

使用PingFederate SAML SSO配置ISE 2.1访客门户

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[流概述](#)

[此使用案例的预期流程](#)

[配置](#)

[步骤1:准备ISE以使用外部SAML身份提供程序](#)

[第二步：将访客门户配置为使用外部身份提供程序](#)

[第三步：配置PingFederate作为ISE访客门户的身份提供程序](#)

[第四步：将IdP元数据导入ISE外部SAML IdP提供程序配置文件](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何为访客门户安全声明标记语言(SAML)配置思科身份服务引擎(ISE)版本2.1单点登录(SSO)功能。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎访客服务。
- 有关SAML SSO的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.1
- 从Ping身份作为SAML身份提供程序(IdP)的PingFederate 8.1.3.0服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

流概述

SAML是基于XML的标准，用于在安全域之间交换身份验证和授权数据。

SAML规范定义了三个角色：主体（访客用户）、身份提供程序[IdP]（IPing Federate服务器）和服务提供程序[SP](ISE)。

在典型的SAML SSO流程中，SP会请求并从IdP获取身份声明。根据此结果，ISE可以执行策略决策，因为IdP可以包括ISE可以使用的可配置属性（即与AD对象关联的组和邮件地址）。

此使用案例的预期流程

1. 无线LAN控制器(WLC)或接入交换机配置为典型集中式Web身份验证(CWA)流程。

提示：在文章底部的“相关信息”部分中查找CWA流的配置示例。

2. 客户端连接且会话根据ISE进行身份验证。网络接入设备(NAD)应用ISE（url-redirect-acl和url-redirect）返回的重定向属性值对(AVP)。

3. 客户端打开浏览器，生成HTTP或HTTPS流量，并重定向到ISE的访客门户。

4. 一旦进入门户，客户端将能够输入先前分配的访客凭证(发起人创建)并自行调配新的访客帐户或使用其AD凭证登录(员工登录)，这将通过SAML提供单点登录功能。

5. 用户选择“员工登录”选项后，ISE会根据IdP验证是否存在与此客户端浏览器会话关联的活动断言。如果没有活动会话，IdP将强制用户登录。在此步骤中，系统将提示用户直接在IdP门户中输入AD凭证。

6. IdP通过LDAP对用户进行身份验证，并创建一个新的断言，该断言将在可配置的时间保持活动状态。

注意：Ping联盟默认应用**60分钟的会话超时**（这意味着如果在初始身份验证后的60分钟内没有来自ISE的SSO登录请求，会话将被删除）和**480分钟的会话最大超时**(即使IdP已收到来自ISE的此用户的常量SSO登录请求，会话将在8小时后过期)。

只要断言会话仍处于活动状态，员工在使用访客门户时将体验SSO。会话超时后，IdP将执行新的用户身份验证。

配置

本节讨论将ISE与Ping Federate集成的配置步骤，以及如何为访客门户启用浏览器SSO。

注意：虽然对访客用户进行身份验证时存在各种选项和可能性，但本文档中并未介绍所有组合。但是，本示例将为您提供必要的信息，帮助您了解如何将该示例修改为要实现的精确配置。

步骤1:准备ISE以使用外部SAML身份提供程序

1. 在Cisco ISE上，选择**管理>身份管理>外部身份源> SAML Id提供程序**。
2. 单击 **Add**。
3. 在**General**选项卡下，输入**Id Provider Name**。Click **Save**。本节中的其余配置取决于后续步骤

中需要从IdP导入的元数据。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The left sidebar shows a tree view of 'External Identity Sources' with categories like Certificate Authentication Profile, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, and SAML Id Providers. The main content area displays the configuration for a 'SAML Identity Provider' named 'PingFederate'. The 'General' tab is active, showing fields for '* Id Provider Name' (PingFederate) and 'Description' (SAML SSO IdP). Other tabs include 'Identity Provider Config.' and 'Service Provider Info.'.

