINGS

18.在Mapping methods下，向下選擇第二個選項，然後按一下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.在「屬性源和使用者查詢」上，按一下Add Attribute Source框。

20.在Data Store下輸入說明，然後從Active Data Store中選擇LDAP連線例項，並定義此目錄服務的型別。如果尚未配置Data Store，請按一下Manage Data Stores以新增新例項。

## 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.在LDAP Directory Search下，定義域中LDAP使用者查詢的Base DN，然後按一下Next。

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

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

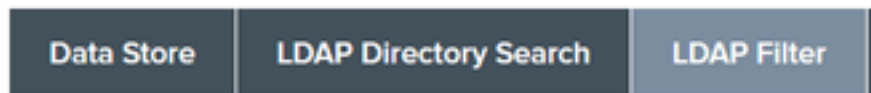
Please configure your directory search. This information, along with the attributes supplied in the contract, will be used

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

**注意：**這一點很重要，因為它將在LDAP使用者查詢期間定義基本DN。錯誤定義的Base DN將導致在LDAP架構中找不到Object Not found。

22.在LDAP Filter下新增字串sAMAccountName=\${username}，然後單擊Next。

## SP Connection | Browser SSO | Assertion

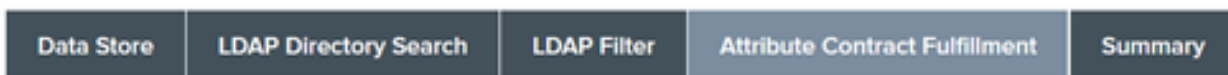


Please enter a Filter for extracting data from your directory.

FILTER

23. 在Attribute Contract Fulfillment下，選擇給定的選項，然後按一下Next。

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



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. 在摘要部分驗證配置，然後按一下完成。

25. 返回Attribute Sources & User lookup，按一下Next。

26. 在Failsafe Attribute Source下，按一下Next。

27. 在Attribute Contract Fulfillment下，選擇這些選項，然後按一下Next。

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

28. 驗證「摘要」部分中的配置，然後按一下**完成**。

29. 返回**Authentication Source Mapping**，按一下**Next**。

30. 在**Summary**頁面下驗證配置後，按一下**Done**。

31. 返回**Assertion Creation**，按一下**Next**。

32. 在**Protocol Settings**下，按一下**Configure Protocol Settings**。此時必須已填充兩個條目。按「**Next**」（下一步）。

#### 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. 在**SLO服務URL**下，按一下**下一步**。

34. 在允許的SAML繫結上，取消選中選項**ARTIFACT**和**SOAP**，然後按一下**下一步**。

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

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

<input type="checkbox"/>	ARTIFACT
<input checked="" type="checkbox"/>	POST
<input checked="" type="checkbox"/>	REDIRECT
<input type="checkbox"/>	SOAP

35. 在「**簽名策略**」下，按一下**下一步**。

36. 在「**加密策略**」下，按一下**下一步**。

37. 檢視「**摘要**」頁中的配置，然後按一下**完成**。

38. 返回**Browser SSO > Protocol settings**，按一下**Next**，驗證配置，然後按一下**Done**。

39. 出現**瀏覽器SSO**頁籤。按「**Next**」（下一步）。

## 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. 在 **Credentials** 下，按一下 **Configure Credentials**，然後選擇在 IdP 與 ISE 通訊期間使用的簽名證書，並選中 **Include the certificate in the signature** 選項。然後點選下一步。

## 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

**注意：**如果沒有配置證書，請點選 **Manage Certificates** 並按照提示生成自簽名證書，用於對 ISE 通訊的 IdP 進行簽名。

41. 驗證摘要頁面下的配置，然後按一下 **完成**。

42. 返回 **憑證** 頁籤，按一下 **下一步**。

43. 在 **Activation & Summary** 下，選擇 **Connection Status ACTIVE**，驗證其餘配置，然後按一下 **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

## 步驟4.將IdP後設資料匯入ISE外部SAML IdP提供程式配置檔案

1. 在PingFederate管理控制檯下，選擇**Server Configuration > Administrative Functions > Metadata Export**。如果伺服器已配置為多個角色（IdP和SP），請選擇**I is the Identity Provider(IdP)**選項。按「Next」（下一步）。
2. 在元資料模式下，選擇「**手動選擇要包括在後設資料中的資訊**」。按「Next」（下一步）。

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3.在Protocol下按一下Next。

4.在屬性合約上按一下下一步。

5.在Signing Key下，選擇之前在連線配置檔案中配置的證書。按「Next」（下一步）。

### 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 this key in the metadata, select a key from the list below.

#### DIGITAL SIGNATURE KEYS/CERTS

01:55:31:36:ED:D8 (cn=██████.147.1) ▼

6.在Metadata Signing下，選擇簽名證書，並選中Include this certificate's public key in the key info element。按「Next」（下一步）。

SIGNING CERTIFICATE

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

SIGNING ALGORITHM

7. 在XML加密證書下，按一下下一步。

**注意：**在此強制加密的選項由網路管理員決定。

8.在Summary部分下，按一下Export。儲存生成的後設資料檔案，然後按一下完成。

## 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.							
<b>Export Metadata</b>							
<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=14.363471, OU=TAC, O=Cisco, L=RTP, C=US						
<b>Metadata Signing</b>							
Signing Certificate	CN=14.363471, 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.在ISE下，選擇Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate。

