

Configurer le portail invité ISE 2.1 avec PingFederate SAML SSO

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation du flux](#)

[Flux attendu pour cet exemple d'utilisation](#)

[Configurer](#)

[Étape 1. Préparation d'ISE à l'utilisation d'un fournisseur d'identité SAML externe](#)

[Étape 2. Configurer le portail Invité pour utiliser un fournisseur d'identité externe](#)

[Étape 3. Configurez PingFederate pour qu'il agisse en tant que fournisseur d'identités pour ISE Guest Portal](#)

[Étape 4. Importer des métadonnées IdP dans le profil du fournisseur SAML externe ISE](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer les fonctionnalités SSO (Single Sign On) de Cisco Identity Services Engine (ISE) version 2.1 pour le langage SAML (Security Assertion Markup Language) du portail invité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Services invités Cisco Identity Services Engine.
- Connaissances de base sur SAML SSO.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine version 2.1
- PingFederate 8.1.3.0 server à partir de Ping Identity en tant que fournisseur d'identité 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation du flux

SAML est une norme XML permettant d'échanger des données d'authentification et d'autorisation entre des domaines de sécurité.

La spécification SAML définit trois rôles : le principal (utilisateur invité), le fournisseur d'identités [IdP] (serveur IPing Federate) et le fournisseur de services [SP] (ISE).

Dans un flux SAML SSO typique, le SP demande et obtient une affirmation d'identité du fournisseur d'identité. En fonction de ce résultat, ISE peut prendre des décisions de stratégie, car le fournisseur d'identité peut inclure des attributs configurables qu'ISE peut utiliser (par exemple, le groupe et l'adresse e-mail associés à l'objet AD).

Flux attendu pour cet exemple d'utilisation

1. Le contrôleur LAN sans fil (WLC) ou le commutateur d'accès est configuré pour un flux d'authentification Web centrale (CWA) typique.

Conseil : retrouvez les exemples de configuration des flux CWA dans la section Informations connexes au bas de l'article.

2. Le client se connecte et la session est authentifiée par rapport à ISE. Le périphérique d'accès réseau (NAD) applique les paires de valeurs d'attributs de redirection (AVP) renvoyées par ISE (url-redirect-acl et url-redirect).

3. Le client ouvre le navigateur, génère du trafic HTTP ou HTTPS et est redirigé vers le portail invité d'ISE.

4. Une fois sur le portail, le client pourra entrer les informations d'identification d'invité précédemment attribuées (**Créé par le sponsor**) et configurer lui-même un nouveau compte d'invité ou utiliser ses informations d'identification Active Directory pour se connecter (**Connexion de l'employé**), ce qui fournira des fonctionnalités d'authentification unique via SAML.

5. Une fois que l'utilisateur a sélectionné l'option « Employee Login », l'ISE vérifie si une assertion active est associée à la session de navigateur de ce client par rapport au fournisseur d'identité. S'il n'y a aucune session active, le fournisseur d'identités appliquera la connexion de l'utilisateur. À cette étape, l'utilisateur est invité à entrer directement les informations d'identification Active Directory dans le portail IdP.

6. Le fournisseur d'identité authentifie l'utilisateur via LDAP et crée une nouvelle assertion qui reste active pendant une durée configurable.

Remarque : Ping Federate applique par défaut un **délai d'expiration de session** de 60 minutes (ce qui signifie que s'il n'y a pas de demandes de connexion SSO d'ISE dans les 60 minutes après l'authentification initiale, la session est supprimée) et un **délai d'expiration maximal de session** de 480 minutes (même si le fournisseur d'identité a reçu des demandes

de connexion SSO constantes d'ISE pour cet utilisateur, la session expirera dans 8 heures).

Tant que la session d'assertion est toujours active, l'employé est soumis à l'authentification unique lorsqu'il utilise le portail invité. Une fois la session expirée, une nouvelle authentification d'utilisateur sera appliquée par le fournisseur d'identité.

