

Konfigurieren des ISE 2.1-Gastportals mit PingFederate SAML SSO

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Flussübersicht](#)

[Erwarteter Ablauf für diesen Anwendungsfall](#)

[Konfigurieren](#)

[Schritt 1: Vorbereiten der ISE auf die Verwendung eines externen SAML-Identitätsanbieters](#)

[Schritt 2: Konfigurieren des Gastportals zur Verwendung eines externen Identitätsanbieters](#)

[Schritt 3: Konfigurieren von PingFederate als Identitätsanbieter für das ISE-Gastportal](#)

[Schritt 4: Import von IDp-Metadaten in das externe ISE-SAML-IDp-Anbieterprofil](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Funktionen der Cisco Identity Services Engine (ISE) Version 2.1 Single Sign On (SSO) für das Gastportal Security Assertion Markup Language (SAML) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Identity Services Engine-Gastservices.
- Grundkenntnisse über SAML SSO.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine Version 2.1
- PingFederate 8.1.3.0-Server von Ping Identity als SAML Identity Provider(IdP)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Flussübersicht

SAML ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen.

Die SAML-Spezifikation definiert drei Rollen: den Principal (Gastbenutzer), den Identity Provider (IdP) (IPing Federate-Server) und den Service Provider (SP) (ISE).

In einem typischen SAML SSO-Fluss fordert der SP eine Identitätszusicherung an und ruft diese vom IdP ab. Auf der Grundlage dieses Ergebnisses kann die ISE Richtlinienentscheidungen durchführen, da die IdP konfigurierbare Attribute enthalten kann, die die ISE verwenden kann (d. h. Gruppen- und E-Mail-Adresse, die mit dem AD-Objekt verknüpft ist).

Erwarteter Ablauf für diesen Anwendungsfall

1. Der Wireless LAN Controller (WLC) oder Access Switch wird für einen typischen CWA-Datenstrom (Central Web Authentication) konfiguriert.

Tip: Konfigurationsbeispiele für CWA-Flows finden Sie im Abschnitt "Related Information" (Verwandte Informationen) unten im Artikel.

2. Der Client stellt eine Verbindung her und die Sitzung wird über die ISE authentifiziert. Das Netzwerkzugriffgerät (Network Access Device, NAD) wendet die von ISE(url-redirect-acl und url-redirect) zurückgegebenen Wertepaare für Umleitungsattribute (AVPs) an.

3. Der Client öffnet den Browser, generiert HTTP- oder HTTPS-Datenverkehr und wird zum Gastportal der ISE umgeleitet.

4. Sobald der Client das Portal betritt, kann er zuvor zugewiesene Gastzugangsdaten eingeben (vom **Sponsor erstellt**) und ein neues Gastkonto selbst bereitstellen oder seine AD-Anmeldeinformationen für die Anmeldung verwenden (**Mitarbeiteranmeldung**), um über SAML Single Sign On-Funktionen bereitzustellen.

5. Sobald der Benutzer die Option "Employee Login" (Mitarbeiteranmeldung) ausgewählt hat, überprüft die ISE, ob eine aktive Assertion für die IdP mit der Browser-Sitzung dieses Clients verbunden ist. Wenn keine aktiven Sitzungen vorhanden sind, erzwingt die IdP die Benutzeranmeldung. In diesem Schritt wird der Benutzer aufgefordert, AD-Anmeldeinformationen direkt in das IdP-Portal einzugeben.

6. Der IdP authentifiziert den Benutzer über LDAP und erstellt eine neue Assertion, die für eine konfigurierbare Zeit am Leben bleibt.

Hinweis: Ping Federate wendet standardmäßig ein **Session-Timeout** von 60 Minuten (d. h., wenn innerhalb von 60 Minuten nach der ersten Authentifizierung keine SSO-Anmeldeanforderungen von ISE vorliegen, wird die Sitzung gelöscht) und ein **Session Max Timeout** von 480 Minuten (auch wenn die IdP für diesen Benutzer konstante SSO-Anmeldeanforderungen von ISE erhalten hat, läuft die Sitzung in 8 Stunden ab) 1.

Solange die Assertion-Sitzung noch aktiv ist, erhält der Mitarbeiter bei der Nutzung des Gastportals eine SSO-Funktion. Sobald die Sitzung abgelaufen ist, wird von IdP eine neue Benutzerauthentifizierung erzwungen.

