

# Configurare ISE 2.1 Guest Portal con PingFederate SAML SSO

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica sul flusso](#)

[Flusso previsto per questo Use Case](#)

[Configurazione](#)

[Passaggio 1. Preparare ISE per l'uso di un provider di identità SAML esterno](#)

[Passaggio 2. Configurare il portale Guest per l'utilizzo di un provider di identità esterno](#)

[Passaggio 3. Configurazione di PingFederate come provider di identità per ISE Guest Portal](#)

[Passaggio 4. Importazione di metadati IdP nel profilo del provider IDP SAML esterno ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come configurare le funzionalità Single Sign-On (SSO) di Cisco Identity Services Engine (ISE) versione 2.1 per il portale guest Security Assertion Markup Language (SAML).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Servizi guest Cisco Identity Services Engine.
- Conoscenze base di SAML SSO.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine versione 2.1
- PingFederate 8.1.3.0 server da Ping Identity come provider di identità SAML (IdP)

**Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata**

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica sul flusso

SAML è uno standard basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di protezione.

La specifica SAML definisce tre ruoli: l'utente principale ( Guest User), il provider di identità [IdP] (IPing Federate Server) e il provider di servizi [SP] (ISE).

In un tipico flusso SAML SSO, l'SP richiede e ottiene un'asserzione di identità dall'IdP. In base a questo risultato, ISE può eseguire decisioni relative alle policy, poiché l'IdP può includere attributi configurabili che ISE può utilizzare (ad esempio, indirizzo di gruppo e e-mail associato all'oggetto AD).

### Flusso previsto per questo Use Case

1. Il controller WLC (Wireless LAN Controller) o lo switch di accesso è configurato per un flusso CWA (Central Web Authentication) tipico.

**Suggerimento:** per gli esempi di configurazione dei flussi CWA, vedere la sezione Informazioni correlate nella parte inferiore dell'articolo.

2. Il client si connette e la sessione viene autenticata con ISE. Il dispositivo di accesso alla rete (NAD) applica le coppie di valori degli attributi di reindirizzamento (AVP) restituite da ISE (url-redirect-acl e url-redirect).
3. Il client apre il browser, genera il traffico HTTP o HTTPS e viene reindirizzato al portale guest di ISE.
4. Una volta inserito nel portale, il client potrà immettere le credenziali guest precedentemente assegnate (**sponsor creato**) ed eseguire il provisioning automatico di un nuovo account guest o utilizzare le credenziali AD per eseguire il login (**Employee Login**) che fornirà le funzionalità Single Sign-On tramite SAML.
5. Una volta che l'utente ha selezionato l'opzione "Employee Login" , l'ISE verifica se esiste un'asserzione attiva associata alla sessione del browser di questo client rispetto all'IdP. Se non ci sono sessioni attive, l'IdP applicherà l'accesso dell'utente. In questo passaggio verrà richiesto all'utente di immettere le credenziali di Active Directory direttamente nel portale IdP.
6. L'IdP autentica l'utente tramite LDAP e crea una nuova Asserzione che rimarrà attiva per un periodo di tempo configurabile.

**Nota:** per impostazione predefinita, Ping Federate applica un **timeout di sessione** di 60 minuti (questo significa che se non ci sono richieste di accesso SSO da ISE nei 60 minuti successivi all'autenticazione iniziale la sessione viene eliminata) e un **timeout massimo di sessione** di 480 minuti (anche se l'IdP ha ricevuto richieste di accesso SSO costanti da ISE per questo utente, la sessione scadrà tra 8 ore).

Finché la sessione Assertion è ancora attiva, il dipendente sperimenterà l'SSO quando utilizza il portale guest. Una volta scaduto il timeout della sessione, il provider di identità applicherà una nuova autenticazione utente.

## Configurazione

In questa sezione vengono illustrati i passaggi di configurazione per integrare ISE con Ping Federate e come abilitare l'SSO del browser per il portale guest.

**Nota:** sebbene esistano varie opzioni e possibilità quando si autenticano gli utenti guest, non tutte le combinazioni sono descritte in questo documento. Tuttavia, in questo esempio vengono fornite le informazioni necessarie per comprendere come modificare l'esempio in base alla configurazione che si desidera ottenere.