Configurer

Cette section décrit les étapes de configuration permettant d'intégrer ISE à Ping Federate et explique comment activer l'authentification unique du navigateur pour le portail invité.

Remarque : bien que diverses options et possibilités existent lorsque vous authentifiez des utilisateurs invités, toutes les combinaisons ne sont pas décrites dans ce document. Cependant, cet exemple vous fournit les informations nécessaires pour comprendre comment modifier l'exemple en fonction de la configuration précise que vous souhaitez obtenir.

Étape 1. Préparation d'ISE à l'utilisation d'un fournisseur d'identité SAML externe

1. Sur Cisco ISE, choisissez **Administration > Identity Management > External Identity Sources > SAML Id Providers**.
2. Cliquez sur **Add**.
3. Sous l'onglet **Général**, entrez un **nom de fournisseur d'ID**. Cliquez sur **Save**. Le reste de la configuration dans cette section dépend des métadonnées qui doivent être importées à partir du fournisseur d'identité dans les étapes ultérieures.

The screenshot displays the Cisco ISE administration interface. The top navigation bar includes 'Identity Services Engine' and various menu items like 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded to show 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Services'. Under 'Identity Management', 'External Identity Sources' is selected, and the 'SAML Id Providers' sub-menu is active.

The main content area is titled 'External Identity Sources' and shows a list of provider types: Certificate Authentication Profile, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, and SAML Id Providers. The 'SAML Id Providers' folder is expanded, showing a list of providers. The selected provider is 'PingFederate', and its configuration page is displayed. The configuration page has three tabs: 'General', 'Identity Provider Config.', and 'Service Provider Info.'. The 'General' tab is active, showing the following fields:

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

Étape 2. Configurer le portail Invité pour utiliser un fournisseur d'identité externe

1. Choisissez **Work Centers > Guest Access > Configure > Guest Portals**.
2. Créez un nouveau portail et sélectionnez **Self-Registered Guest Portal**.

Remarque : il ne s'agira pas du portail principal que l'utilisateur utilisera, mais d'un sous-portail qui interagira avec le fournisseur d'identité afin de vérifier l'état de la session. Ce portail s'appelle SSOSubPortal.

3. Développez **Paramètres du portail** et choisissez **PingFederate** pour **Méthode d'authentification**.

4. Dans **Séquence source d'identité**, choisissez le fournisseur d'ID SAML externe précédemment défini (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. Développez les sections **Acceptable Use Policy(AUP)** et **Post-Login Banner Page Settings** et désactivez les deux.

Le flux du portail est :



6. Enregistrez les modifications.

7. Retournez à Guest Portals et créez-en un nouveau avec l'option **Self-Registered Guest Portal**.

Remarque : il s'agit du portail principal visible par le client. Le portail principal utilisera le sous-portail SOS comme interface entre ISE et le fournisseur d'identité. Ce portail s'appelle PrimaryPortal.

