

Configurar o Portal de Convidado do ISE 2.1 com PingFederate SAML SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Visão geral do fluxo](#)

[Fluxo esperado para este caso de uso](#)

[Configurar](#)

[Etapa 1. Preparar o ISE para usar um provedor de identidade SAML externo](#)

[Etapa 2. Configurar o portal Convidado para usar um Provedor de Identidade externo](#)

[Etapa 3. Configurar o PingFederate para atuar como um provedor de identidade para o portal de convidado do ISE](#)

[Etapa 4. Importar metadados IdP para o perfil do provedor IdP SAML externo do ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar os recursos do Cisco Identity Services Engine (ISE) versão 2.1 Single Sign On (SSO) para o Security Assertion Markup Language (SAML) do portal de convidados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviços para convidados do Cisco Identity Services Engine.
- Conhecimento básico sobre SAML SSO.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine versão 2.1
- Servidor PingFederate 8.1.3.0 a partir da Identidade de Ping como Provedor de Identidade SAML (IdP)

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do fluxo

O SAML é um padrão baseado em XML para a troca de dados de autenticação e autorização entre domínios de segurança.

A especificação SAML define três funções: Principal (Usuário Convidado), Provedor de Identidade [IdP] (servidor Federado de IPing) e Provedor de Serviços [SP] (ISE).

Em um fluxo SAML SSO típico, o SP solicita e obtém uma declaração de identidade do IdP. Com base nesse resultado, o ISE pode executar decisões de política, pois o IdP pode incluir atributos configuráveis que o ISE pode usar (ou seja, grupo e endereço de e-mail associados ao objeto do AD).

Fluxo esperado para este caso de uso

1. A controladora Wireless LAN (WLC) ou o switch de acesso é configurado para um fluxo típico de Autenticação da Web Central (CWA).

Dica: localize os exemplos de configuração para fluxos do CWA na seção Informações relacionadas na parte inferior do artigo.

2. O cliente se conecta e a sessão é autenticada no ISE. O Network Access Device (NAD) aplica os pares de valores de atributos de redirecionamento (AVPs) retornados pelo ISE (url-redirect-acl e url-redirect).

3. O cliente abre o navegador, gera tráfego HTTP ou HTTPS e é redirecionado para o Portal do Convidado do ISE.

4. Uma vez no portal, o cliente poderá inserir credenciais de convidado previamente atribuídas (**Criado pelo Patrocinador**) e provisionar automaticamente uma nova conta de convidado ou usar suas credenciais do AD para fazer logon (**Logon do Funcionário**), que fornecerá recursos de Logon Único por meio do SAML.

5. Depois que o usuário seleciona a opção "Login do funcionário" , o ISE verifica se há uma asserção ativa associada à sessão do navegador desse cliente no IdP. Se não houver sessões ativas, o IdP forçará o login do usuário. Nesta etapa, o usuário será solicitado a inserir credenciais do AD diretamente no portal do IdP.

6. O IdP autentica o usuário via LDAP e cria uma nova Assertion que permanecerá ativa por um tempo configurável.

Observação: o ping federado aplica por padrão um **tempo limite da sessão** de 60 minutos (isso significa que se não houver solicitações de login de SSO do ISE em 60 minutos após a autenticação inicial, a sessão será excluída) e um **tempo limite máximo da sessão de 480 minutos (mesmo se o IdP tiver recebido solicitações de login de SSO constantes do ISE para esse usuário, a sessão expirará em 8 horas).**

Enquanto a sessão de Asserção ainda estiver ativa, o Funcionário passará por SSO quando usar o Portal do Convidado. Quando a sessão expirar , uma nova autenticação de usuário será imposta pelo IdP.

Configurar

Esta seção discute as etapas de configuração para integrar o ISE com o Ping Federado e como habilitar o SSO do Navegador para o Portal do Convidado.

Nota:Embora existam várias opções e possibilidades ao autenticar usuários Convidados, nem todas as combinações são descritas neste documento. No entanto, este exemplo fornece as informações necessárias para entender como modificar o exemplo para a configuração precisa que você deseja obter.

