

Configuratie ISE 2.1 Guest Portal met PingFederate SAML SSO

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Flow - Overzicht](#)

[Verwachte doorloop voor deze gebruikscase](#)

[Configureren](#)

[Stap 1. Voorbereiden op ISE voor gebruik van een externe SAML Identity Provider](#)

[Stap 2. Het gastportal configureren voor gebruik van een externe identiteitsprovider](#)

[Stap 3. PingFederate configureren om op te treden als Identity Provider voor ISE Guest Portal](#)

[Stap 4. IDp-metagegevens importeren in ISE-profiel van externe SAML IDP-provider](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de mogelijkheden van Cisco Identity Services Engine (ISE), versie 2.1 Single Sign On (SSO), kunt configureren voor guest portal Security Assertion Markup Language (SAML).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Gastservices voor Cisco Identity Services Engine.
- Basiskennis van SAML SSO.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.1
- PingFederate 8.1.3.0-server van Ping Identity as SAML Identity Provider (IDP)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Flow - Overzicht

SAML is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen beveiligingsdomeinen.

SAML-specificatie definieert drie rollen: de Principal (Guest User), de Identity Provider [IdP] (IPing Federate server) en de Service Provider [SP] (ISE).

In een typische SAML SSO-stroom vraagt en verkrijgt de SP een identiteitsbewering van de IdP. Op basis van dit resultaat kan ISE beleidsbeslissingen uitvoeren, omdat de IDP configureerbare kenmerken kan bevatten die ISE kan gebruiken (bijv. groep- en e-mailadres gekoppeld aan het AD-object).

Verwachte doorloop voor deze gebruikscase

1. Wireless LAN Controller (WLC) of Access switch is geconfigureerd voor een typische Central Web Verification (CWA)-stroom.

Tip: Vind de configuratievoorbeelden voor CWA-stromen in de sectie Verwante informatie onder aan het artikel.

2. De client maakt verbinding en de sessie wordt geverifieerd op basis van ISE. Het Network Access Device (NAD) past de door ISE (url-redirect-acl en url-redirect) geretourneerde waardeparen van omleidingskenmerken (AVP's) toe.

3. De client opent de browser, genereert HTTP- of HTTPS-verkeer en wordt omgeleid naar de ISE-gastenportal.

4. Eenmaal in de portal zal de client in staat zijn om eerder toegewezen gastreferenties (**Sponsor Created**) in te voeren en zelf te voorzien van een nieuw gastaccount of gebruik zijn AD-referenties om in te loggen (**Employee Login**) die Single Sign On-mogelijkheden zal bieden via SAML.

5. Zodra de gebruiker de optie "Aanmelden bij werknemer" selecteert, controleert de ISE of er een actieve bewering is gekoppeld aan de browsersessie van deze klant tegen de IDp. Als er geen actieve sessies zijn, zal de IdP de gebruikersaanmelding afdwingen. Bij deze stap zal de gebruiker worden gevraagd om AD-referenties in het IDP-portal direct in te voeren.

6. De IDp authenticceert de gebruiker via LDAP en maakt een nieuwe bewering die zal blijven leven voor een configureerbare tijd.

Opmerking: Ping Federate past standaard een **Sessietime-out** van 60 minuten toe (dit betekent dat als er geen SSO-inlogaanvragen van ISE zijn in 60 minuten na de eerste authenticatie de sessie wordt verwijderd) en een **Session Max-time-out** van 480 minuten (zelfs als de IdP constante SSO-inlogaanvragen van ISE heeft ontvangen voor deze gebruiker, zal de sessie verlopen in 8 uur).

Zolang de Assertion-sessie nog actief is, zal de werknemer SSO ervaren wanneer hij gebruik maakt van het Guest Portal. Zodra de sessietijden zijn verlopen, wordt een nieuwe

gebruikersverificatie afgedwongen door de IDp.

Configureren

In deze sectie worden de configuratiestappen besproken om ISE met Ping Federate te integreren en hoe u Browser SSO voor het Guest Portal kunt inschakelen.

Opmerking: Hoewel er verschillende opties en mogelijkheden bestaan wanneer u Gastgebruikers authenticceert, worden niet alle combinaties beschreven in dit document. Dit voorbeeld geeft u echter de informatie die nodig is om te begrijpen hoe u het voorbeeld kunt aanpassen aan de exacte configuratie die u wilt bereiken.