### Passaggio 1. Preparare ISE per l'uso di un provider di identità SAML esterno

1. Su Cisco ISE, scegliere **Amministrazione > Gestione identità > Origini identità esterne > Provider di ID SAML**.
2. Fare clic su **Add**.
3. In Scheda **Generale**, immettere un **nome provider ID**. Fare clic su **Salva**. Il resto della configurazione in questa sezione dipende dai metadati che devono essere importati dal provider di identità nei passaggi successivi.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Administration > Identity Management > External Identity Sources > SAML Id Providers. The main content area is titled "SAML Identity Provider" and shows the configuration for a provider named "PingFederate". The "General" tab is selected, and the "Description" field is set to "SAML SSO IdP".

**External Identity Sources**

- ▶ Certificate Authentication Profile
- ▶ Active Directory
- ▶ LDAP
- ▶ ODBC
- ▶ RADIUS Token
- ▶ RSA SecurID
- ▶ SAML Id Providers

**Identity Provider List > PingFederate**

**SAML Identity Provider**

General | Identity Provider Config. | Service Provider Info.

\* Id Provider Name: PingFederate

Description: SAML SSO IdP

### Passaggio 2. Configurare il portale Guest per l'utilizzo di un provider di identità esterno

1. Scegliete **Centri di lavoro > Accesso guest > Configura > Portali guest**.
2. Creare un nuovo portale e scegliere **Portale guest con registrazione automatica**.

**Nota:** questo non sarà il portale principale utilizzato dall'utente, ma un sottoportale che interagirà con l'IdP per verificare lo stato della sessione. Questo portale è denominato SSOSubPortal.

3. Espandere **Impostazioni portale** e scegliere **PingFederate** per il **metodo di autenticazione**.

4. Da **Sequenza origine identità**, scegliere l'IdP SAML esterno definito in precedenza (PingFederate).

### Portals Settings and Customization

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

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

5. Espandere le sezioni **Acceptable Use Policy( AUP)** e **Post-login Banner Page Settings** e disabilitare entrambe.

Flusso portale:



6. Salvare le modifiche.

7. Tornare a Portali guest e crearne uno nuovo con l'opzione **Self-Registered Guest Portal**.

**Nota:** questo sarà il portale principale visibile al client. Il portale principale utilizzerà il sottoportale SSOS come interfaccia tra ISE e il provider di identità. Questo portale è denominato PrimaryPortal.

<b>Portal Name: *</b>	<b>Description:</b>
<input type="text" value="PrimaryPortal"/>	<input type="text" value="Portal visible to the client during CWA flow."/>

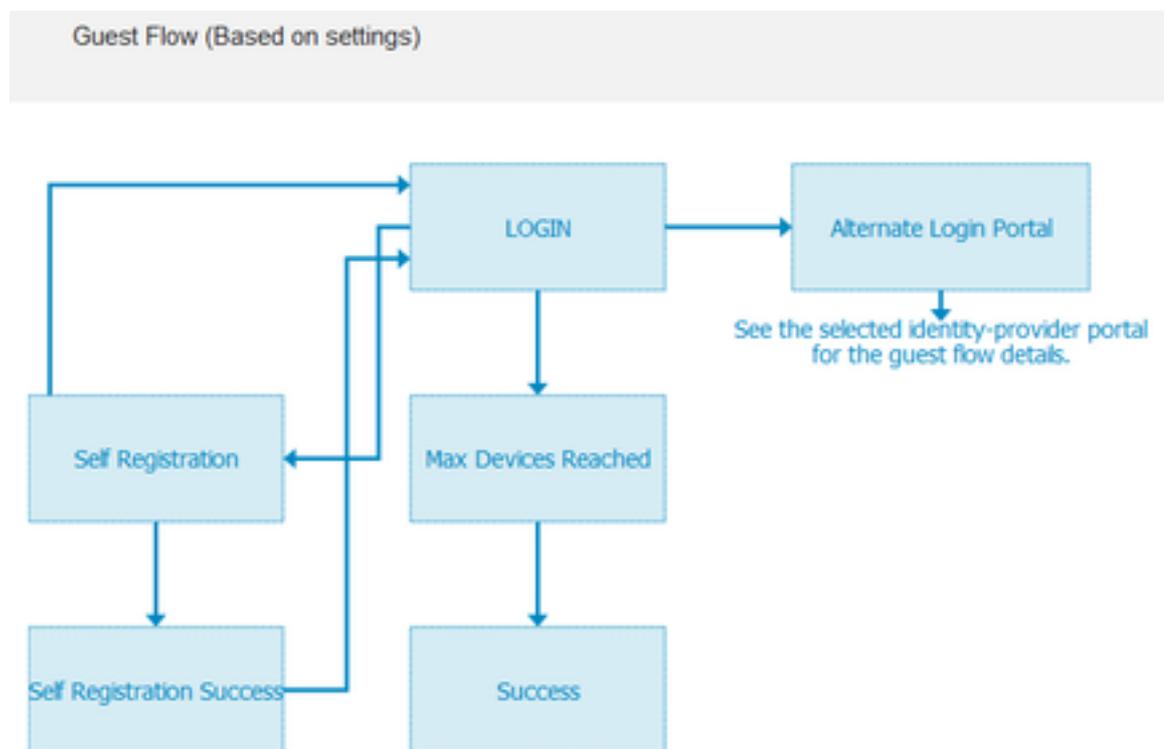
8. Espandere le **impostazioni della pagina di accesso** e scegliere **SSOSubPortal** creato in precedenza in "**Consenti l'utilizzo per l'accesso del seguente portale guest del provider di identità**".