Etapa 1. Preparar o ISE para usar um provedor de identidade SAML externo

1. No Cisco ISE, escolha **Administration > Identity Management > External Identity Sources > SAML Id Providers**.
2. Clique em Add.
3. Na guia **Geral**, insira um **Nome do provedor de ID**. Click **Save**. O restante da configuração nesta seção depende dos metadados que precisam ser importados do IdP em etapas posteriores.

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 left sidebar shows a tree view of External Identity Sources, with 'SAML Id Providers' selected. The main content area shows the configuration for a 'SAML Identity Provider' named 'PingFederate'. The 'General' tab is active, showing the following fields:

- * Id Provider Name: PingFederate
- Description: SAML SSO IdP

Etapa 2. Configurar o portal Convidado para usar um Provedor de Identidade externo

1. Escolha **Centros de trabalho > Acesso de convidado > Configurar > Portais de convidado**.
2. Crie um novo portal e escolha **Portal de convidado com registro automático**.

Observação: este não será o portal principal que o usuário experimentalá, mas um subportal que interagirá com o IdP para verificar o status da sessão. Este portal é chamado SSOSubPortal.

3. Expanda **Configurações do Portal** e escolha **PingFederate** para **Método de Autenticação**.

4. Em **Sequência de Origem da Identidade**, escolha o IdP SAML Externo definido anteriormente (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 ⓘ
method: * *Configure authentication methods at:*

5. Expanda as seções **Política de Uso Aceitável(AUP)** e **Configurações da Página do Banner de Pós-Login** e desative ambas.

O fluxo do portal é:



6. Salve as alterações.

7. Volte para Portais de Convidado e crie um novo com a opção **Portal de Convidado Registrado Automaticamente**.

Observação: este será o portal principal visível para o cliente. O portal principal usará o SSOSubportal como uma interface entre o ISE e o IdP. Esse portal é chamado de PrimaryPortal.

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

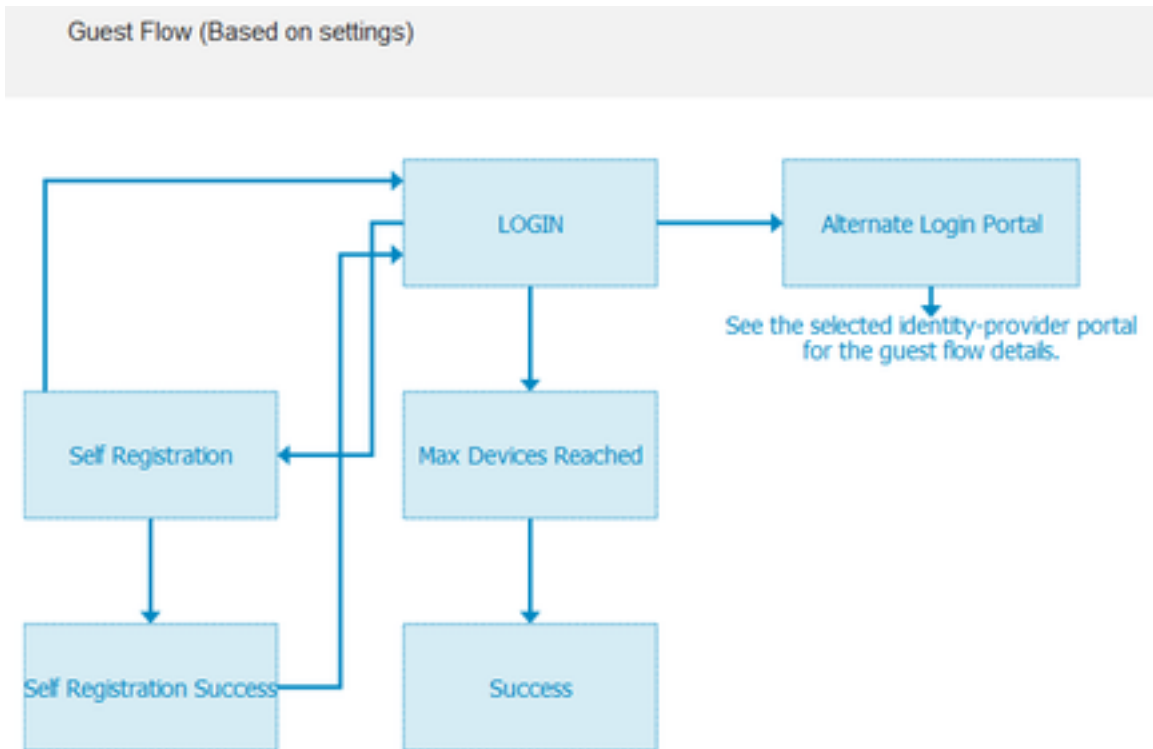
8. Expanda as **Configurações da página de logon** e escolha o **SSOSubPortal** criado anteriormente em "Permitir que o seguinte portal de convidado do provedor de identidade seja usado para logon".