Stap 1. Voorbereiden op ISE voor gebruik van een externe SAML Identity Provider

1. Kies in Cisco ISE **Beheer > Identity Management > Externe Identity Resources > SAML ID Providers**.
2. Klik op **Add (Toevoegen)**.
3. Voer onder **het** tabblad **General** een **naam in van de ID-provider**. Klik op **Save (Opslaan)**. De rest van de configuratie in deze sectie is afhankelijk van de metagegevens die in latere stappen uit de IDp moeten worden geïmporteerd.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Identity Management > External Identity Sources > Identity Source Sequences > Settings. The 'External Identity Sources' section is expanded to show 'SAML Id Providers'. The 'SAML Identity Provider' configuration page for 'PingFederate' is displayed, with the 'General' tab selected. The 'Id Provider Name' field contains 'PingFederate' and the 'Description' field contains 'SAML SSO IdP'.

Stap 2. Het gastportal configureren voor gebruik van een externe identiteitsprovider

1. Kies **Werkcentra > Gasttoegang > Configureren > Gastenportalen**.
2. Maak een nieuwe portal en kies **Self-Registered Guest Portal**.

Opmerking: dit is niet het hoofdportaal dat de gebruiker ervaart, maar een subportaal dat interageert met de IDp om de sessiestatus te controleren. Dit portaal heet SSOSubPortal.

3. Breid **Portal-instellingen** uit en kies **PingFederate** voor **Verificatiemethode**.
4. Kies uit **Identity Source Sequence** de externe SAML IDP die eerder is gedefinieerd

(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. Breid de secties **Acceptable Use Policy (AUP)** en **Post-Login Banner Page Settings** uit en schakel beide uit.

Poortstroom is:



6. Sla de wijzigingen op.

7. Ga terug naar Guest Portals en maak een nieuwe met de optie **Self-Registered Guest Portal**.

Opmerking: dit is de primaire portal die zichtbaar is voor de client. Het primaire portaal gebruikt het SOSubportal als interface tussen ISE en de IdP. Dit portaal heet PrimaryPortal.

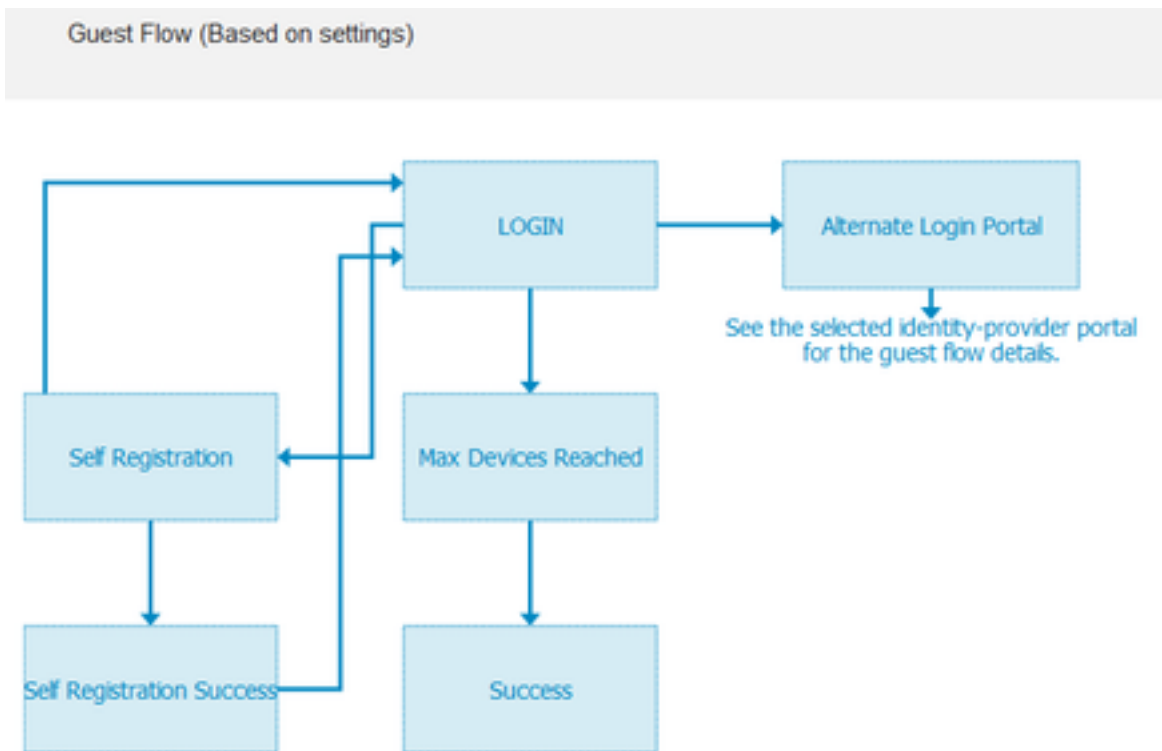
Portal Name: *	Description:
<input type="text" value="PrimaryPortal"/>	<input type="text" value="Portal visible to the client during CWA flow."/>