第二步：将访客门户配置为使用外部身份提供程序

1. 选择Work Centers > Guest Access > Configure > Guest Portals。
2. 创建新门户并选择Self-Registered Guest Portal。

注：这不是用户体验的主要门户，而是与IdP交互以验证会话状态的子门户。此门户称为 SOSubPortal。

3. 展开Portal Settings，然后选择PingFederate 以执行身份验证。
4. 从身份源序列中，选择先前定义的外部SAML IdP(PingFederate)。

Portals Settings and Customization

Portal Name: *	Description:	
<input type="text" value="SSOSubPortal"/>	<input type="text" value="SubPortal that will connect to the SAML IdP"/>	Portal test URL

Authentication	<input type="text" value="PingFederate"/>	<input type="button" value="i"/>
method: *	<i>Configure authentication methods at:</i>	

5. 展开Acceptable Use Policy(AUP)和Post-Login Banner Page Settings部分，并禁用这两个部分。

门户流为：



6.保存更改。

7.返回访客门户，并使用**Self-Registered Guest Portal**选项创建新门户。

注意：这将是对客户端可见的主门户。主门户将使用SSOSubportal作为ISE和IdP之间的接口。此门户称为PrimaryPortal。

Portal Name: *	Description:
PrimaryPortal	Portal visible to the client during CWA flow.

8. 展开**Login Page Settings**并选择之前在“**Allow the following identity-provider guest portal to be used for login**”下创建的**SSOSubPortal**。

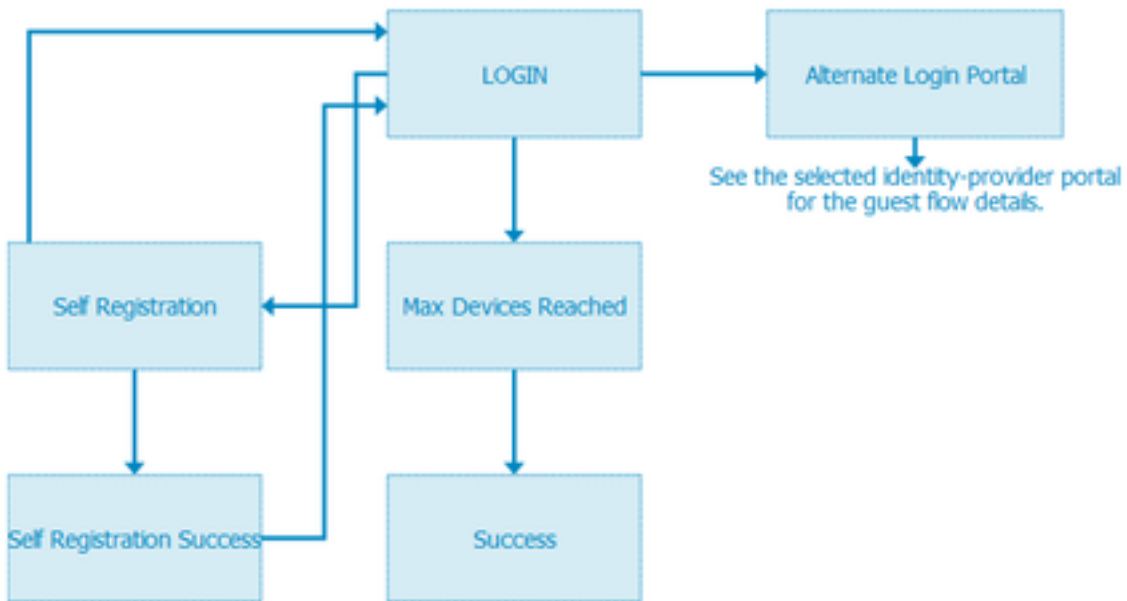
Allow the following identity-provider guest portal to be used for login ⓘ

SSOSubPortal ▼

9.展开**Acceptable Use Policy AUP**和**Post-login Banner Page Settings**并取消选中它们。

此时，门户流必须如下所示：

Guest Flow (Based on settings)



