

Configuración de ISE 2.1 Guest Portal con PingFederate SAML SSO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Visión general de flujo](#)

[Flujo esperado para este caso práctico](#)

[Configurar](#)

[Paso 1. Preparación de ISE para utilizar un proveedor de identidad SAML externo](#)

[Paso 2. Configure el portal de invitados para que utilice un proveedor de identidad externo](#)

[Paso 3. Configurar PingFederate para que actúe como proveedor de identidad para el portal de invitados de ISE](#)

[Paso 4. Importar metadatos IdP en el perfil del proveedor de idP de SAML externo de ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar las capacidades de inicio de sesión único (SSO) de Cisco Identity Services Engine (ISE) versión 2.1 para el lenguaje de marcado de aserción de seguridad (SAML) del portal de invitados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios de invitados de Cisco Identity Services Engine.
- Conocimientos básicos sobre SAML SSO.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine versión 2.1
- Servidor PingFederate 8.1.3.0 desde identidad de ping como proveedor de identidad SAML (IdP)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Visión general de flujo

SAML es un estándar basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad.

La especificación SAML define tres funciones: la principal (usuario invitado), el proveedor de identidad [IdP] (servidor federado de IPing) y el proveedor de servicios [SP] (ISE).

En un flujo SSO SAML típico, el SP solicita y obtiene una aserción de identidad del IdP. En función de este resultado, ISE puede realizar decisiones de políticas, ya que el IdP puede incluir atributos configurables que ISE puede utilizar (es decir, el grupo y la dirección de correo electrónico asociados al objeto AD).

Flujo esperado para este caso práctico

1. El controlador de LAN inalámbrica (WLC) o switch de acceso se configura para un flujo típico de autenticación web central (CWA).

Sugerencia: busque los ejemplos de configuración para los flujos de CWA en la sección Información Relacionada en la parte inferior del artículo.

2. El cliente se conecta y la sesión se autentica con ISE. El dispositivo de acceso a la red (NAD) aplica los pares de valores de atributos de redirección (AVP) devueltos por ISE (url-redirect-acl y url-redirect).

3. El cliente abre el navegador, genera tráfico HTTP o HTTPS y se redirige al portal de invitados de ISE.

4. Una vez en el portal, el cliente podrá introducir credenciales de invitado previamente asignadas (**patrocinador creado**) y autoabastecerse de una nueva cuenta de invitado o utilizar sus credenciales de AD para iniciar sesión (**inicio de sesión de empleado**), lo que proporcionará capacidades de inicio de sesión único a través de SAML.

5. Una vez que el usuario selecciona la opción de "Inicio de sesión de empleado", ISE verifica si hay una afirmación activa asociada a la sesión del navegador de este cliente con respecto al IdP. Si no hay sesiones activas, el IdP exigirá el login del usuario. En este paso, se le solicitará al usuario que ingrese las credenciales de AD directamente en el portal IdP.

6. El IdP autentica al usuario vía LDAP y crea una nueva Assertion que permanecerá activa por un tiempo configurable.

Nota: Ping Federate aplica de forma predeterminada un **tiempo de espera de sesión** de 60 minutos (esto significa que si no hay solicitudes de inicio de sesión SSO de ISE en 60 minutos después de la autenticación inicial, se elimina la sesión) y un tiempo de espera **máximo de sesión** de 480 minutos (incluso si el IdP ha recibido solicitudes de inicio de

sesión SSO constantes de ISE para este usuario, la sesión caducará en 8 horas).

Mientras la sesión de aserción siga activa, el empleado experimentará SSO cuando utilice el portal de invitados. Una vez que se agote el tiempo de espera de la sesión , el IdP aplicará una nueva autenticación de usuario.

Configurar

Esta sección trata sobre los pasos de configuración para integrar ISE con Ping Federate y sobre cómo habilitar el SSO del navegador para el portal de invitados.