8. Breid de **inlogpagina-instellingen** uit en kies het **SOSubPortal** dat eerder is gemaakt onder "Toestaan dat de volgende identiteits-provider gastportal wordt gebruikt voor inloggen".

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

9. Breid de **instellingen voor Acceptable Use Policy AUP** en **Post-login Banner Page** uit en verwijder deze.

Op dit punt moet de portalstroom er als volgt uitzien:



10. Kies **Poortaanpassing > Pagina's > Aanmelden**. U moet nu de optie hebben om de **alternatieve inlogopties** aan te passen (pictogram, tekst, enzovoort).


Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



Opmerking: Merk op dat aan de rechterkant, onder de portal preview, de extra inlogoptie zichtbaar is.

You can also login with



11. Klik op **Opslaan**.

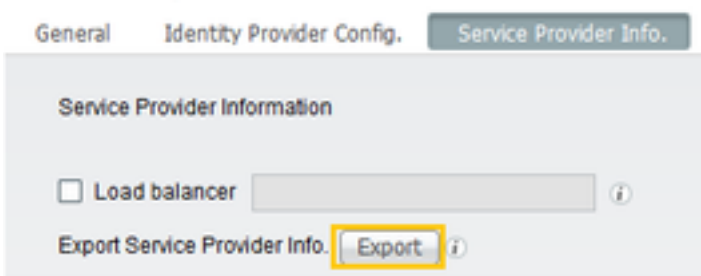
Beide portals staan nu onder de lijst van het gastportaal.

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

Stap 3. PingFederate configureren om op te treden als Identity Provider voor ISE Guest Portal

1. Kies in ISE **Beheer > Identity Management > Externe identiteitsbronnen > SAML ID Providers > PingFederate** en klik op **Service Provider Info**.
2. Klik onder **Exporteren** voor **Serviceprovider-informatie** op **Exporteren**.

SAML Identity Provider



3. Opslaan en het gegenereerde zip-bestand ophalen. Het XML-bestand hier wordt gebruikt om het profiel in PingFederate in latere stappen te maken.



Opmerking: vanaf dit punt behandelt dit document de configuratie van de PingFederate. Deze configuratie is hetzelfde voor meerdere oplossingen zoals Sponsor portal, MyDevices en BYOD portals. (Deze oplossingen vallen niet onder dit artikel).

4. Open het PingFederate-beheerportal (meestal <https://ip:9999/pingfederate/app>).
5. Kies onder het tabblad **IDP Configuration > sectie SP Connections Nieuw maken**.

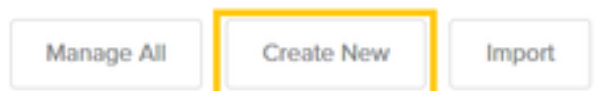
IdP Configuration

APPLICATION INTEGRATION

- Adapters
- Default URL
- Application Endpoints

AUTHENTICATION POLICIES

SP CONNECTIONS



6. Klik onder **Verbindingstype** op **Volgende**.

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. Klik onder **Verbindingsopties** op **Volgende**.

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. Klik onder **Metagegevens importeren** op het keuzerondje **Bestand**, klik op **Kies een bestand** en kies het XML-bestand dat eerder uit ISE is geëxporteerd.

SP Connection

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

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

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

No file selected

9. Klik onder **Metagegevens Samenvatting** op **Volgende**.

10. Voer op de pagina Algemene informatie onder Verbindingsnaam een naam in (zoals ISEGuestWebAuth) en klik op **Volgende**.