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

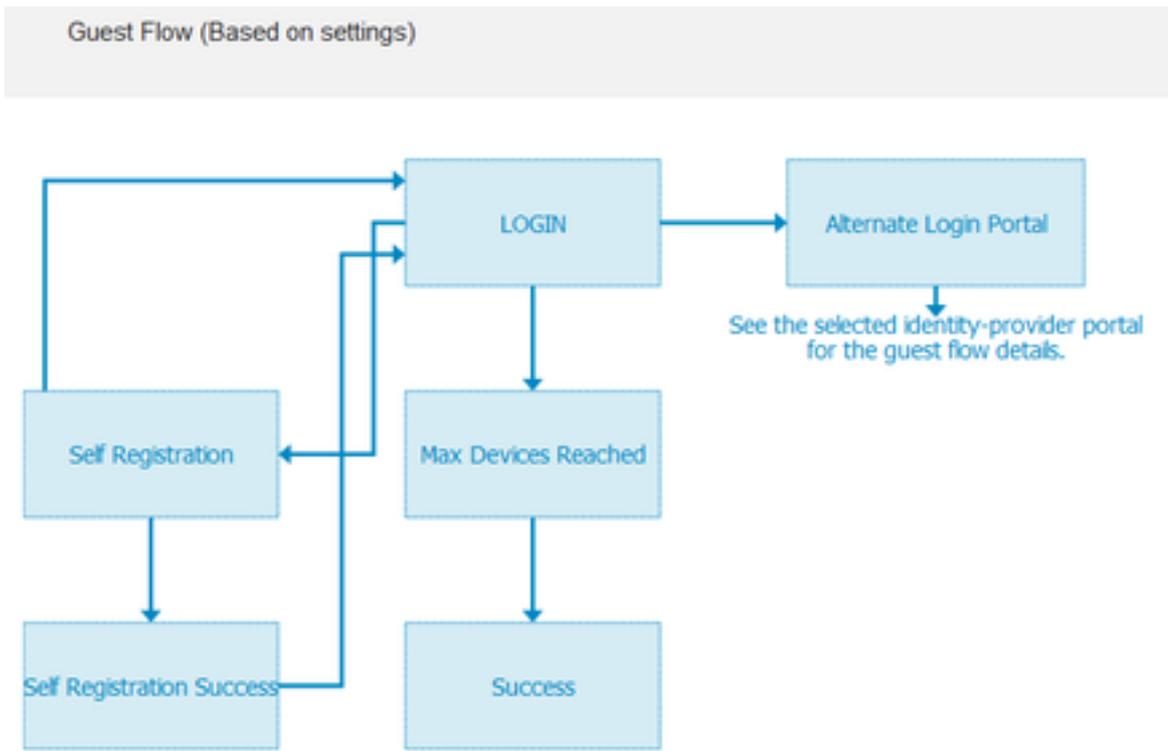
8. Développez **Login Page Settings** et choisissez le **SSOSubPortal** précédemment créé sous « **Allow the following identity-provider guest portal to be used for login** ».

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

SSOSubPortal

9. Développez les **paramètres des pages AUP et Bannière après connexion de la stratégie d'utilisation acceptable** et désactivez-les.

À ce stade, le flux du portail doit ressembler à ceci :



10. Choisissez **Portal Customization > Pages > Login**. Vous devez maintenant avoir la possibilité de personnaliser les **Options de connexion alternatives** (Icône, texte, etc.).

Alternative login: (static text)

Alternative login access portal:

Use this text: as link as icon tooltip

Remarque : notez que sur le côté droit, sous l'aperçu du portail, l'option de connexion supplémentaire est visible.

You can also login with



11. Cliquez sur **Enregistrer**.

Les deux portails apparaissent désormais sous la liste Guest Portal List.

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

Étape 3. Configurez PingFederate pour qu'il agisse en tant que fournisseur d'identités pour ISE Guest Portal

1. Dans ISE, choisissez **Administration > Identity Management > External identity Sources > SAML Id Providers > PingFederate** et cliquez sur **Service Provider Info**.
2. Sous **Export Service Provider Info**, cliquez sur **Export**.

SAML Identity Provider

General Identity Provider Config. Service Provider Info.

Service Provider Information

Load balancer ⓘ

Export Service Provider Info. **Export** ⓘ

3. Enregistrez et extrayez le fichier zip généré. Le fichier XML contenu ici est utilisé pour créer le profil dans PingFederate dans les étapes ultérieures.

SSOSubPortal.xml

Remarque : à partir de ce point, ce document couvre la configuration PingFederate. Cette configuration est identique pour plusieurs solutions telles que le portail des sponsors, MyDevices et les portails BYOD. (Ces solutions ne sont pas couvertes dans cet article).