Konfigurieren

In diesem Abschnitt werden die Konfigurationsschritte zur Integration von ISE mit Ping Federate und die Aktivierung von Browser SSO für das Gastportal erläutert.

Hinweis: Bei der Authentifizierung von Gastbenutzern gibt es zwar verschiedene Optionen und Möglichkeiten, jedoch werden in diesem Dokument nicht alle Kombinationen beschrieben. In diesem Beispiel erhalten Sie jedoch die erforderlichen Informationen, um zu verstehen, wie Sie das Beispiel an die gewünschte Konfiguration anpassen können.

Schritt 1: Vorbereiten der ISE auf die Verwendung eines externen SAML-Identitätsanbieters

1. Wählen Sie auf der Cisco ISE **Administration > Identity Management > External Identity Sources > SAML Id Providers** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Registerkarte **Allgemein** einen **ID-Anbieternamen ein**. Klicken Sie auf **Speichern**. Der Rest der Konfiguration in diesem Abschnitt hängt von den Metadaten ab, die in späteren Schritten aus dem IdP importiert werden müssen.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation 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 displays the configuration for a SAML Identity Provider named 'PingFederate'. The 'General' tab is active, showing the 'Id Provider Name' field with the value 'PingFederate' and the 'Description' field with the value 'SAML SSO IdP'.

Schritt 2: Konfigurieren des Gastportals zur Verwendung eines externen Identitätsanbieters

1. Wählen Sie **Work Centers > Guest Access > Configure > Guest Portals** aus.
2. Erstellen Sie ein neues Portal, und wählen Sie **Self-Registered Guest Portal** aus.

Hinweis: Dies ist nicht das Hauptportal, das die Benutzererfahrung ermöglicht, sondern ein Subportal, das mit dem IdP interagiert, um den Sitzungsstatus zu überprüfen. Dieses Portal heißt SSOSubPortal.

3. Erweitern Sie **Portal Settings**, und wählen Sie **PingFederate** für die **Authentifizierungsmethode** aus.

4. Wählen Sie aus **Identity Source Sequence** die zuvor definierte externe SAML-IDp (PingFederate) aus.

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	<input type="text" value="PingFederate"/>	<input type="button" value="▼"/>	<input type="button" value="i"/>
method: *	<i>Configure authentication methods at:</i>		

5. Erweitern Sie die Abschnitte **Richtlinien zur akzeptablen Nutzung (AUP)** und **Einstellungen für die Bannerseite nach der Anmeldung**, und deaktivieren Sie beide.

Portalablauf:



6. Speichern Sie die Änderungen.

7. Gehen Sie zurück zu Guest Portals und erstellen Sie ein neues Portal mit der Option **Self-Registered Guest Portal**.

Hinweis: Dies ist das primäre Portal, das für den Client sichtbar ist. Das primäre Portal verwendet das SSOSubportal als Schnittstelle zwischen ISE und IdP. Dieses Portal heißt PrimaryPortal.