PARTNER'S ENTITY ID
(CONNECTION ID)

http://CiscoISE/5b4c

CONNECTION NAME

ISEGuestWebAuth

11. Onder **Browser SSO**, klik op **Configure Browser SSO** en onder **SAML Profiles** controleer de opties en klik op **Volgende**.

SP Connection | Browser SSO

SAML Profiles

Assertion Lifetime

Assertion Creation

Protocol Settings

Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are formatted. This information is used to configure the SAML configuration for your SP connection.

Single Sign-On (SSO) Profiles

Single Logout (SLO) Profiles

IDP-INITIATED SSO

IDP-INITIATED SLO

SP-INITIATED SSO

SP-INITIATED SLO

12. Klik op **de levenscyclus van de activering** op **Volgende**.

13. On **Assertion Creation** klik op **Configure Assertion Creation**.

14. Kies **Standaard** onder **Identity Mapping** en klik op **Volgende**.

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 the local user. This process may affect the way that the SP will look up and associate the user to a specific local account.



STANDARD: Send the SP a known attribute value as the name identifier. The

15. Voer op kenmerkencontract > **Uitbreidingscontract** de kenmerken **mail** en **lidVan in** en klik op **toevoegen**. Klik op **Next (Volgende)**.

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

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

Dankzij de configuratie van deze optie kan de Identity Provider de attributen **MemberOf** en **Email** die door Active Directory worden geboden doorgegeven aan ISE, die ISE later kan gebruiken als voorwaarde tijdens het beleidsbesluit.

16. Klik onder **Toewijzing van verificatiebronnen** op **Map nieuwe adapter instantie**.

17. On **Adapter Instance** kies **HTML Form Adapter**. Klik op **Volgende**

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: HTML Form Adapter

Adapter Contract

givenName

mail

memberOf

objectGUID

sn

username

userPrincipalName

OVERRIDE INSTANCE SETTINGS

18. Kies onder **Toewijzingsmethoden** de tweede optie uit en klik op **Volgende**.

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. Op **Attributen Source & User Lookup** klikt u op **Add Attribute Source** box.

20. Onder **Data Store** voer een beschrijving in en kies LDAP-verbindinginstantie uit **Active Data Store** en definieer welk type Directory Service dit is. Als er nog geen **gegevensopslag** geconfigureerd is, klikt u op **Gegevensopslag beheren** om de nieuwe instantie toe te voegen.

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. Onder **LDAP Directory Search** definieert u de **Base DN** voor LDAP gebruiker Lookup in het domein en klikt u op **Volgende**.

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

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

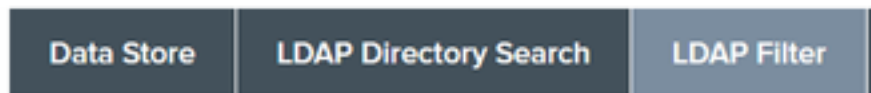
Please configure your directory search. This information, along with the attributes supplied in the contract, will be used

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

Opmerking: dit is belangrijk omdat het de basis-DN tijdens de LDAP-gebruiker lookup zal definiëren. Een onjuist gedefinieerde Base-DN zal resulteren in Object niet gevonden in LDAP-schema.

22. Onder **LDAP Filter** voeg de string **sAMAaccountName=\${gebruikersnaam}** toe en klik op **Volgende**.

SP Connection | Browser SSO | Assertion

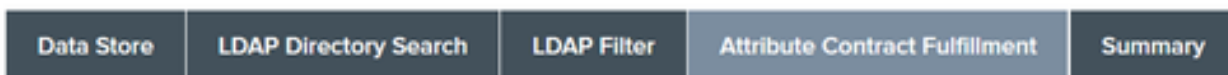


Please enter a Filter for extracting data from your directory.