10.选择Portal Customization > Pages > Login。现在，您必须具有自定义Alternative Login Options (图标、文本等) 的选项。


Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



注意：请注意，在右侧，门户预览下方会显示其他登录选项。

You can also login with



11.单击Save。

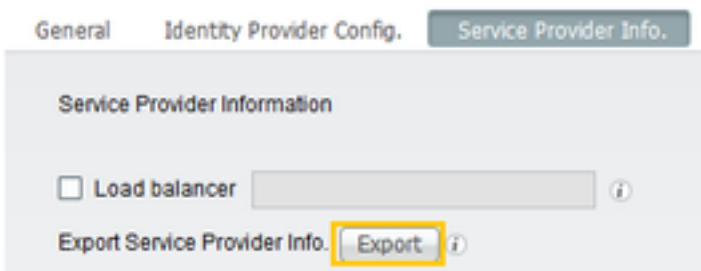
现在，两个门户都显示在Guest Portal List下。

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

第三步：配置PingFederate作为ISE访客门户的身份提供程序

1. 在ISE中，选择Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate，然后点击Service Provider Info。
2. 在Export Service Provider Info下，单击Export。

SAML Identity Provider



3. 保存并提取生成的zip文件。此处包含的XML文件用于在后续步骤中的PingFederate中创建配置文件。



注意：从此时起，本文档将介绍PingFederate配置。对于多个解决方案（如发起人门户、MyDevices和BYOD门户），此配置相同。（本文未涵盖这些解决方案）。

4. 打开PingFederate管理员门户(通常为<https://ip:9999/pingfederate/app>)。
5. 在IdP配置选项卡> SP连接部分下，选择新建。

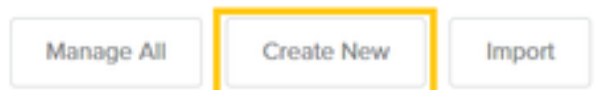
IdP Configuration

APPLICATION INTEGRATION

Adapters
 Default URL
 Application Endpoints

AUTHENTICATION POLICIES

SP CONNECTIONS



6. 在Connection Type(连接类型)下，单击Next(下一步)。

SP Connection

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

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“连接选项”下，单击“下一步”。

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.在导入元数据下，单击文件单选按钮，单击选择文件，然后选择之前从ISE导出的XML文件。

SP Connection

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

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

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

No file selected Choose file

9.在元数据摘要下，单击下一步。

10.在General Info页面的Connection Name下，输入名称（例如ISEGuestWebAuth），然后单击Next。

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11.在Browser SSO下，单击Configure Browser SSO，然后在SAML Profiles下选中选项，然后单击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 messages are exchanged. This information is used to configure the SAML configuration 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

12.在Assertion lifetime上，单击Next。

13.在Assertion Creation中，单击Configure Assertion Creation。

14.在身份映射下，选择标准，然后单击下一步。

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 on the SP. 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“属性合同”>“延长合同”上，输入属性mail和memberOf，然后单击add。单击 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

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

通过配置此选项，身份提供程序可以将MemberOf和Email属性由Active Directory提供给ISE，ISE稍

后可以在策略决策期间将其用作条件。

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

17.在适配器实例上，选择HTML Form Adapter。单击“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 for partner.