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

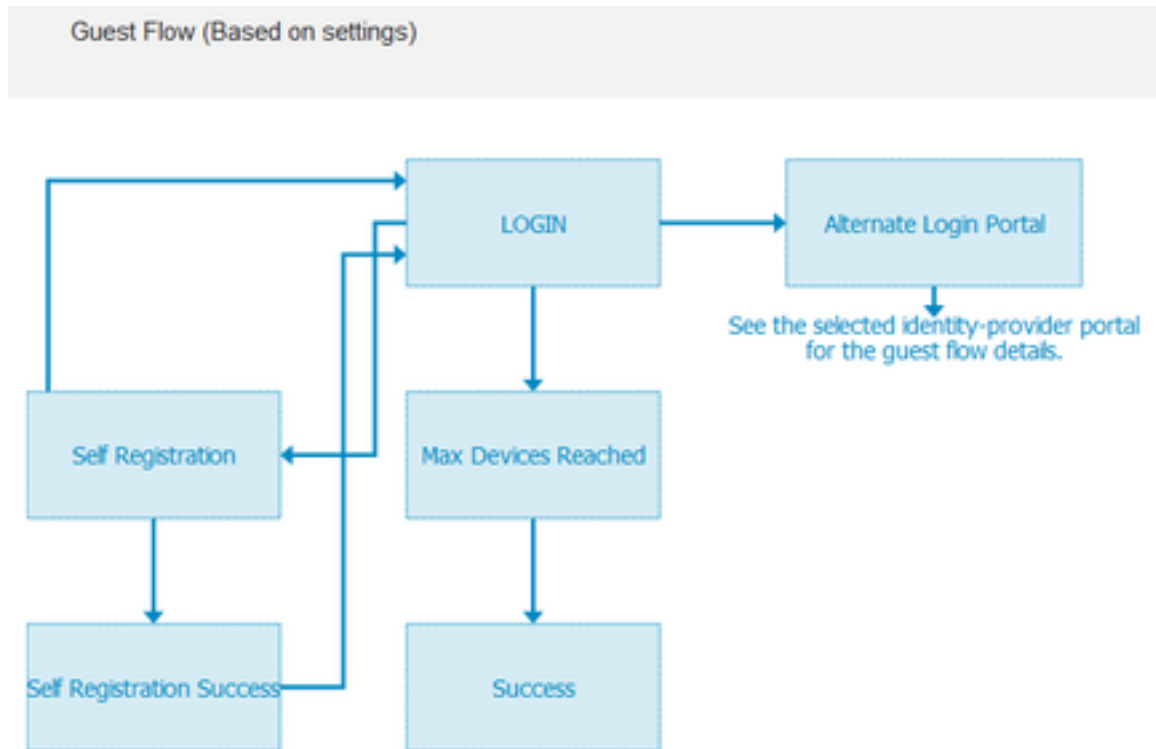
8. Erweitern Sie die **Anmeldeseiteneinstellungen**, und wählen Sie das zuvor unter "**Folgende Gastportal des Identitätsanbieters für die Anmeldung zulassen**" erstellte **SSOSubPortal** aus.

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

SSOSubPortal

9. Erweitern Sie die **Einstellungen** für die **Nutzungsrichtlinie** für die **Nutzungsrichtlinie** und die **Bannerseite nach der Anmeldung**, und deaktivieren Sie sie.

An dieser Stelle muss der Portalfluss wie folgt aussehen:



10. Wählen Sie **Portalanpassung > Seiten > Anmelden**. Sie müssen nun die Option haben, die **alternativen Anmeldeoptionen** (Symbol, Text usw.) anzupassen.


Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



Hinweis: Beachten Sie, dass auf der rechten Seite unter der Portalvorschau die zusätzliche Anmeldeoption sichtbar ist.

You can also login with



11. Klicken Sie auf **Speichern**.

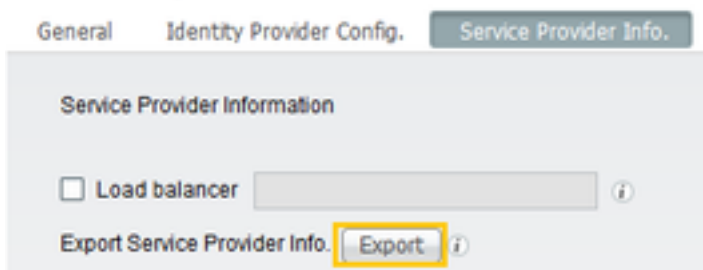
Beide Portale werden nun in der Liste des Gastportals angezeigt.

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

Schritt 3: Konfigurieren von PingFederate als Identitätsanbieter für das ISE-Gastportal

1. Wählen Sie in ISE Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate aus, und klicken Sie auf Service Provider Info.
2. Klicken Sie unter Export Service Provider Info auf Exportieren.

SAML Identity Provider



3. Speichern und extrahieren Sie die erstellte ZIP-Datei. Die hier enthaltene XML-Datei wird in späteren Schritten zum Erstellen des Profils in PingFederate verwendet.

 SSOSubPortal.xml

Hinweis: Ab diesem Punkt wird in diesem Dokument die PingFederate-Konfiguration behandelt. Diese Konfiguration ist für mehrere Lösungen wie das Sponsorportal, MyDevices und BYOD-Portale identisch. (Diese Lösungen werden in diesem Artikel nicht behandelt.)