FILTER

23. Selecteer onder **Attribute Contract Fulfillment** de gegeven opties en klik op **Next**.

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



Fulfill your Attribute Contract with values from the authentication adapter, dynamic text values, or from a data store lookup.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
mail	Adapter	mail
memberOf	Adapter	memberOf

24. Controleer de configuratie in het overzichtsgedeelte en klik op **Gereed**.

25. Terug in **Attribute Sources & User lookup** klikt u op **Volgende**.

26. Klik onder **Failsafe Attribute Source** op **Next**.

27. Selecteer onder **Attribute Contract Fulfillment** deze opties en klik op **Volgende**.

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

28. Controleer de configuratie in de overzichtsectie en klik op **Gereed**.
29. Terug op **Verificatie-brontoewijzing** klikt u op **Volgende**.
30. Zodra de configuratie onder de **overzichtspagina** is geverifieerd, klikt u op **Gereed**.
31. Terug op **Assertion Creation** klik op **Volgende**.
32. Klik onder **Protocolinstellingen** op **Protocolinstellingen configureren**. Op dit punt moeten er twee ingangen reeds bevolkt zijn. Klik op Next (Volgende).

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL	Allowable SAML Bindings	Signature Policy	Encryption Policy	Summary
--------------------------------	-------------------------	------------------	-------------------	---------

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible

Default	Index	Binding	Endpoint URL
default	0	POST	https://14.36.157.210:8443/portal/SSOLoginResponse.action
	1	POST	https://forise21a.rtpaaa.net:8443/portal/SSOLoginResponse.action

3. Klik onder URL's voor SND-service op **Volgende**.
34. Schakel op Toegestane SAML-banden de opties ARTIFACT en SOAP uit en klik op **Volgende**.

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. Klik onder Handtekeningsbeleid op **Volgende**.
36. Klik onder Encryptiebeleid op **Volgende**.
37. Controleer de configuratie op de overzichtspagina en klik op **Gereed**.
38. Terug op Browser SSO > Protocol instellingen klik op **Volgende**, valideer de configuratie en klik op **Gereed**.
39. Het tabblad SSO van de browser wordt weergegeven. Klik op **Next** (Volgende).

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. Onder **Credentials** klik op **Credentials configureren** en kies het ondertekeningscertificaat dat moet worden gebruikt tijdens IDp naar ISE-communicatie en controleer de optie **Certificaat opnemen in handtekening**. Klik vervolgens op **Volgende**.

SP Connection | Credentials

Digital Signature Settings	Signature Verification Settings	Summary
----------------------------	---------------------------------	---------

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/c

SIGNING CERTIFICATE	01:55:31:36:ED:D8 (cn=██████████147.1) ▼
<input checked="" type="checkbox"/>	INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.
<input type="checkbox"/>	INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.
SIGNING ALGORITHM	RSA SHA256 ▼

Opmerking: Als er geen certificaten geconfigureerd zijn, klikt u op **Certificaten beheren** en volgt u de aanwijzingen om een **zelfondertekend certificaat** te genereren dat gebruikt moet worden voor het ondertekenen van IDP-naar-ISE-communicatie.

41. Bevestig de configuratie onder de overzichtspagina en klik op **Gereed**.

42. Terug op het tabblad **Credentials** klikt u op **Volgende**.

43. Kies onder **Activering en Samenvatting de Verbindingsstatus ACTIEF**, valideer de rest van de configuratie en klik op **Gereed**.

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

Stap 4. IDp-metagegevens importeren in ISE-profiel van externe SAML IDP-provider

1. Kies onder de PingFederate beheerconsole **Serverconfiguratie > Administratieve functies > Metagegevens exporteren**. Als de server is geconfigureerd voor meerdere rollen(IdP en SP), kies dan de optie **Ik ben de Identity Provider (IDP)**. Klik op **Next (Volgende)**.
2. Selecteer onder **Metagegevens** modus "**Informatie selecteren om handmatig in metagegevens op te nemen**". Klik op Next (Volgende).

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. Klik onder **Protocol** op **Volgende**.

4. Klik op **Volgende op het contract voor kenmerken**.

5. Kies onder **Sleutel Ondertekenen** het certificaat dat eerder in het verbindingsprofiel is geconfigureerd. Klik op **Next (Volgende)**.

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. Onder **Metadata Signing** kies je het ondertekeningscertificaat en check **Neem de openbare sleutel van dit certificaat op in het sleutelinfo element**. Klik op **Next (Volgende)**.

SIGNING CERTIFICATE

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

SIGNING ALGORITHM

7. Klik onder **XML-encryptie certificaat** op **Volgende**.

Opmerking: de optie om de codering hier uit te voeren is aan de Network Admin.