Nota: Aunque existen varias opciones y posibilidades al autenticar usuarios invitados, no todas las combinaciones se describen en este documento. Sin embargo, este ejemplo le proporciona la información necesaria para comprender cómo modificar el ejemplo a la configuración precisa que desea lograr.

Paso 1. Preparación de ISE para utilizar un proveedor de identidad SAML externo

1. En Cisco ISE, elija **Administration > Identity Management > External Identity Sources > SAML Id Providers**.
2. Haga clic en Add (Agregar).
3. En la pestaña **General**, ingrese un **Nombre del Proveedor de Id**. Click **Save**. El resto de la configuración de esta sección depende de los metadatos que deben importarse desde el IdP en pasos posteriores.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded to show 'Identity Management', which is further expanded to 'External Identity Sources'. The 'External Identity Sources' page is active, showing a list of providers on the left and the configuration for a 'SAML Identity Provider' on the right. The configuration page has tabs for 'General', 'Identity Provider Config.', and 'Service Provider Info.'. The 'General' tab is selected, showing the 'Id Provider Name' field set to 'PingFederate' and the 'Description' field set to 'SAML SSO IdP'.

Paso 2. Configure el portal de invitados para que utilice un proveedor de identidad externo

1. Elija **Centros de trabajo > Acceso de invitado > Configurar > Portales de invitado**.
2. Cree un nuevo portal y seleccione **Portal de invitados registrado automáticamente**.

Nota: Este no será el portal principal que la experiencia del usuario sino un subportal que

interactuará con el IdP para verificar el estado de la sesión. Este portal se denomina SSOSubPortal.

3. Expanda **Configuración del portal** y elija **PingFederate** para el **Método de autenticación**.

4. En **Secuencia de Origen de Identidad**, seleccione el IdP de SAML externo definido anteriormente (PingFederate).

Portals Settings and Customization

Portal Name: * **Description:** [Portal test URL](#)



5. Expanda las secciones **Política de uso aceptable (AUP)** y **Configuración de la página de banner posterior al inicio de sesión** y desactive ambas.

El flujo del portal es:



6. Guarde los cambios.

7. Vuelva a los portales de invitados y cree uno nuevo con la opción **Portal de invitados registrado automáticamente**.

Nota: Este será el portal principal visible para el cliente. El portal principal utilizará el subportal SSOS como interfaz entre ISE y el IdP. Este portal se denomina PrimaryPortal.

Portal Name: * **Description:**

8. Expanda la **Configuración de la página de inicio de sesión** y elija el **SSOSubPortal** creado anteriormente en "Permitir que el siguiente portal de invitados del proveedor de identidad se utilice