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

SSOSubPortal

9. Espandere le impostazioni **Acceptable Use Policy AUP** e **Post-login Banner Page** e deselezionarle.

A questo punto il flusso del portale deve avere il seguente aspetto:



10. Scegliere **Personalizzazione portale > Pagine > Accesso**. A questo punto è necessario avere la possibilità di personalizzare le **Opzioni di login alternative** (icona, testo e così via).

Alternative login:  (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



**Nota:** nella parte destra dell'anteprima del portale è visibile l'opzione di accesso aggiuntiva.

---

You can also login with



## 11. Fare clic su **Salva**.

Entrambi i portali verranno visualizzati sotto l'elenco dei portali guest.

<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

## Passaggio 3. Configurazione di PingFederate come provider di identità per ISE Guest Portal

1. In ISE, scegliere **Amministrazione > Gestione delle identità > Origini identità esterne > Provider di ID SAML > PingFederate** e fare clic su **Informazioni provider di servizi**.
2. In **Esporta informazioni provider di servizi** fare clic su **Esporta**.

### SAML Identity Provider

General Identity Provider Config. Service Provider Info.

Service Provider Information

Load balancer  ⓘ

Export Service Provider Info. **Export** ⓘ

3. Salvare ed estrarre il file zip generato. Il file XML qui contenuto viene utilizzato per creare il profilo in PingFederate nei passaggi successivi.

 SSOSubPortal.xml

**Nota:** da questo punto in poi, questo documento descrive la configurazione di PingFederate. Questa configurazione è la stessa per più soluzioni come Sponsor Portal, MyDevices e BYOD portals. (Tali soluzioni non sono trattate nel presente articolo).

4. Aprire il portale di amministrazione PingFederate (in genere <https://ip:9999/pingfederate/app> ).
5. Sotto la scheda **Configurazione IdP > Connessioni SP** sezione scegliere **Crea nuovo**.

## IdP Configuration

### APPLICATION INTEGRATION

[Adapters](#)

[Default URL](#)

[Application Endpoints](#)

### AUTHENTICATION POLICIES

### SP CONNECTIONS

Manage All

Create New

Import

6. In **Tipo connessione** fare clic su **Avanti**.

## 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. In **Opzioni di connessione**, fare clic su **Avanti**.

## 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. In **Importa metadati**, fare clic sul pulsante di opzione **File**, fare clic su **Scegli file** e scegliere il file XML precedentemente esportato da ISE.

## SP Connection

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

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

METADATA  NONE  FILE

No file selected

9. In **Riepilogo metadati**, fare clic su **Avanti**.

10. Nella pagina Informazioni generali, in Nome connessione, immettere un nome ( ad esempio ISEGuestWebAuth) e fare clic su **Avanti**.

PARTNER'S ENTITY ID  
(CONNECTION ID)

CONNECTION NAME

11. In **SSO browser**, fare clic su **Configura SSO browser** e in **Profili SAML** controllare le opzioni e fare clic su **Avanti**.

## 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. In **Durata asserzione** fare clic su **Avanti**.

13. In **Creazione asserzioni** fare clic su **Configura creazione asserzioni**.

14. In **Mapping identità** scegliere **Standard** e fare clic su **Avanti**.

## 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 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. In **Attributo contratto** > **Estendi contratto** inserire gli attributi **mail** e **memberOf** e fare clic su **aggiungi**. Fare clic su **Next (Avanti)**.

### 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>

La configurazione di questa opzione consente al provider di identità di passare gli attributi **MemberOf** e **Email** forniti da Active Directory a ISE, che ISE potrà utilizzare in seguito come condizione durante la decisione della policy.