4. Ouvrez le portail d'administration de PingFederate (généralement <https://ip:9999/pingfederate/app>).

5. Sous l'onglet **IdP Configuration > section SP Connections**, choisissez **Create New**.

IdP Configuration

APPLICATION INTEGRATION

[Adapters](#)

[Default URL](#)

[Application Endpoints](#)

AUTHENTICATION POLICIES

SP CONNECTIONS

Manage All

Create New

Import

6. Sous **Type de connexion**, cliquez sur **Suivant**.

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. Sous **Options de connexion**, cliquez sur **Suivant**.

SP Connection

Connection Type

Connection Options

Please select options that apply to this connection.



BROWSER SSO



IDP DISCOVERY



ATTRIBUTE QUERY

8. Sous **Importer des métadonnées**, cliquez sur la case d'option **Fichier**, cliquez sur **Choisir un fichier** et choisissez le fichier XML précédemment exporté à partir d'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. Sous **Résumé des métadonnées**, cliquez sur **Suivant**.

10. Sur la page Informations générales, sous Nom de la connexion, entrez un nom (par exemple ISEGuestWebAuth) et cliquez sur **Suivant**.

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11. Sous **Browser SSO**, cliquez sur **Configure Browser SSO** et sous **SAML Profiles** vérifiez les options et cliquez sur **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. Dans **Durée de vie des assertions**, cliquez sur **Suivant**.

13. Dans **Création d'assertions**, cliquez sur **Configurer la création d'assertions**.

14. Sous **Identity Mapping**, choisissez **Standard** et cliquez sur **Next**.

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. Dans Contrat d'attribut > **Prolonger le contrat**, saisissez le **message** d'attributs et le **membreDe**, puis cliquez sur **Ajouter**. Cliquez sur **Next (Suivant)**.

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

La configuration de cette option permet au fournisseur d'identité de passer les attributs **MemberOf** et **Email** fournis par Active Directory à ISE, qu'ISE peut utiliser ultérieurement comme condition lors de la décision de stratégie.

16. Sous **Authentication Source Mapping**, cliquez sur **Map New Adapter Instance**.

17. Dans **Instance d'adaptateur**, sélectionnez **Adaptateur de formulaire HTML**. Cliquez sur **Next (suivant)**.

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 from a partner.

ADAPTER INSTANCE

Adapter Contract

OVERRIDE INSTANCE SETTINGS

18. Sous **Méthodes de mappage**, sélectionnez la deuxième option vers le bas et cliquez sur **Suivant**.

- 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. Dans **Sources d'attribut et recherche utilisateur**, cliquez sur la case **Ajouter une source d'attribut**.

20. Sous **Banque de données**, entrez une description, choisissez instance de connexion LDAP dans **Banque de données active** et définissez le type de service d'annuaire. Si aucune banque de données n'est configurée, cliquez sur **Manage Data Stores** pour ajouter la nouvelle instance.

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. Sous **LDAP Directory Search**, définissez le **DN de base** pour la recherche d'utilisateur LDAP dans le domaine et cliquez sur **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=██████,DC=net
SEARCH SCOPE	Subtree

Remarque : ceci est important car il définit le DN de base lors de la recherche d'utilisateur LDAP. Un DN de base incorrectement défini entraînera la présence d'un objet introuvable dans le schéma LDAP.

22. Sous **LDAP Filter**, ajoutez la chaîne **sAMAccountName=\${username}** et cliquez sur **Next**.

SP Connection | Browser SSO | Assertion

Data Store	LDAP Directory Search	LDAP Filter
------------	-----------------------	-------------

Please enter a Filter for extracting data from your directory.

FILTER
sAMAccountName=\${username}

23. Sous **Attribut Exécution du contrat**, choisissez les options données et cliquez sur **Suivant**.

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

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. Vérifiez la configuration dans la section Résumé et cliquez sur **Terminé**.
25. Revenez à la page **Sources d'attributs et recherche d'utilisateur** et cliquez sur **Suivant**.
26. Sous **Failsafe Attribute Source**, cliquez sur **Next**.
27. Sous **Attribut Exécution du contrat**, choisissez ces options et cliquez sur **Suivant**.