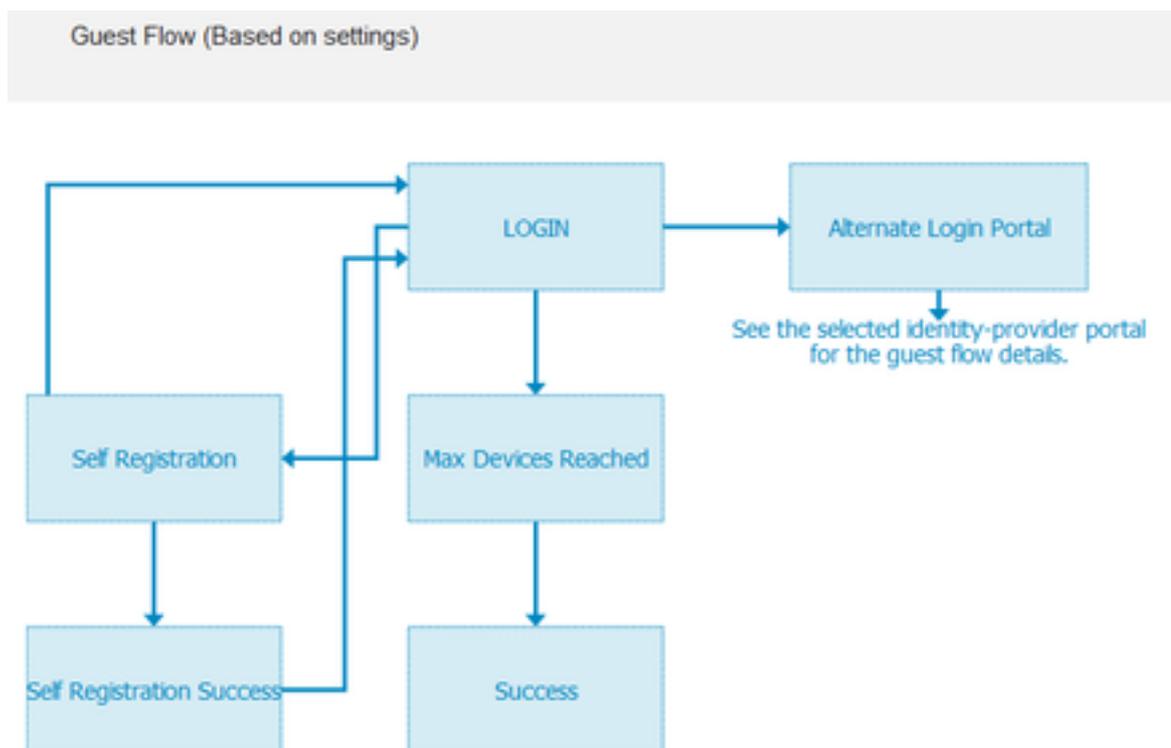
para el inicio de sesión".

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

SSOSubPortal

9. Amplíe la **política de uso aceptable AUP** y la configuración de la página de banner posterior al inicio de sesión y desactívela.

En este punto, el flujo del portal debe verse de la siguiente manera:



10. Elija **Portal Customization > Pages > Login**. Ahora debe tener la opción de personalizar las opciones de inicio de sesión alternativo (icono, texto, etc.).

Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



Nota: Observe que en el lado derecho, debajo de la vista previa del portal, la opción de inicio de sesión adicional está visible.

You can also login with



11. Haga clic en **Guardar**.

Ahora ambos portales aparecen en la Lista de portales de invitados.

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

Paso 3. Configurar PingFederate para que actúe como proveedor de identidad para el portal de invitados de ISE

1. En ISE, elija **Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate** y haga clic en **Service Provider Info**.
2. En **Exportar información del proveedor de servicios**, haga clic en **Exportar**.

SAML Identity Provider

General Identity Provider Config. **Service Provider Info.**

Service Provider Information

Load balancer ⓘ

Export Service Provider Info. **Export** ⓘ

3. Guarde y extraiga el archivo zip generado. El archivo XML contenido aquí se utiliza para crear el perfil en PingFederate en pasos posteriores.



Nota: A partir de este momento, este documento trata la configuración de PingFederate. Esta configuración es la misma para varias soluciones, como el portal de patrocinadores, Mis dispositivos y portales BYOD. (Estas soluciones no se tratan en este artículo).

4. Abra el portal de administración de PingFederate (por lo general, <https://ip:9999/pingfederate/app>).

5. En la sección **Configuración de IdP > Conexiones SP**, seleccione **Crear Nuevo**.

IdP Configuration

APPLICATION INTEGRATION

[Adapters](#)

[Default URL](#)

[Application Endpoints](#)

AUTHENTICATION POLICIES

SP CONNECTIONS

Manage All

Create New

Import

6. En **Tipo de conexión**, haga clic en **Siguiente**.

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. En **Opciones de conexión**, haga clic en **Siguiente**.

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. En **Importar metadatos**, haga clic en el botón de opción **Archivo**, haga clic en **Elegir archivo** y seleccione el archivo XML exportado anteriormente desde ISE.

SP Connection

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

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

METADATA NONE FILE

No file selected

9. En **Metadata Summary**, haga clic en **Next**.

10. En la página Información general, en Nombre de la conexión, introduzca un nombre (como ISEGuestWebAuth) y haga clic en **Siguiente**.