16. In **Mapping origine autenticazione** fare clic su **Mapping nuova istanza adattatore**.

17. Su **istanza adattatore** scegliere **HTML Form Adapter**. Fare clic su **Avanti**.

### 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	<input type="text" value="HTML Form Adapter"/>
Adapter Contract	
givenName	
mail	
memberOf	
objectGUID	
sn	
username	
userPrincipalName	
<input type="checkbox"/>	OVERWRITE INSTANCE SETTINGS

18. In **Metodi di mapping** scegliere la seconda opzione e fare clic su **Avanti**.

- 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. In **Origini attributo e ricerca utente** fare clic su **Aggiungi origine attributo**.

20. In **Archivio dati** immettere una descrizione, scegliere l'istanza di connessione LDAP da **Archivio dati attivo** e definire il tipo di servizio directory. Se non sono presenti **archivi dati** configurati, fare clic su **Gestisci archivi dati** per aggiungere la nuova istanza.

## 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="██████████.net"/>
ACTIVE DATA STORE	<input type="text" value="██████████.net"/>
DATA STORE TYPE	LDAP

[Manage Data Stores](#)

21. In **Ricerca nella directory LDAP** definire il **DN di base** per la ricerca degli utenti LDAP nel dominio e fare clic su **Avanti**.

## 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

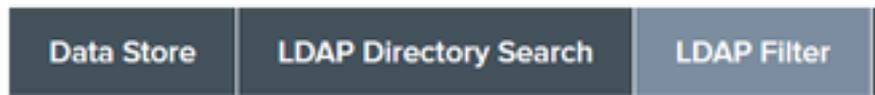
BASE DN	<input type="text" value="CN=Users,DC=██████████,DC=net"/>
SEARCH SCOPE	<input type="text" value="Subtree"/>

**Nota:** questa operazione è importante in quanto definirà il DN di base durante la ricerca dell'utente LDAP. Un DN di base definito in modo non corretto determinerà il mancato

rilevamento dell'oggetto nello schema LDAP.

22. In **Filtro LDAP** aggiungere la stringa **sAMAccountName=\${username}** e fare clic su **Avanti**.

## SP Connection | Browser SSO | Assertion

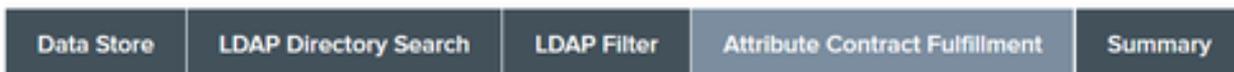


Please enter a Filter for extracting data from your directory.

FILTER

23. In **Attributo: evasione contratto** scegliere le opzioni specificate e fare clic su **Avanti**.

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



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. Verificare la configurazione nella sezione di riepilogo e fare clic su **Fine**.

25. Tornare a **Origini attributi e ricerca utente** e fare clic su **Avanti**.

26. In **Origine attributo Failsafe** fare clic su **Avanti**.

27. In **Attributo: evasione contratto** scegliere queste opzioni e fare clic su **Avanti**.

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

28. Verificare la configurazione nella sezione di riepilogo e fare clic su **Fine**.

29. Tornare al **mapping dell'origine di autenticazione** e fare clic su **Avanti**.

30. Dopo aver verificato la configurazione nella pagina **Riepilogo**, fare clic su **Fine**.

31. Tornare alla **creazione dell'asserzione** e fare clic su **Avanti**.

32. In **Impostazioni protocollo** fare clic su **Configura impostazioni protocollo**. A questo punto devono essere già presenti due voci. Fare clic su Next (Avanti).

#### 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 possibl

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

3. In URL servizio SLO fare clic su **Avanti**.

34. In Associazioni SAML consentite, deselezionare le opzioni ARTIFACT e SOAP e fare clic su **Avanti**.

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. In Criteri firma fare clic su **Avanti**.

36. In Criterio di crittografia fare clic su **Avanti**.

37. Esaminare la configurazione nella pagina Riepilogo e fare clic su **Fine**.

38. Tornare a Browser SSO > Protocol settings (Impostazioni protocollo), fare clic su **Next** (Avanti), convalidare la configurazione e fare clic su **Done** (Fine).

39. Viene visualizzata la scheda SSO del browser. Fare clic su **Next** (Avanti).

## 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. In **Credenziali** fare clic su **Configura credenziali**, quindi scegliere il certificato di firma da utilizzare durante l'IdP per la comunicazione ISE e selezionare l'opzione **Includi il certificato nella firma**. Quindi fare clic su **Avanti**.