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

28. Vérifiez la configuration dans la section Summary et cliquez sur **Done**.
29. Retour sur **Authentication Source Mapping** et cliquez sur **Next**.
30. Une fois la configuration vérifiée dans la page **Résumé**, cliquez sur **Terminé**.
31. Retour sur **Création d'assertion** cliquez sur **Suivant**.
32. Sous **Protocol Settings**, cliquez sur **Configure Protocol Settings**. À ce stade, deux entrées doivent déjà être renseignées. Cliquez sur **Next** (Suivant).

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://torise21a.rtpaaa.net:8443/portal/SSOLoginResponse.action

33. Sous URL du service SLO, cliquez sur **Suivant**.
34. Sur les liaisons SAML autorisées, décochez les options **ARTIFACT** et **SOAP** et cliquez sur **Suivant**.

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. Sous Signature Policy, cliquez sur **Next**.

36. Sous Encryption Policy, cliquez sur **Next**.

37. Vérifiez la configuration dans la page Résumé et cliquez sur **Terminé**.

38. Dans Browser SSO > Protocol settings, cliquez sur **Next**, validez la configuration, puis cliquez sur **Done**.

39. L'onglet SSO du navigateur apparaît. Cliquez sur **Next** (Suivant).

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. Sous **Credentials**, cliquez sur **Configure Credentials** et choisissez le certificat de signature à utiliser pendant la communication IdP à ISE et cochez l'option **Include the certificate in the signature**. Cliquez ensuite sur **Next**.

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

Remarque : si aucun certificat n'est configuré, cliquez sur **Manage Certificates (Gérer les certificats)** et suivez les invites afin de générer un **certificat auto-signé** à utiliser pour signer les communications IdP vers ISE.

41. Validez la configuration sous la page de résumé et cliquez sur **Done**.

42. Dans l'onglet **Informations d'identification**, cliquez sur **Suivant**.

43. Sous **Activation & Summary**, choisissez **Connection Status ACTIVE**, validez le reste de la configuration, puis cliquez sur **Done**.

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status ACTIVE INACTIVE

Étape 4. Importer des métadonnées IdP dans le profil du fournisseur SAML externe ISE

1. Sous la console de gestion PingFederate, choisissez **Server Configuration > Administrative Functions > Metadata Export**. Si le serveur a été configuré pour plusieurs rôles (IdP et SP), choisissez l'option **Je suis le fournisseur d'identité (IdP)**. Cliquez sur **Next (Suivant)**.
2. Sous **Metadata** mode, sélectionnez « **Select Information to Include In Metadata Manually** ». Cliquez sur **Next (Suivant)**.

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

3. Sous **Protocole**, cliquez sur **Suivant**.

4. Dans **Contrat d'attribut**, cliquez sur **Suivant**.

5. Sous **Signing Key**, sélectionnez le certificat précédemment configuré sur le profil de connexion. Cliquez sur **Next** (Suivant).

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 the public key, select the certificate from the list below.

DIGITAL SIGNATURE KEYS/CERTS

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

6. Sous **Signature des métadonnées**, sélectionnez le certificat de signature et cochez la case **Inclure la clé publique de ce certificat dans l'élément d'informations de clé**. Cliquez sur **Next** (Suivant).

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. Sous **Certificat de chiffrement XML**, cliquez sur **Suivant**.

Remarque : l'option permettant d'appliquer le cryptage est laissée à l'administrateur réseau.

8. Sous la section **Résumé**, cliquez sur **Exporter**. Enregistrez le fichier de métadonnées généré, puis cliquez sur **Terminé**.