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11. En **Browser SSO**, haga clic en **Configure Browser SSO** y en **SAML Profiles** marque las opciones y haga clic en **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 metadata is exchanged for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input type="checkbox"/> IDP-INITIATED SSO	<input checked="" type="checkbox"/> IDP-INITIATED SLO
<input checked="" type="checkbox"/> SP-INITIATED SSO	<input checked="" type="checkbox"/> SP-INITIATED SLO

12. En **Duración de la aserción**, haga clic en **Siguiente**.

13. En **Creación de aserción**, haga clic en **Configurar creación de aserción**.

14. En **Asignación de identidad**, seleccione **Estándar** y haga clic en **Siguiente**.

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 a local user. This mapping 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. En Attribute Contract > **Extend Contract**, introduzca los atributos **mail** y **memberOf** y haga clic en add. Haga clic en Next (Siguiente).

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:fnameid-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

La configuración de esta opción permite al proveedor de identidad transferir los atributos **MemberOf** y **Email** proporcionados por Active Directory a ISE, que ISE puede utilizar más adelante como condición durante la decisión de la política.

16. En **Authentication Source Mapping**, haga clic en **Map New Adapter Instance**.

17. En **Instancia del adaptador** elija **Adaptador de formulario HTML**. Haga clic en Next (Siguiente)

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 this partner.

ADAPTER INSTANCE

Adapter Contract

givenName

mail

memberOf

objectGUID

sn

username

userPrincipalName

OVERRIDE INSTANCE SETTINGS

18. En **Métodos de asignación**, seleccione la segunda opción hacia abajo y haga clic en

Siguiente.

- 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. En **Orígenes de Atributos y Búsqueda de Usuarios**, haga clic en el cuadro **Agregar Origen de Atributo**.

20. En **Almacén de Datos**, introduzca una descripción y seleccione Instancia de conexión LDAP de **Almacén de Datos Activo** y defina el tipo de servicio de directorio. Si no hay **almacenes de datos** configurados aún, haga clic en **Administrar almacenes de datos** para agregar la nueva instancia.

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

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

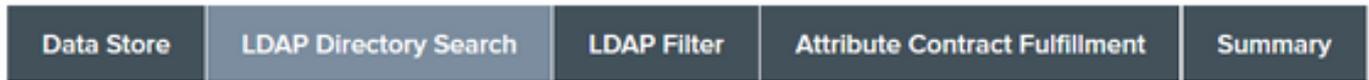
This server uses local data stores to retrieve supplemental attributes to be sent in an assertion. Specify an Attribute Source

ATTRIBUTE SOURCE DESCRIPTION	<input type="text" value="et"/>
ACTIVE DATA STORE	<input type="text" value="et"/>
DATA STORE TYPE	LDAP

[Manage Data Stores](#)

21. En **Búsqueda de directorio LDAP**, defina el **DN base** para la búsqueda de usuarios LDAP en el dominio y haga clic en **Siguiente**.

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



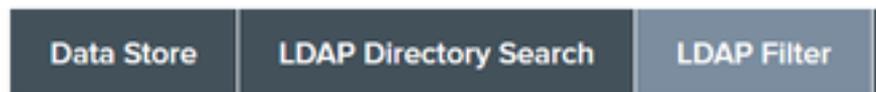
Please configure your directory search. This information, along with the attributes supplied in the contract, will be used

The screenshot shows a form with two fields. The first field is labeled 'BASE DN' and contains the text 'CN=Users,DC=[REDACTED],DC=net'. The second field is labeled 'SEARCH SCOPE' and is a dropdown menu currently set to 'Subtree'.

Nota: Esto es importante ya que definirá el DN base durante la búsqueda de usuarios LDAP. Un DN base definido incorrectamente dará como resultado un objeto no encontrado en el esquema LDAP.

22. En **LDAP Filter**, agregue la cadena **sAMAccountName=\${username}** y haga clic en **Next**.

SP Connection | Browser SSO | Assertion



Please enter a Filter for extracting data from your directory.