## 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:** se non sono configurati certificati, fare clic su **Gestisci certificati** e seguire le istruzioni per generare un **certificato autofirmato** da utilizzare per firmare IdP alle comunicazioni ISE.

41. Convalidare la configurazione nella pagina di riepilogo e fare clic su **Fine**.

42. Tornare alla scheda **Credenziali** e fare clic su **Avanti**.

43. In **Attivazione e riepilogo** scegliere **Stato connessione ATTIVO**, convalidare il resto della

configurazione e fare clic su **Fine**.

## 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

## Passaggio 4. Importazione di metadati IdP nel profilo del provider IDP SAML esterno ISE

1. Nella console di gestione PingFederate, scegliere **Configurazione server > Funzioni amministrative > Esportazione metadati**. Se il server è stato configurato per più ruoli (IdP e SP), scegliere l'opzione **I am the Identity Provider(IdP)**. Fare clic su **Next (Avanti)**.
2. In modalità **metadati** selezionare "**Seleziona informazioni da includere manualmente nei metadati**". Fare clic su Next (Avanti).

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. In **Protocollo** fare clic su **Avanti**.

4. In **Contratto attributo** fare clic su **Avanti**.

5. In **Chiave di firma** scegliere il certificato precedentemente configurato nel profilo di connessione. Fare clic su **Next (Avanti)**.

## 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=██████████.147:1) ▼

6. In **Firma metadati** scegliere il certificato di firma e selezionare **Includi la chiave pubblica del certificato nell'elemento info chiave**. Fare clic su **Next (Avanti)**.

SIGNING CERTIFICATE 01:55:31:36:ED:D8 (cn=14.36.147.1) ▼

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

SIGNING ALGORITHM RSA SHA256 ▼

7. In **Certificato di crittografia XML** fare clic su **Avanti**.

**Nota:** l'opzione per applicare la crittografia qui è di competenza dell'amministratore di rete.

8. Nella sezione **Riepilogo** fare clic su **Esporta**. Salvate il file di metadati generato, quindi fate clic su **Fine (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

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=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US
<b>Metadata Signing</b>	
Signing Certificate	CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US
Include Certificate in KeyInfo	false
Include Raw Key in Key/Value	false
Selected Signing Algorithm	RSA SHA256
<b>XML Encryption Certificate</b>	
Encryption Keys/Certs	NONE

Export

Cancel Previous Done

9. In ISE, scegliere **Amministrazione > Gestione delle identità > Origini identità esterne > Provider di ID SAML > PingFederate**.

10. Fare clic su **Configurazione provider di identità > Sfoglia** e continuare a importare i metadati salvati dall'operazione di esportazione metadati PingFederate.

## SAML Identity Provider

General

Identity Provider Config.

Service Provider I

### Identity Provider Configuration

Import Identity Provider Config File

Browse...



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. Scegliere la scheda **Gruppi**, in **Attributo appartenenza a gruppi** aggiungere **memberOf**, quindi fare clic su **Aggiungi**

In **Nome in asserzione (Name in Assertion)** aggiungete il nome distinto che **IdP** deve restituire quando l'attributo **memberOf** viene recuperato dall'autenticazione LDAP. In questo caso, il gruppo configurato è collegato al gruppo sponsor di TOR e il DN per questo gruppo è il seguente:

### SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

#### Groups

Group Membership Attribute

memberOf



+ Add Edit X Delete

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

Save Cancel

Una volta aggiunti il DN e la descrizione "Nome in ISE", fare clic su **OK**.

12. Scegliere la scheda **Attributi** e fare clic su **Aggiungi**.

In questo passaggio, aggiungere l'attributo "mail" contenuto nel token SAML passato dall'IdP che in base alla query di Ping su LDAP, deve contenere l'attributo email per quell'oggetto.

**Add Attribute** X

\*Name in Assertion

Type

Default value

\*Name in ISE  i

OK Cancel

**Nota:** i passaggi 11 e 12 garantiscono che ISE riceva gli attributi Email e MemberOf dell'oggetto AD tramite l'azione di accesso IdP.

## Verifica

1. Avviare il portale guest utilizzando l'URL del test del portale o seguendo il flusso CWA. L'utente avrà le opzioni per immettere le credenziali guest, creare il proprio account e Accesso dipendente.