ADAPTER INSTANCE: HTML Form Adapter

Adapter Contract

givenName

mail

memberOf

objectGUID

sn

username

userPrincipalName

OVERRIDE INSTANCE SETTINGS

18.在“映射方法”下，向下选择第二个选项，然后单击“下一步”。

RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

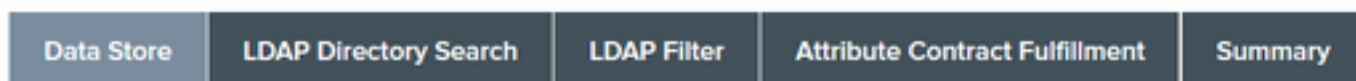
RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE – INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

19.在Attribute Sources & User Lookup上，单击Add Attribute Source框。

20.在Data Store下输入说明，然后从Active Data Store中选择LDAP连接实例，并定义此目录服务的类型。如果未配置Data Stores，请单击Manage Data Stores以添加新实例。

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



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

ATTRIBUTE SOURCE DESCRIPTION

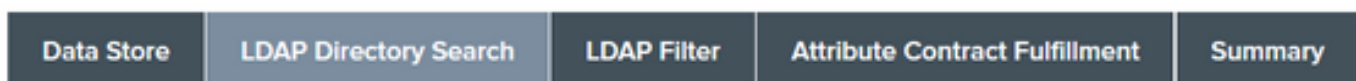
ACTIVE DATA STORE

DATA STORE TYPE LDAP

[Manage Data Stores](#)

21.在LDAP Directory Search下，定义域中LDAP用户查找的基本DN，然后单击Next。

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



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

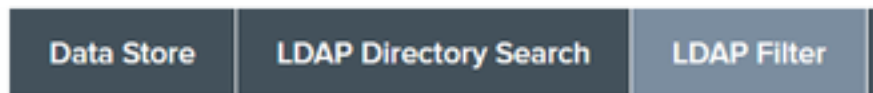
BASE DN

SEARCH SCOPE

注意：这很重要，因为它将在LDAP用户查找期间定义基本DN。错误定义的基础DN将导致在LDAP架构中找不到对象。

22.在LDAP Filter下，添加字符串sAMAccountName=\${username}，然后单击Next。

SP Connection | Browser SSO | Assertior

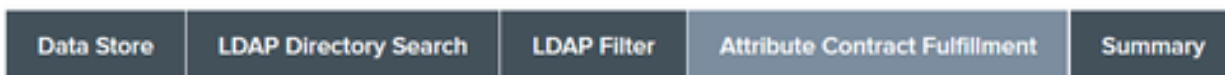


Please enter a Filter for extracting data from your directory.

FILTER

23. 在Attribute Contract Fulfillment下，选择给定的选项，然后单击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. 在摘要部分验证配置，然后单击完成。

25. 返回属性源和用户查找，单击下一步。

26. 在Failsafe Attribute Source下，单击Next。

27. 在Attribute Contract Fulfillment下，选择这些选项，然后单击“下一步”。

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

28. 验证“摘要”部分中的配置，然后单击**完成**。

29. 返回**Authentication Source Mapping**并单击**Next**。

30. 在**Summary**页面下验证配置后，单击**Done**。

31. 返回**Assertion Creation**并单击**Next**。

32. 在**Protocol Settings**下，单击**Configure Protocol Settings**。此时必须已填充两个条目。单击**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.rpeaa.net:8443/portal/SSOLoginResponse.action

33. 在**SLO服务URL**下，单击**下一步**。

34. 在允许的SAML绑定上，取消选中选项**ARTIFACT**和**SOAP**，然后单击**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“签名策略”下，单击**下一步**。

36. 在“加密策略”下，单击**下一步**。

37. 查看“摘要”页面中的配置，然后单击**完成**。

38. 返回**浏览器SSO > 协议设置**，单击**下一步**，验证配置，然后单击**完成**。

39. 系统将显示**浏览器SSO**选项卡。单击 **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.在**Credentials**下，单击**Configure Credentials**，然后选择IdP与ISE通信期间要使用的签名证书，并选中**Include the certificate in the signature**选项。然后，单击下一步。

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	01:55:31:36:ED:D8 (cn=██████████1471) ▼
<input checked="" type="checkbox"/>	INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.
<input type="checkbox"/>	INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.
SIGNING ALGORITHM	RSA SHA256 ▼

注：如果没有配置证书，请点击**Manage Certificates**，然后按照提示生成**Self-signed certificate**，用于对ISE通信的IdP进行签名。