4. Öffnen Sie das PingFederate-Admin-Portal (in der Regel <https://ip:9999/pingfederate/app>).
5. Wählen Sie auf der Registerkarte **IdP-Konfiguration > SP-Verbindungen** die Option **Neu erstellen**.

IdP Configuration

APPLICATION INTEGRATION

[Adapters](#)

[Default URL](#)

[Application Endpoints](#)

AUTHENTICATION POLICIES

SP CONNECTIONS

[Manage All](#)

[Create New](#)

[Import](#)

6. Klicken Sie unter **Verbindungstyp** auf **Weiter**.

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. Klicken Sie unter **Verbindungsoptionen** auf **Weiter**.

SP Connection

Connection Type

Connection Options

Please select options that apply to this connection.



BROWSER SSO



IDP DISCOVERY



ATTRIBUTE QUERY

8. Klicken Sie unter **Metadaten importieren** auf das Optionsfeld **Datei**, klicken Sie auf **Datei auswählen** und wählen Sie die zuvor von ISE exportierte XML-Datei aus.

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. Klicken Sie unter **Metadatenübersicht** auf **Weiter**.

10. Geben Sie auf der Seite Allgemeine Informationen unter Verbindungsname einen Namen ein (z. B. ISEGuestWebAuth), und klicken Sie auf **Weiter**.

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11. Klicken Sie unter **Browser SSO** auf **Browser SSO konfigurieren** und unter **SAML Profiles** die Optionen und klicken Sie auf **Weiter**.

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. On **Assertion lifetime** click **Next**.

13. Klicken Sie beim **Erstellen von Assertionen** auf **Assertion erstellen konfigurieren**.

14. Wählen Sie unter **Identitätszuordnung** die Option **Standard** aus, und klicken Sie auf **Weiter**.

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. Unter **Attributvertrag > Vertrag verlängern** geben Sie die Attribute **mail** und **memberOf** ein und klicken Sie auf **Hinzufügen**. Klicken Sie auf **Next (Weiter)**.

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:fnameid-format:unspecified	
Extend the Contract	Attribute Name Format	Action
mail	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete

Durch die Konfiguration dieser Option kann der Identitätsanbieter die von Active Directory bereitgestellten **MemberOf**- und **E-Mail**-Attribute an die ISE übergeben, die später als Bedingung für die Richtlinienentscheidung verwendet werden kann.

16. Klicken Sie unter **Authentifizierungsquellenzuordnung** auf **Neue Adapterinstanz zuordnen**.

17. On **Adapter Instance** wählen Sie **HTML Form Adapter**. Klicken Sie auf **Weiter**

SP Connection | Browser SSO | Assertion Creation

Adapter Instance | Mapping Method | Attribute Contract Full

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

ADAPTER INSTANCE:

Adapter Contract

givenName
mail
memberOf
objectGUID
sn
username
userPrincipalName

OVERRIDE INSTANCE SETTINGS

18. Wählen Sie unter **Zuordnungsmethoden** die zweite Option aus, und klicken Sie auf **Weiter**.

- 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. Klicken Sie bei **Attributquellen und Benutzersuche** auf **Attributquelle** hinzufügen.

20. Geben Sie unter **Datenspeicher** eine Beschreibung ein, wählen Sie die LDAP-Verbindungsinstanz im **aktiven Datenspeicher** aus, und legen Sie fest, welcher Typ von Verzeichnisdienst dies ist. Wenn noch keine **Datenspeicher** konfiguriert sind, klicken Sie auf **Datenspeicher verwalten**, um die neue Instanz hinzuzufügen.

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 Description

ATTRIBUTE SOURCE DESCRIPTION	<input type="text" value="██████████.net"/>
ACTIVE DATA STORE	<input type="text" value="██████████.net"/>
DATA STORE TYPE	LDAP
<input type="button" value="Manage Data Stores"/>	

21. Definieren Sie unter **LDAP-Verzeichnissuche** die **Basis-DN** für die LDAP-Benutzersuche in der Domäne, und klicken Sie auf **Weiter**.