### Sign On

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

Username:

Password:

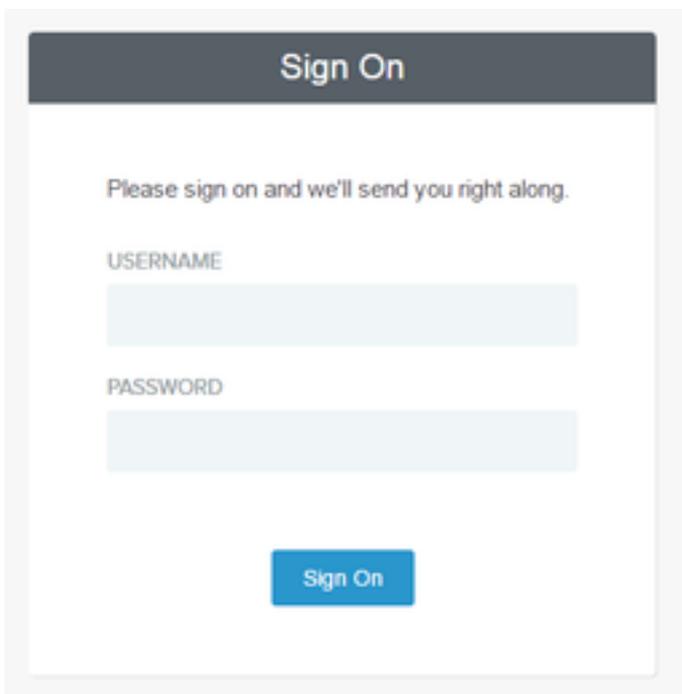
Sign On

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

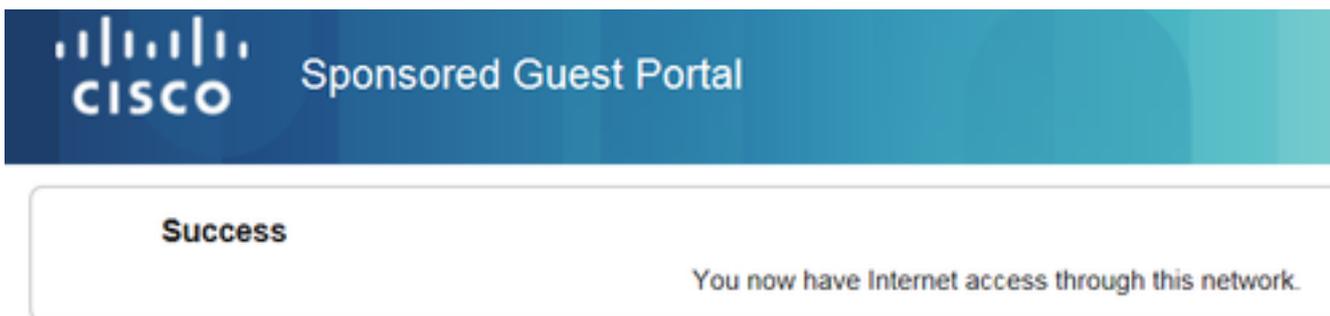
You can also login with



2. Fare clic su **Accesso dipendente**. Poiché non sono presenti sessioni attive, l'utente verrà reindirizzato al portale di accesso IdP.



3. Immettere le credenziali di Active Directory e fare clic su **Accedi**.
4. La schermata di accesso IdP reindirizza l'utente alla pagina di riuscita del portale guest.



5. A questo punto, ogni volta che l'utente ritorna al portale guest e sceglie "Employee Login" sarà consentito nella rete finché la sessione è ancora attiva nell'IdP.

## Risoluzione dei problemi

Eventuali problemi di autenticazione SAML verranno registrati in ise-psc.log. È disponibile un componente dedicato (SAML) in **Amministrazione > Log > Configurazione log di debug > Selezionare il nodo in questione > Imposta il componente SAML a livello di debug**.

È possibile accedere ad ISE dalla CLI e immettere il comando **show logging application ise-psc.log tail** e monitorare gli eventi SAML, oppure è possibile scaricare ise-psc.log per ulteriori analisi in **Operazioni > Risoluzione dei problemi > Log di download > Selezionare il nodo ISE > scheda Log di debug > fare clic su ise-psc.log** per scaricare i 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

```

## Informazioni correlate

- [Esempio di autenticazione Web centrale con Cisco WLC e configurazione ISE.](#)
- [Esempio di autenticazione Web centrale con switch e configurazione di Identity Services Engine.](#)
- [Note sulla versione di Cisco Identity Services Engine, versione 2.1](#)
- [Guida per l'amministratore di Cisco Identity Services Engine, versione 2.1](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).