41.验证摘要页面下的配置，然后单击**完成**。

42.返回**凭证**选项卡，单击**下一步**。

43. 在**Activation & Summary**下，选择**Connection Status ACTIVE**，验证其余配置，然后单击**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

第四步：将IdP元数据导入ISE外部SAML IdP提供程序配置文件

1. 在PingFederate管理控制台下，选择**Server Configuration > Administrative Functions > Metadata Export**。如果服务器已配置为多个角色（IdP和SP），请选择**I am the Identity Provider(IdP)**选项。单击 **Next**。
2. 在元数据模式下，选择“手动选择要包括在元数据中的信息”。单击 **Next**。

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3.在协议下单击下一步。

4.在“属性合同”上，单击下一步。

5.在**Signing Key**下，选择之前在连接配置文件中配置的证书。单击 **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 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，选择签名证书，并选中**Include this certificate's public key in the key info element**。单击 **Next**。

SIGNING CERTIFICATE ▼

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

SIGNING ALGORITHM ▼

7. 在**XML加密证书**下，单击下一步。

注意：此处执行加密的选项由网络管理员决定。

8.在**摘要部分**下，单击**导出**。保存生成的元数据文件，然后单击**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.							
Export Metadata							
Metadata Role							
Metadata role	Identity Provider						
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	CN=14.36347L, OU=TAC, O=Cisco, L=RTP, C=US						
Metadata Signing							
Signing Certificate	CN=14.36347L, OU=TAC, O=Cisco, L=RTP, C=US						
Include Certificate in KeyInfo	false						
Include Raw Key in KeyValue	false						
Selected Signing Algorithm	RSA SHA256						
XML Encryption Certificate							
Encryption Keys/Certs	NONE						

Export

Cancel Previous Done

9.在ISE下，选择Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate。

10.单击Identity Provider Config > Browse，然后继续导入从PingFederate元数据导出操作保存的元数据。

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.选择组成员属性下的组选项卡，添加memberOf，然后单击添加

在Name in Assertion下，添加从LDAP身份验证检索memberOf属性时必须返回的Distinguished Name。在这种情况下，配置的组链接到TOR的发起人组，并且此组的DN如下：

SAML Identity Provider

General Identity Provider Config. Service Provider Info. **Groups** Attributes Advanced Settings

Groups

Group Membership Attribute ⓘ

+ Add Edit Delete

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

Save Cancel

添加DN和“ISE中的名称”说明后，单击OK。

12.选择属性选项卡，然后单击添加。

在此步骤中，添加从IdP传递的SAML令牌中包含的属性“mail”，该令牌基于LDAP上的Ping查询，必须包含该对象的电子邮件属性。

Add Attribute X

*Name in Assertion

Type

Default value

*Name in ISE ⓘ

OK Cancel

注意：步骤11和12确保ISE通过IdP登录操作接收AD对象Email和MemberOf属性。

验证

1. 使用门户测试URL或通过遵循CWA流程启动访客门户。用户可以选择输入访客凭证、创建自己的帐户和员工登录。

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.单击**员工登录**。由于没有活动会话，用户将被重定向到IdP登录门户。

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." 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.输入AD凭证，然后单击**登录**。

4. IdP登录屏幕会将用户重定向到“访客门户成功”页面。



Success

You now have Internet access through this network.

5.此时，每次用户返回访客门户并选择“Employee Login”时，只要会话在IdP中仍处于活动状态，就会允许他们进入网络。

故障排除

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

CLI **ISE show logging application ise-psc.log tail SAMLise-psc.log Operations > 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
```

相关信息

- [使用思科WLC和ISE的集中网络身份验证配置示例。](#)
- [带交换机和身份服务引擎的集中式Web身份验证配置示例。](#)
- [思科身份服务引擎版本说明，版本2.1](#)
- [思科身份服务引擎管理员指南，版本2.1](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。