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

SSOSubPortal

9. Expanda **Política de Uso Aceitável AUP** e Configurações da Página do Banner de Pós-login e desmarque-as.

Neste ponto, o fluxo do portal deve ter esta aparência:



10. Escolha **Portal Customization > Pages > Login**. Agora você deve ter a opção de personalizar as **Opções alternativas de login** (ícone, texto e assim por diante).


Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



Observação: observe que, no lado direito, na visualização do portal, a opção de login adicional está visível.

You can also login with



11. Clique em **Salvar**.

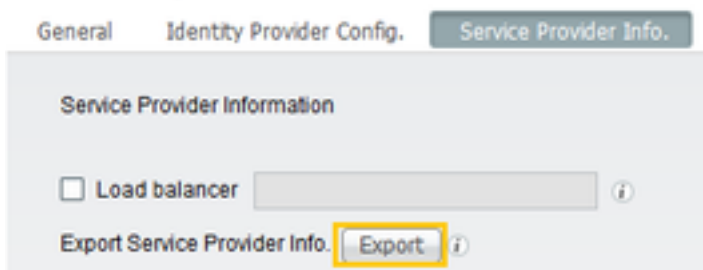
Agora os dois portais aparecem na Lista de portais de convidados.

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

Etapa 3. Configurar o PingFederate para atuar como um provedor de identidade para o portal de convidado do ISE

1. No ISE, escolha **Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate** e clique em **Service Provider Info**.
2. Em **Export Service Provider Info**, clique em **Export**.

SAML Identity Provider



3. Salve e extraia o arquivo zip gerado. O arquivo XML contido aqui é usado para criar o perfil no PingFederate em etapas posteriores.



Observação: deste ponto em diante, este documento aborda a configuração do PingFederate. Essa configuração é igual para várias soluções, como o portal do patrocinador, MyDevices e os portais de BYOD. (Essas soluções não são abordadas neste artigo).

4. Abra o portal de administração do PingFederate (normalmente <https://ip:9999/pingfederate/app>).
5. Na seção **Configuração de IdP > Conexões de SP**, escolha **Criar Novo**.

IdP Configuration

APPLICATION INTEGRATION

[Adapters](#)

[Default URL](#)

[Application Endpoints](#)

AUTHENTICATION POLICIES

SP CONNECTIONS

Manage All

Create New

Import

6. Em **Tipo de Conexão**, clique em **Próximo**.

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



BROWSER SSO PROFILES

PROTOCOL
SAML 2.0

7. Em **Opções de Conexão**, clique em **Próximo**.

SP Connection

Connection Type

Connection Options

Please select options that apply to this connection.



BROWSER SSO



IDP DISCOVERY



ATTRIBUTE QUERY

8. Em **Importar metadados**, clique no botão de opção **Arquivo**, clique em **Escolher arquivo** e escolha o arquivo XML exportado anteriormente do 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. Em **Resumo de Metadados**, clique em **Próximo**.

10. Na página **Informações gerais**, em **Nome da conexão**, insira um nome (como **ISEGuestWebAuth**) e clique em **Avançar**.

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11. Em **SSO do Navegador**, clique em **Configurar SSO do Navegador** e em **Perfis SAML** verifique as opções e clique em **Próximo**.

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. Em **Tempo de vida da Asserção**, clique em **Próximo**.

13. Em **Criação de Asserção**, clique em **Configurar Criação de Asserção**.

14. Em **Mapeamento de identidade**, escolha **Padrão** e clique em **Próximo**.

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. Em Atributo Contrato > **Estender Contrato**, insira os atributos **mail** e **memberOf** e clique em adicionar. Clique em Next.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Summary

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

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

A configuração dessa opção permite que o Provedor de identidade passe os atributos **MemberOf** e **Email** fornecidos pelo Ative Directory para o ISE, que pode ser usado posteriormente como condição durante a decisão da política.