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

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

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

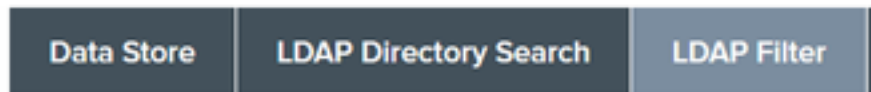
BASE DN	<input type="text" value="CN=Users,DC=██████████,DC=net"/>
SEARCH SCOPE	<input type="text" value="Subtree"/>

Hinweis: Dies ist wichtig, da die Basis-DN während der LDAP-Benutzersuche definiert wird.

Ein falsch definierter Basis-DN führt dazu, dass das Objekt im LDAP-Schema nicht gefunden wird.

22. Fügen Sie unter **LDAP-Filter** die Zeichenfolge **sAMAccountName=\${username}** hinzu, und klicken Sie auf **Weiter**.

SP Connection | Browser SSO | Assertion

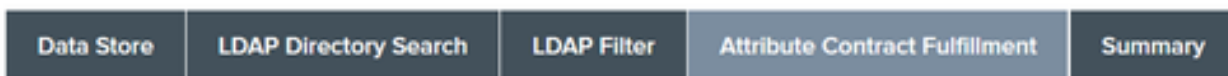


Please enter a Filter for extracting data from your directory.

FILTER

23. Wählen Sie unter **Erfüllung von Attributverträgen** die gewünschten Optionen aus, und klicken Sie auf **Weiter**.

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



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. Überprüfen Sie die Konfiguration im Abschnitt "Übersicht", und klicken Sie auf **Fertig**.

25. Zurück in **Attributquellen & Benutzer-Suche** klicken Sie auf **Weiter**.

26. Klicken Sie unter **Failsafe-Attributquelle** auf **Weiter**.

27. Wählen Sie unter **Erfüllung von Attributverträgen** diese Optionen aus, und klicken Sie auf **Weiter**.

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

28. Überprüfen Sie die Konfiguration im Abschnitt "Übersicht", und klicken Sie auf **"Fertig"**.

29. Zurück zur **Authentifizierungsquellenzuordnung** klicken Sie auf **Weiter**.

30. Nachdem die Konfiguration auf der Seite **Übersicht** überprüft wurde, klicken Sie auf **Fertig**.

31. Zurück zur **Erstellung von Assertionen** klicken Sie auf **Weiter**.

32. Klicken Sie unter **Protokolleinstellungen** auf **Protokolleinstellungen konfigurieren**. An dieser Stelle müssen zwei Einträge bereits ausgefüllt sein. Klicken Sie auf Next (Weiter).

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://orise21a.rtpaa.net:8443/portal/SSOLoginResponse.action

33. Klicken Sie unter SLO Service URLs auf **Weiter**.

34. Bei zulässigen SAML-Bindungen deaktivieren Sie die Optionen ARTIFACT und SOAP und klicken auf **Weiter**.

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. Klicken Sie unter Signaturreichtlinie auf **Weiter**.

36. Klicken Sie unter Verschlüsselungsrichtlinie auf **Weiter**.

37. Überprüfen Sie die Konfiguration auf der Seite "Übersicht", und klicken Sie auf **Fertig**.

38. Zurück zu Browser SSO > Protokolleinstellungen klicken Sie auf **Weiter**, validieren Sie die Konfiguration, und klicken Sie auf **Fertig**.

39. Die Registerkarte Browser SSO wird angezeigt. Klicken Sie auf **Next** (Weiter).

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. Klicken Sie unter **Anmeldedaten** auf **Anmeldedaten konfigurieren**, und wählen Sie das Signaturzertifikat aus, das während der IdP-ISE-Kommunikation verwendet werden soll, und aktivieren Sie die Option **Zertifikat in Signatur einschließen**. Klicken Sie dann auf **Weiter**.

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

Hinweis: Wenn keine Zertifikate konfiguriert sind, klicken Sie auf **Manage Certificates (Zertifikate verwalten)** und befolgen Sie die Anweisungen, um ein **selbstsigniertes Zertifikat** zu generieren, das zum Signieren von IDP-zu-ISE-Kommunikation verwendet wird.

41. Validieren Sie die Konfiguration auf der Übersichtsseite, und klicken Sie auf **Fertig**.

42. Klicken Sie auf der Registerkarte **Anmeldeinformationen** erneut auf **Weiter**.

43. Wählen Sie unter **Aktivierung und Zusammenfassung** die Option **Verbindungsstatus AKTIV**, validieren Sie den Rest der Konfiguration, und klicken Sie auf **Fertig**.