10.按一下Identity Provider Config > Browse，然後繼續匯入從PingFederate後設資料匯出操作儲存的后設資料。

## 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

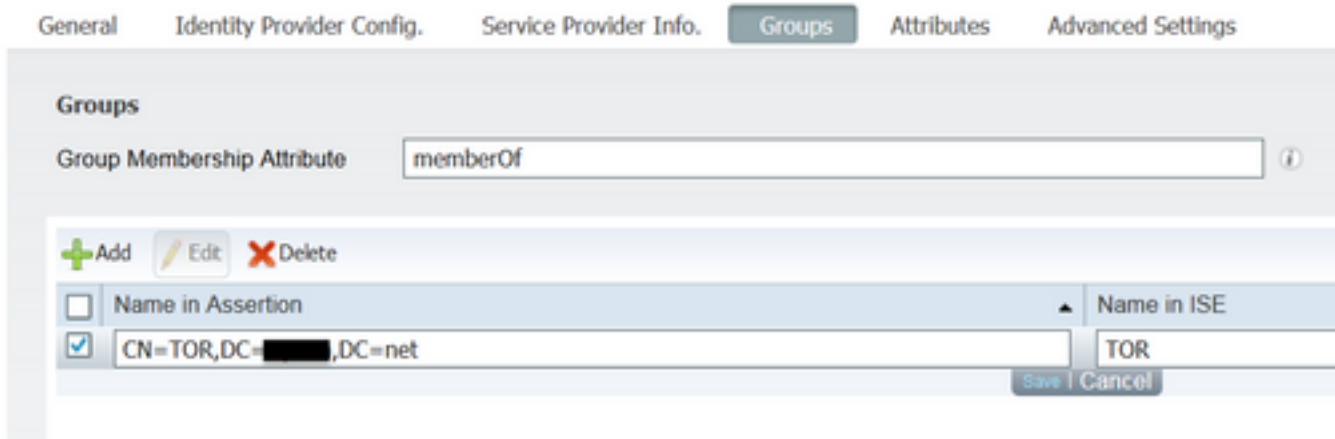
### Signing Certificates

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

11.在Group Membership Attribute下選擇Groups頁籤，然後按一下Add

在Name in Assertion下，新增從LADP身份驗證檢索memberOf屬性時IdP必須返回的可分辨名稱。在這種情況下，配置的組連結到TOR的發起人組，並且此組的DN如下：

### SAML Identity Provider

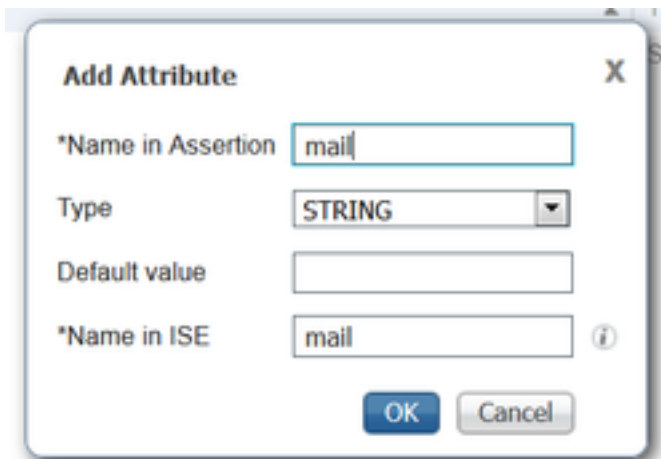


The screenshot shows the 'Groups' configuration page for a SAML Identity Provider. The 'Group Membership Attribute' is set to 'memberOf'. Below this, there is a table with columns 'Name in Assertion' and 'Name in ISE'. A row is added with 'CN=TOR,DC=[redacted],DC=net' in the 'Name in Assertion' column and 'TOR' in the 'Name in ISE' column. The 'Name in Assertion' cell has a checkmark in the left margin. At the bottom right, there are 'Save' and 'Cancel' buttons.

新增DN和「ISE中的名稱」說明後，按一下OK。

12.選擇Attributes頁籤，然後按一下Add。

在此步驟中，新增從IdP傳遞的SAML令牌中包含的屬性「mail」（根據LDAP上的Ping查詢），該令牌必須包含該對象的電子郵件屬性。



The screenshot shows the 'Add Attribute' dialog box. It has four input fields: '\*Name in Assertion' with the value 'mail', 'Type' with a dropdown menu set to 'STRING', 'Default value' which is empty, and '\*Name in ISE' with the value 'mail'. There are 'OK' and 'Cancel' buttons at the bottom.

**注意：**步驟11和12確保ISE通過IdP登入操作接收AD對象Email和MemberOf屬性。

## 驗證

1. 使用門戶測試URL或遵循CWA流程啟動訪客門戶。使用者可以選擇輸入訪客憑證、建立自己的帳戶和員工登入。



## 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. 按一下**Employee Login**。由於沒有活動會話，使用者將被重定向到IdP登入門戶。

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

3. 輸入AD憑證，然後按一下**登入**。

4. IdP登入螢幕會將使用者重定向到「訪客門戶成功」頁面。



Success

You now have Internet access through this network.

5.此時，每次使用者返回訪客門戶並選擇「Employee Login」時，只要會話在IdP中仍然處於活動狀態，就會允許他們進入網路。

## 疑難排解

SAMLise-psc.logAdministration > Logging > Debug log Configuration > Select the node issued > Set SAML component to debug level(SAML)

CLIISEshow logging application ise-psc.log tailSAMLise-psc.logOperations > Troubleshoot > Download Logs > Select the ISE node > Debug Logs>ise-psc.log

```
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
```

## 相關資訊

- [使用思科WLC和ISE進行中央Web身份驗證的配置示例。](#)
- [使用交換機和身份服務引擎進行中央Web身份驗證的配置示例。](#)
- [思科身份服務引擎版本2.1發行說明](#)
- [思科身份服務引擎管理員指南2.1版](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。