16. Em **Authentication Source Mapping**, clique em **Map New Adapter Instance**.

17. Em **Instância do Adaptador** escolha **Adaptador de Formulário HTML**. Clique em Next

SP Connection | Browser SSO | Assertion Creation

Adapter Instance

Mapping Method

Attribute Contract Full

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

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

18. Em **Métodos de mapeamento**, escolha a segunda opção para baixo e clique em **Próximo**.

- 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. Em **Origens de Atributo e Pesquisa de Usuário**, clique na caixa **Adicionar Origem do Atributo**.

20. Em **Repositório de Dados**, insira uma descrição, escolha a instância de conexão LDAP em **Repositório de Dados Ativos** e defina o tipo de Serviço de Diretório que é. Se não houver **Data Stores** configurados ainda clique em **Manage Data Stores** para adicionar a nova instância.

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. Em **LDAP Directory Search**, defina o **DN de Base** para a Pesquisa de usuário LDAP no domínio e clique em **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

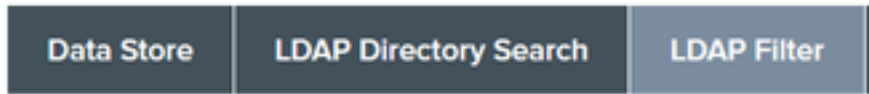
BASE DN	CN=Users,DC=[Redacted],DC=net
SEARCH SCOPE	Subtree

Observação: isso é importante, pois definirá o DN base durante a pesquisa de usuário LDAP. Um DN base definido incorretamente resultará em Objeto não encontrado no

esquema LDAP.

22. Em **Filtro LDAP**, adicione a string `sAMAccountName=${username}` e clique em **Avançar**.

SP Connection | Browser SSO | Assertior

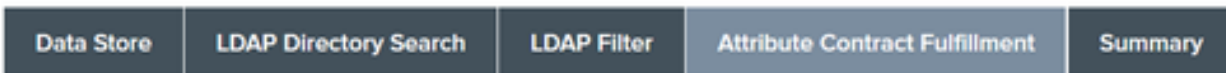


Please enter a Filter for extracting data from your directory.

FILTER

23. Em **Atendimento do Contrato do Atributo**, escolha as opções fornecidas e clique em **Próximo**.

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



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 a configuração na seção de resumo e clique em **Concluído**.

25. Voltar em **Origens de Atributo e Pesquisa de Usuário** clique em **Próximo**.

26. Em **Origem de Atributo Failsafe**, clique em **Avançar**.

27. Em **Atendimento do Contrato do Atributo**, escolha essas opções e clique em **Próximo**.

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

28. Verifique a configuração na Seção Resumo e clique em **Concluído**.

29. Voltar no **Mapeamento de Origem de Autenticação** clique em **Próximo**.

30. Depois que a configuração tiver sido verificada na página **Resumo**, clique em **Concluído**.

31. Voltar na **Criação de Asserção** clique em **Próximo**.

32. Em **Protocol Settings**, clique em **Configure Protocol Settings**. Neste ponto, deve haver duas entradas já preenchidas. Clique em 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://forise21a.rpaaa.net:8443/portal/SSOLoginResponse.action

33. Em URLs de serviço do SLO, clique em **Avançar**.

34. Em Associações SAML Permitidas, desmarque as opções ARTEFATO e SOAP e clique em **Próximo**.

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. Em Signature Policy (Política de Assinatura), clique em **Next**.

36. Em Política de Criptografia, clique em **Próximo**.

37. Revise a configuração na página Resumo e clique em **Concluído**.

38. Voltar no Navegador SSO > Configurações de protocolo, clique em **Próximo**, valide a configuração e clique em **Concluído**.

39. A guia SSO do navegador é exibida. Clique em 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. Em **Credenciais**, clique em **Configurar Credenciais** e escolha o certificado de autenticação a ser usado durante a comunicação IdP para ISE e marque a opção **Incluir o certificado na assinatura**. Em seguida, clique em Avançar.

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

Observação: se não houver certificados configurados, clique em **Gerenciar certificados** e siga os prompts para gerar um **certificado autoassinado** a ser usado para assinar IdP para comunicações do ISE.