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						

Schritt 4: Import von IDp-Metadaten in das externe ISE-SAML-IDp-Anbieterprofil

1. Wählen Sie in der PingFederate-Verwaltungskonsole **Serverkonfiguration > Verwaltungsfunktionen > Metadatenexport** aus. Wenn der Server für mehrere Rollen (IdP und SP) konfiguriert wurde, wählen Sie die Option **I am the Identity Provider (IdP)**. Klicken Sie auf **Next (Weiter)**.
2. Wählen Sie im **Metadaten**-Modus "**Informationen für manuelles Einfügen auswählen**" aus. Klicken Sie auf **Next (Weiter)**.

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. Klicken Sie unter **Protokoll** auf **Weiter**.

4. Klicken Sie auf **Attributvertrag** auf **Weiter**.

5. Wählen Sie unter **Signaturschlüssel** das zuvor für das Verbindungsprofil konfigurierte Zertifikat aus. Klicken Sie auf **Next (Weiter)**.

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. Wählen Sie unter **Metadaten-signierung** das Signaturzertifikat aus, und aktivieren Sie **Öffentlichen Schlüssel dieses Zertifikats in das Schlüsselinfo-Element einbeziehen**. Klicken Sie auf **Next (Weiter)**.

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. Klicken Sie unter **XML-Verschlüsselungszertifikat** auf **Weiter**.

Hinweis: Die Verschlüsselung kann hier vom Netzwerkadministrator erzwungen werden.

8. Klicken Sie im Abschnitt "**Übersicht**" auf **Exportieren**. Speichern Sie die generierte Metadatenfile, und klicken Sie dann auf **Fertig**.

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=14.36.147.1, 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. Wählen Sie unter ISE **Administration > Identity Management > External Identity Sources > SAML Id Providers > PingFederate** aus.

10. Klicken Sie auf **Identity Provider Config > Browse (Identitätsanbieter-Konfiguration)**, und fahren Sie fort, um die aus dem PingFederate-Metadatenexportvorgang gespeicherten Metadaten zu importieren.

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. Wählen Sie **Gruppen** Registerkarte, unter **Gruppenmitgliedschaft Attribut** add **memberOf** und klicken Sie dann auf **Hinzufügen**

Fügen Sie unter **Name in Assertion** den Distinguished Name hinzu, den die **IdP** zurückgeben muss, wenn das **memberOf**-Attribut aus der LADP-Authentifizierung abgerufen wird. In diesem Fall ist die konfigurierte Gruppe mit der Sponsorgruppe von TOR verknüpft, und die DN für diese Gruppe lautet wie folgt:

SAML Identity Provider

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

Groups

Group Membership Attribute ⓘ

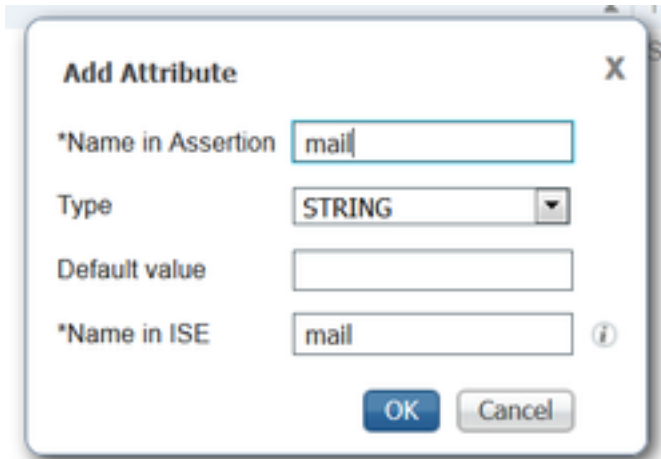
<input type="checkbox"/> Name in Assertion	<input type="button" value="▲"/> Name in ISE
<input checked="" type="checkbox"/> CN=TOR,DC=[redacted],DC=net	TOR

Nachdem Sie die DN- und "Name in ISE"-Beschreibung hinzugefügt haben, klicken Sie auf **OK**.