The screenshot shows a form with a single field labeled 'FILTER' containing the text 'sAMAccountName=\${username}'.

23. En **Cumplimentación de Contrato de Atributo**, seleccione las opciones proporcionadas y pulse **Siguiente**.

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. Verifique la configuración en la sección de resumen y haga clic en **Finalizado**.

25. De nuevo en **Orígenes de atributos y búsqueda de usuarios**, haga clic en **Siguiente**.

26. En **Origen de atributo de Failsafe**, haga clic en **Siguiente**.

27. En **Cumplimentación de Contrato de Atributo**, seleccione estas opciones y pulse **Siguiente**.

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

28. Compruebe la configuración en la sección Resumen y haga clic en **Finalizado**.

29. De nuevo en **Authentication Source Mapping** haga clic en **Next**.

30. Una vez verificada la configuración en la página **Summary**, haga clic en **Done**.

31. Vuelva a la **creación de aserción** y haga clic en **Siguiente**.

32. En **Protocol Settings**, haga clic en **Configure Protocol Settings**. En este punto debe haber dos entradas ya rellenas. Haga clic en Next (Siguiente).

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://forise21a.rtpaaa.net:8443/portal/SSOLoginResponse.action

33. En URL de servicios SLO, haga clic en **Siguiente**.

34. En Enlaces SAML permitidos, desmarque las opciones ARTIFACT y SOAP y haga clic en **Siguiente**.

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. En Directiva de firmas, haga clic en **Siguiente**.

36. En Encryption Policy, haga clic en **Next**.

37. Revise la configuración en la página Resumen y haga clic en **Finalizado**.

38. De nuevo en el SSO del navegador > Configuración de protocolo haga clic en **Siguiente**, valide la configuración y haga clic en **Finalizado**.

39. Aparece la pestaña SSO del navegador. Haga clic en Next (Siguiente).

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. En **Credenciales**, haga clic en **Configurar Credenciales** y seleccione el certificado de firma que se utilizará durante la comunicación de IdP a ISE y active la opción **Incluir el certificado en la**

firma. Luego haga clic en Next (Siguiente).

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

Nota: Si no hay certificados configurados, haga clic en **Administrar certificados** y siga las indicaciones para generar un **certificado autofirmado** que se utilizará para firmar las comunicaciones de IdP a ISE.

41. Valide la configuración en la página de resumen y haga clic en **Finalizado**.

42. De nuevo en la pestaña **Credenciales**, haga clic en **Siguiente**.

43. En **Activación y resumen** elija **Estado de conexión ACTIVO**, valide el resto de la configuración y haga clic en **Finalizado**.

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

Paso 4. Importar metadatos IdP en el perfil del proveedor de idP de SAML externo de ISE

1. En la consola de administración de PingFederate, elija **Configuración del servidor > Funciones administrativas > Exportación de metadatos**. Si el servidor se ha configurado para varios roles (IdP y SP), elija la opción **Soy el proveedor de identidad (IdP)**. Haga clic en Next (Siguiente).
2. En el modo **Metadatos**, seleccione **"Seleccionar información para incluir en metadatos manualmente"**. Haga clic en Next (Siguiente).

- USE A CONNECTION FOR METADATA GENERATION
 - SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY
- USE THE SECONDARY PORT FOR SOAP CHANNEL

3. En **Protocolo**, haga clic en **Siguiente**.

4. En **Contrato de Atributo**, pulse **Siguiente**.

5. En **Signing Key**, seleccione el certificado configurado previamente en el perfil de conexión. Haga clic en Next (Siguiente).

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 the key from the list below.

DIGITAL SIGNATURE KEYS/CERTS

01:55:31:36:ED:D8 (cn=████████.147.1) ▼

6. En **Firma de metadatos**, seleccione el certificado de firma y marque **Incluir la clave pública de este certificado en el elemento de información de clave**. Haga clic en Next (Siguiente).