41. Valide a configuração na página de resumo e clique em **Concluído**.

42. De volta à guia **Credenciais**, clique em **Avançar**.

43. Em **Ativation & Summary**, escolha **Connection Status ACTIVE**, valide o resto da configuração e clique em **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 <input checked="" type="radio"/> ACTIVE <input type="radio"/> INACTIVE						

Etapa 4. Importar metadados IdP para o perfil do provedor IdP SAML externo do ISE

1. No console de gerenciamento PingFederate, escolha **Server Configuration > Administrative Functions > Metadata Export**. Se o servidor tiver sido configurado para várias funções (IdP e SP), escolha a opção **Eu sou o provedor de identidade (IdP)**. Clique em **Next**.
2. No modo **Metadados**, selecione **"Selecionar informações para incluir nos metadados manualmente"**. Clique em **Next**.

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. Em **Protocolo**, clique em **Próximo**.

4. Em **Atribuir Contrato**, clique em **Próximo**.

5. Em **Chave de Assinatura**, escolha o certificado previamente configurado no perfil de conexão. Clique em **Next**.

Export Metadata

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

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

DIGITAL SIGNATURE KEYS/CERTS

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

6. Em **Assinatura de Metadados**, escolha o certificado de assinatura e marque **Incluir a chave pública deste certificado no elemento de informações da chave**. Clique em **Next**.

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. Em **Certificado de criptografia XML**, clique em **Avançar**.

Observação: a opção de impor a criptografia aqui depende do administrador da rede.

8. Na seção **Resumo**, clique em **Exportar**. Salve o arquivo de Metadados gerado e clique em **Concluído**.

Export Metadata

Metadada 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=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US
Metadata Signing	
Signing Certificate	CN=14.36.147.1, 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. No ISE, escolha **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**.

10. Clique em **Configuração do Provedor de Identidade > Procurar** e continue a importar os metadados salvos da operação de Exportação de Metadados do 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. Escolha a guia **Grupos**, em **Atributo de membro do grupo**, adicione **memberOf** e clique em **Adicionar**

Em **Name in Assertion**, adicione o Distinguished Name (Nome Distinto) que **IdP** deve retornar quando o atributo **memberOf** for recuperado da autenticação LDAP. Nesse caso, o grupo configurado é vinculado ao grupo patrocinador do TOR e o DN desse grupo é o seguinte:

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Groups

Group Membership Attribute

memberOf



+ Add Edit X Delete

Name in Assertion

Name in ISE

CN=TOR,DC=[redacted],DC=net

TOR

Save Cancel

Depois de adicionar o DN e a descrição "Name in ISE", clique em **OK**.

12. Escolha a guia **Atributos** e clique em **Adicionar**.

Nesta etapa, adicione o atributo "mail" contido no token SAML passado do IdP que, com base na consulta de Ping sobre LDAP, deve conter o atributo de e-mail para esse objeto.

Add Attribute X

*Name in Assertion

Type

Default value

*Name in ISE i

OK Cancel

Observação: as etapas 11 e 12 garantem que o ISE receba os atributos Email e MemberOf do objeto do AD por meio da ação de logon do IdP.

Verificar

1. Inicie o Portal do convidado usando a URL de teste do portal ou seguindo o fluxo do CWA. O usuário terá as opções de inserir credenciais de convidado, criar sua própria conta e Login do funcionário.

Sign On

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

Username:

Password:

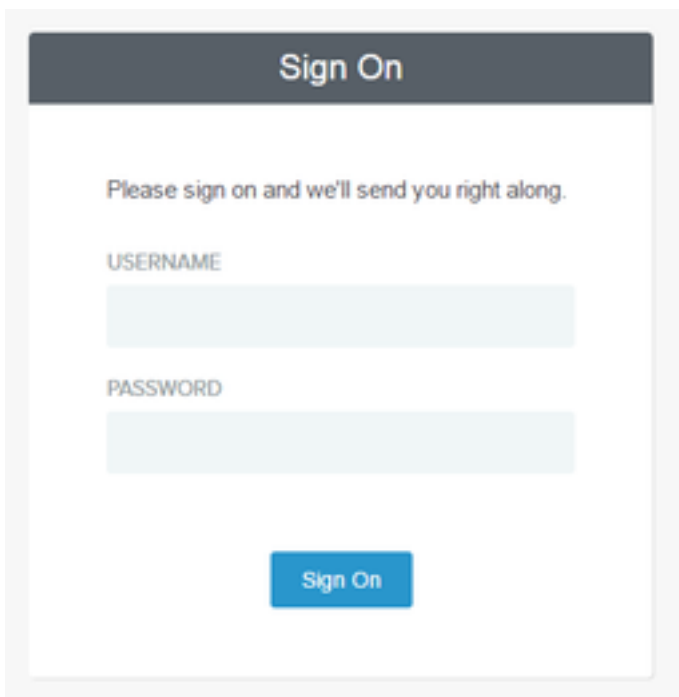
Sign On

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

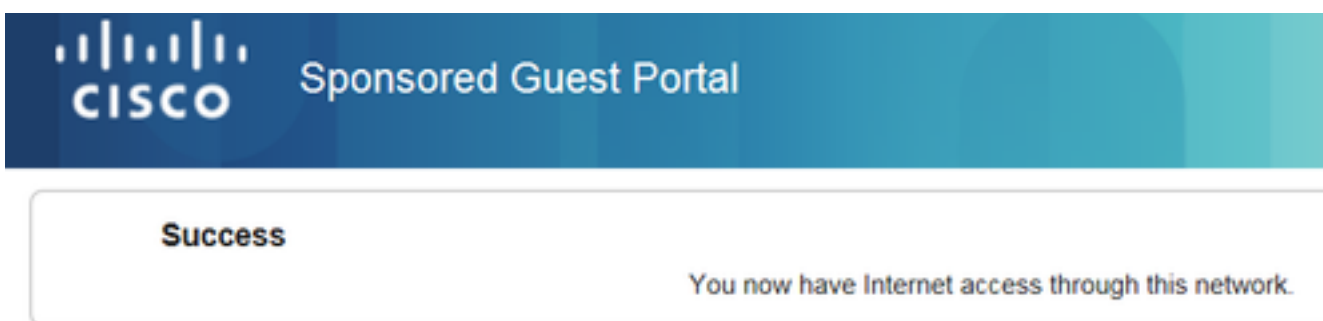
You can also login with



2. Clique em **Login do Funcionário**. Como não há sessões ativas, o usuário será redirecionado para o portal de login do IdP.



3. Insira as credenciais do AD e clique em **Sign On**.
4. A tela de logon do IdP redirecionará o usuário para a Página de Êxito do Portal do Convidado.



5. Nesse ponto, toda vez que o usuário voltar ao Portal do Convidado e escolher "Logon do Funcionário", ele será permitido na rede, desde que a Sessão ainda esteja ativa no IdP.

Troubleshoot

Qualquer problema de autenticação SAML será registrado em `ise-psc.log`. Há um componente dedicado (SAML) em **Administration > Logging > Debug log Configuration > Select the node in question > Set SAML component to debug level**.

Você pode acessar o ISE por meio da CLI e inserir o comando **show logging application ise-psc.log tail** e monitorar os eventos SAML, ou você pode baixar `ise-psc.log` para análise adicional em **Operações > Solução de problemas > Fazer download de logs > Selecionar o nó ISE > guia Logs de depuração > clicar em ise-psc.log** para fazer download dos logs.

```
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][[]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://10.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][[]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
```

```

2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- ResponseValidationContext:
    IdP URI: PingFederate
    SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
    Assertion Consumer URL: https://10.36.157.210:8443/portal/SSOLoginResponse.action
    Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER10.36.157.210
    Client Address: 10.0.25.62
    Load Balancer: null
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Validate signature to SAML standard
with cert:CN=10.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for guest
IDPResponse
:
    IdP ID: PingFederate
    Subject: guest
    SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
    SAML Success:true
    SAML Status Message:null
    SAML email:guest@example
    SAML Exception:null
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED

```

Informações Relacionadas

- [Exemplo de configuração da Autenticação da Web Central com Cisco WLC e ISE.](#)
- [Exemplo de Configuração da Autenticação Central da Web com um Switch e um Identity Services Engine.](#)
- [Notas de versão do Cisco Identity Services Engine, Versão 2.1](#)
- [Guia do Administrador do Cisco Identity Services Engine, Versão 2.1](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.