Export Metadata

Metadata Role	Metadata Mode	Protocol	Attribute Contract	Signing Key	Metadata Signing	XML Encryption Certificate	Export & Summary
Click the Export button to export this metadata to the file system.							
Export Metadata							
Metadata Role							
Metadata role	Identity Provider						
Metadata Mode							
Metadata mode	Select information manually						
Use the secondary port for SOAP channel	false						
Protocol							
Protocol	SAML 2.0						
Attribute Contract							
Attribute	None defined						
Signing Key							
Signing Key	CN=14.36347L, OU=TAC, O=Cisco, L=RTP, C=US						
Metadata Signing							
Signing Certificate	CN=14.36347L, OU=TAC, O=Cisco, L=RTP, C=US						
Include Certificate in KeyInfo	false						
Include Raw Key in KeyValue	false						
Selected Signing Algorithm	RSA SHA256						
XML Encryption Certificate							
Encryption Keys/Certs	NONE						

Export

Cancel Previous Done

9. Sous ISE, choisissez **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate**.

10. Cliquez sur **Identity Provider Config > Browse** et continuez à importer les métadonnées enregistrées à partir de l'opération d'exportation de métadonnées PingFederate.

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

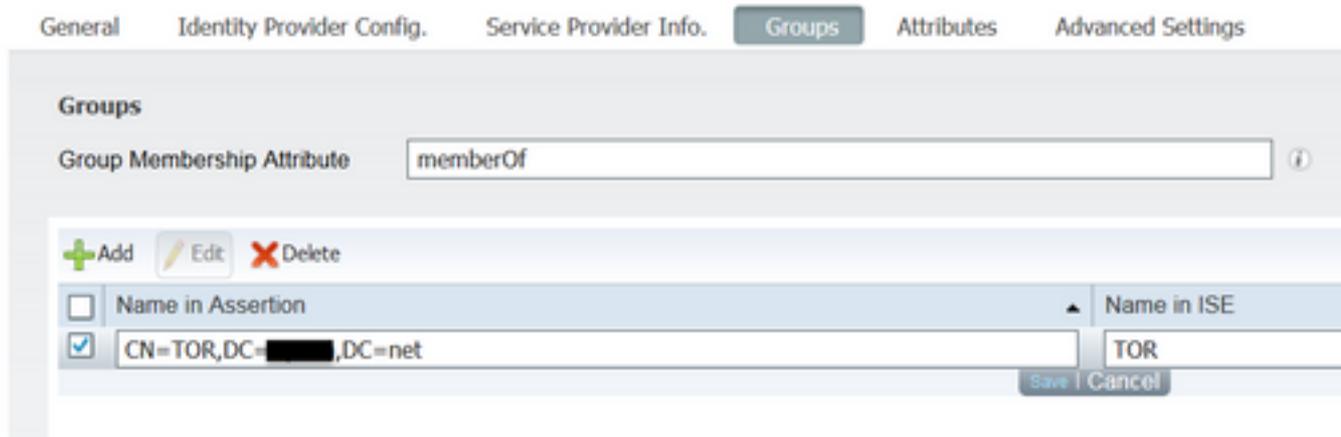
Signing Certificates

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

11. Sélectionnez l'onglet **Groupes**, sous **Attribut d'appartenance au groupe**, ajoutez **memberOf**, puis cliquez sur **Ajouter**

Sous **Name in Assertion**, ajoutez le nom unique que le **fournisseur d'identités** doit renvoyer lorsque l'attribut **memberOf** est récupéré à partir de l'authentification LDAP. Dans ce cas, le groupe configuré est lié au groupe sponsor de TOR et le DN de ce groupe est le suivant :

SAML Identity Provider



The screenshot shows the 'Groups' configuration page for a SAML Identity Provider. The 'Group Membership Attribute' is set to 'memberOf'. Below this, there are buttons for '+ Add', 'Edit', and 'Delete'. A table lists the groups:

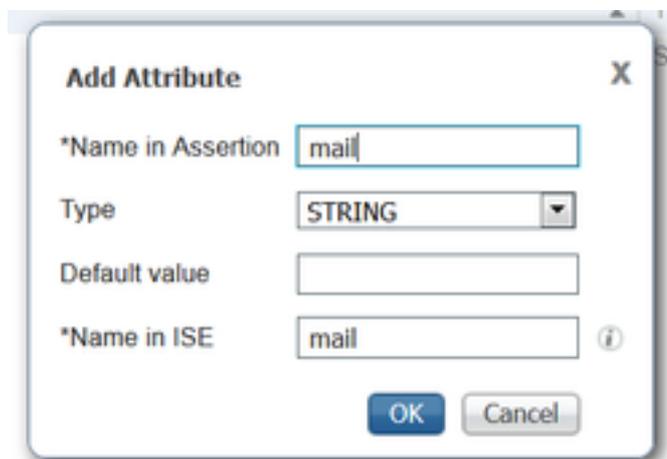
<input type="checkbox"/>	Name in Assertion	Name in ISE
<input checked="" type="checkbox"/>	CN=TOR,DC=[REDACTED],DC=net	TOR

Buttons for 'Save' and 'Cancel' are visible at the bottom right of the table.

Une fois que vous avez ajouté le DN et la description « Nom dans ISE », cliquez sur **OK**.

12. Sélectionnez l'onglet **Attributs** et cliquez sur **Ajouter**.

À cette étape, ajoutez l'attribut « mail » qui est contenu dans le jeton SAML transmis par le fournisseur d'identité qui, en fonction de la requête ping sur LDAP, doit contenir l'attribut email pour cet objet.



The 'Add Attribute' dialog box is shown with the following fields:

- *Name in Assertion: mail
- Type: STRING
- Default value: (empty)
- *Name in ISE: mail

Buttons for 'OK' and 'Cancel' are at the bottom.

Remarque : les étapes 11 et 12 garantissent qu'ISE reçoit les attributs Email et MemberOf de l'objet AD via l'action de connexion IdP.

Vérier

1. Lancez le portail invité à l'aide de l'URL de test du portail ou en suivant le flux CWA. L'utilisateur aura la possibilité d'entrer des informations d'identification d'invité, de créer son propre compte et de se connecter à l'employé.

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. Cliquez sur **Connexion employé**. Puisqu'il n'y a pas de sessions actives, l'utilisateur sera redirigé vers le portail de connexion IdP.

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

3. Entrez les informations d'identification AD et cliquez sur **Sign On**.

4. L'écran d'ouverture de session IdP redirige l'utilisateur vers la page Guest Portal Success.



Success

You now have Internet access through this network.

5. À ce stade, chaque fois que l'utilisateur revient sur le portail invité et choisit « **Employee Login** », il est autorisé à accéder au réseau tant que la session est toujours active dans le fournisseur d'identité.

Dépannage

Tout problème d'authentification SAML sera consigné sous `ise-psc.log`. Il existe un composant dédié (SAML) sous **Administration > Logging > Debug log Configuration > Select the node in question > Set SAML component to debug level**.

Vous pouvez accéder à ISE via l'interface de ligne de commande et entrer la commande **show logging application ise-psc.log tail** et surveiller les événements SAML, ou vous pouvez télécharger `ise-psc.log` pour une analyse plus approfondie sous **Operations > Troubleshoot > Download Logs > Sélectionnez le noeud ISE > onglet Debug Logs > cliquez sur ise-psc.log** pour télécharger les journaux.

```
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
```

Informations connexes

- [Exemple de configuration de l'authentification Web centralisée avec Cisco WLC et ISE.](#)
- [Exemple de configuration de l'authentification Web centrale avec un commutateur et Identity Services Engine.](#)
- [Notes de version de Cisco Identity Services Engine, version 2.1](#)
- [Guide de l'administrateur de Cisco Identity Services Engine, version 2.1](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.