8. Klik onder **Samenvatting** op **Exporteren**. Sla het gegenereerde Metagegevens-bestand op en klik op **Gereed**.

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=14.36.1471, OU=TAC, O=Cisco, L=RTIP, C=US
Metadata Signing	
Signing Certificate	CN=14.36.1471, OU=TAC, O=Cisco, L=RTIP, C=US
Include Certificate in KeyInfo	false
Include Raw Key in KeyValae	false
Selected Signing Algorithm	RSA SHA256
XML Encryption Certificate	
Encryption Keys/Certs	NONE

Export

Cancel Previous Done

9. Kies onder ISE voor **Administratie > Identity Management > Externe Identity Resources > SAML ID Providers > PingFederate**.

10. Klik op **Identity Provider Config > Bladeren** en ga verder met het importeren van de metagegevens die zijn opgeslagen uit de PingFederate Exportoperatie van metagegevens.

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. Kies het tabblad **Groepen**, onder **Groepsledenkenmerk** voeg **memberOf** toe en klik vervolgens op **Add**

Onder de **Naam in Bewering** voeg de Distinguished Name toe die de **IdP** moet retourneren wanneer **memberOf** attribuut wordt opgehaald van LDAP authenticatie. In dit geval is de gevormde groep verbonden met de sponsorgroep TOR en is de DN voor deze groep als volgt:

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Groups

Group Membership Attribute

memberOf



Name in Assertion



Name in ISE



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

TOR

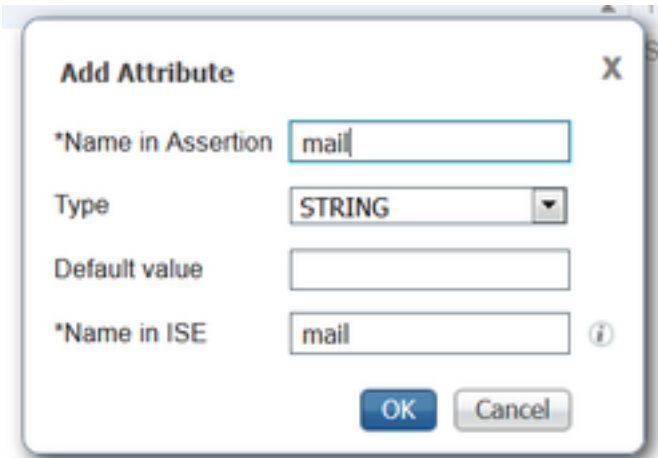
Save | Cancel

Zodra u de DN en "Name in ISE"-beschrijving toevoegt, klikt u op **OK**.

12. Kies het tabblad **Kenmerken** en klik op **Toevoegen**.

Bij deze stap, voeg het attribuut "mail" toe dat in het teken SAML bevat is dat van IdP wordt overgegaan dat gebaseerd op de vraag van Ping over LDAP, moet het de e-mailattributen voor

dat voorwerp bevatten.



Opmerking: Stappen 11 en 12 zorgen ervoor dat ISE de eigenschappen van het AD-object Email en MemberOf ontvangt via de inlogactie van IdP.

Verifiëren

1. Start het Gastenportaal met behulp van de Portal Test URL of door de CWA-stroom te volgen. De gebruiker zal de opties hebben om gastreferenties in te voeren, hun eigen account aan te maken en Werknemerslogin.

Sign On

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

Username:

Password:

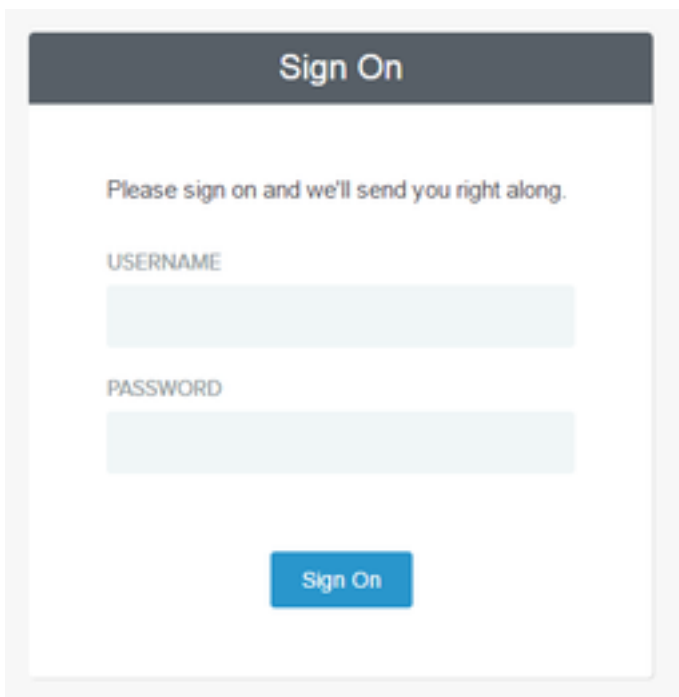
Sign On

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

You can also login with

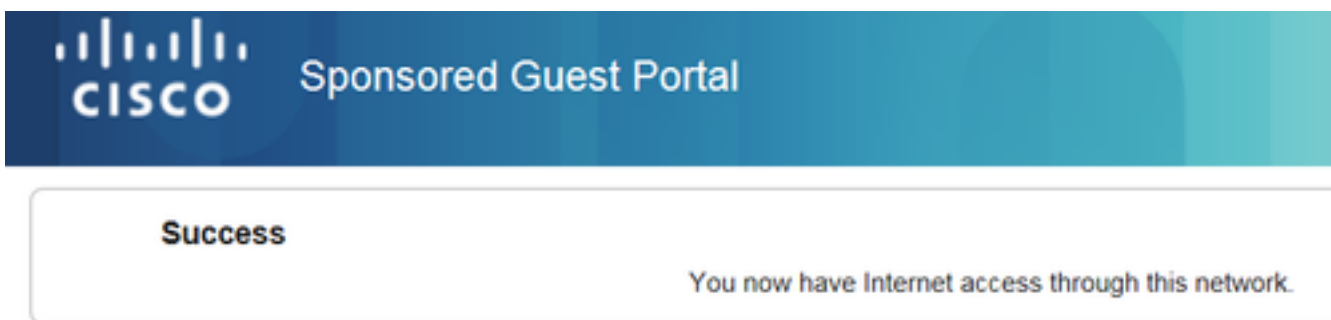


2. Klik op **Medewerker inloggen**. Aangezien er geen actieve sessies zijn, wordt de gebruiker doorgestuurd naar het inlogportal van IdP.

A screenshot of a 'Sign On' form. At the top, there is a dark header with the text 'Sign On'. Below the header, the text 'Please sign on and we'll send you right along.' is displayed. There are two input fields: one labeled 'USERNAME' and one labeled 'PASSWORD'. Below the input fields is a blue button with the text 'Sign On'.

3. Voer referenties voor advertenties in en klik op **Aanmelden**.

4. Het aanmeldingsscherm van de IDp zal de gebruiker doorverwijzen naar de Succespagina van het Guest Portal.



5. Op dit punt, elke keer dat de gebruiker terugkomt naar het Gastenportaal en "Werknemerslogin" kiest zullen zij in het netwerk worden toegestaan zolang de Sessie nog actief is in de IDp.

Problemen oplossen

Alle problemen met SAML-verificatie worden vastgelegd onder ise-psc.log. Er is een speciale component (SAML) onder **Beheer > Vastlegging > Debug log Configuration > Selecteer het knooppunt in kwestie > Stel SAML-component in om niveau te zuiveren**.

U kunt toegang krijgen tot ISE via CLI en de opdracht **show logging applicatie ise-psc.log** **start** invoeren en de SAML-gebeurtenissen bewaken, of u kunt ISE-psc.log downloaden voor verdere analyse onder **Operations > Troubleshoot > Download Logs > Selecteer de ISE-node > Debug Logs tabblad > klik op ISE-psc.log** om de logs te downloaden.

```
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

```

Gerelateerde informatie

- [Centrale webverificatie met configuratievoorbeeld Cisco WLC en ISE.](#)
- [Central Web Verification met een configuratievoorbeeld van een Switch- en Identity Services Engine.](#)
- [Releaseopmerkingen voor Cisco Identity Services Engine, release 2.1](#)
- [Beheerdershandleiding voor Cisco Identity Services Engine, release 2.1](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.