SIGNING CERTIFICATE	01:55:31:36:ED:D8 (cn=14.36.147.1) ▼
<input type="checkbox"/>	INCLUDE THIS CERTIFICATE'S PUBLIC KEY CERTIFICATE IN THE <KEYINFO> ELEMENT.
SIGNING ALGORITHM	RSA SHA256 ▼

7. En **Certificado de cifrado XML**, haga clic en **Siguiente**.

Nota: La opción para aplicar el cifrado aquí corresponde al administrador de red.

8. En la sección **Resumen**, haga clic en **Exportar**. Guarde el archivo de metadatos generado y haga clic en **Finalizado**.

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=14.363471, OU=TAC, O=Cisco, L=RTP, C=US						
Metadata Signing							
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						
XML Encryption Certificate							
Encryption Keys/Certs	NONE						
<input type="button" value="Export"/>							
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input type="button" value="Done"/>							

9. En ISE, seleccione **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**.

10. Haga clic en **Identity Provider Config > Browse** y proceda a importar los metadatos guardados de la operación PingFederate Metadata Export.

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. Seleccione la pestaña **Grupos**, en **Atributo de pertenencia a grupo**, agregue **memberOf** y, a continuación, haga clic en **Agregar**

Bajo el **Nombre en la Aserción** agregue el Nombre distinguido que el **IdP** debe devolver cuando el atributo **memberOf** se recupera de la autenticación LADP. En este caso, el grupo configurado está vinculado al grupo patrocinador de TOR y el DN para este grupo es el siguiente:

SAML Identity Provider

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

Groups

Group Membership Attribute ⓘ

+ Add Edit X Delete

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

Save Cancel

Una vez que haya agregado el DN y la descripción "Nombre en ISE", haga clic en **Aceptar**.

12. Seleccione la pestaña **Atributos** y haga clic en **Agregar**.

En este paso, agregue el atributo "mail" que está contenido en el token SAML pasado desde el IdP que, según la consulta de Ping sobre LDAP, debe contener el atributo email para ese objeto.

Add Attribute X

*Name in Assertion

Type

Default value

*Name in ISE ⓘ

OK Cancel

Nota: los pasos 11 y 12 garantizan que ISE reciba los atributos Email y MemberOf del objeto AD a través de la acción de inicio de sesión de IdP.

Verificación

1. Inicie el portal de invitados mediante la URL de prueba del portal o siguiendo el flujo de CWA. El usuario tendrá la opción de introducir credenciales de invitado, crear su propia cuenta e iniciar sesión como empleado.

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. Haga clic en **Conexión del empleado**. Dado que no hay Sesiones Activas, el usuario será redirigido al portal de login IdP.

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

3. Introduzca las credenciales de AD y haga clic en **Iniciar sesión**.

4. La pantalla de inicio de sesión de IdP redirigirá al usuario a la página de acceso al portal de invitados.



Success

You now have Internet access through this network.

5. En este punto, cada vez que el usuario regrese al Portal de Invitados y elija "Inicio de sesión del empleado" se le permitirá en la red mientras la sesión siga activa en el IdP.

Troubleshoot

Cualquier problema de autenticación de SAML se registrará en ise-psc.log. Hay un componente dedicado (SAML) en **Administration > Logging > Debug log Configuration > Select the node in question > Set SAML component to debug level.**

Puede acceder a ISE a través de CLI e introducir el comando **show logging application ise-psc.log tail** y supervisar los eventos SAML, o puede descargar ise-psc.log para realizar un análisis más detallado en **Operaciones > Solución de problemas > Descargar registros > Seleccione el nodo ISE > ficha Registros de depuración > haga clic en ise-psc.log** para descargar los registros.

```
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
```

Información Relacionada

- [Ejemplo de configuración de Autenticación Web Central con Cisco WLC e ISE.](#)
- [Ejemplo de Configuración de Autenticación Web Central con un Switch y Identity Services Engine.](#)
- [Notas de la versión de Cisco Identity Services Engine, versión 2.1](#)
- [Guía del administrador de Cisco Identity Services Engine, versión 2.1](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).