12. Wählen Sie die Registerkarte **Attribute**, und klicken Sie auf **Hinzufügen**.

Fügen Sie in diesem Schritt das Attribut "mail" hinzu, das in dem von der IdP übergebenen SAML-

Token enthalten ist und das auf der LDAP-Abfrage von Ping basiert und das E-Mail-Attribut für dieses Objekt enthalten muss.



Hinweis: Mit den Schritten 11 und 12 wird sichergestellt, dass die ISE über die IdP-Anmeldeaktion die Attribute "AD object Email" und "MemberOf" empfängt.

Überprüfung

1. Starten Sie das Gastportal über die Portal Test-URL, oder folgen Sie dem CWA-Fluss. Der Benutzer hat die Möglichkeit, Gastanmeldeinformationen einzugeben, ein eigenes Konto zu erstellen und sich bei einem Mitarbeiter anzumelden.

Sign On

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

Username:

Password:

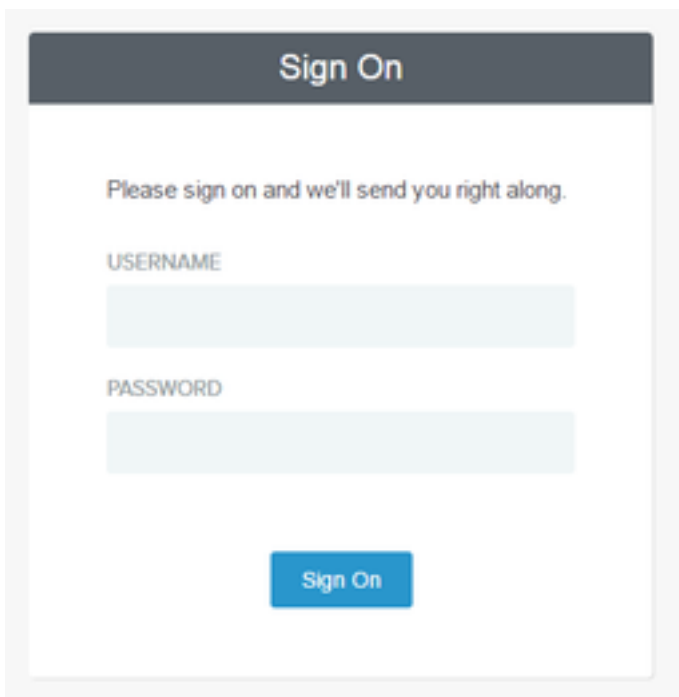
Sign On

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

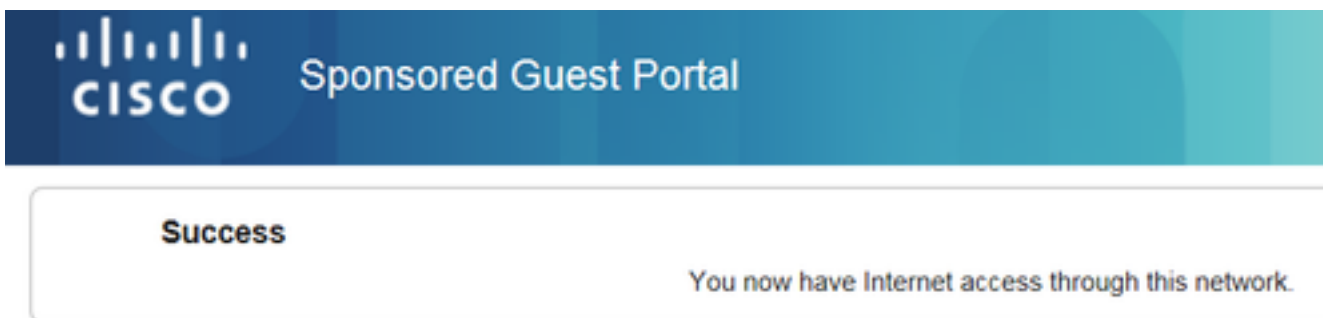
You can also login with



2. Klicken Sie auf **Mitarbeiteranmeldung**. Da es keine aktiven Sitzungen gibt, wird der Benutzer zum IdP-Anmeldeportal umgeleitet.

A screenshot of a web form titled "Sign On". The form has a dark header with the text "Sign On". Below the header, there is a message: "Please sign on and we'll send you right along." The form contains two input fields: "USERNAME" and "PASSWORD", both with light blue borders. Below the input fields is a blue button with the text "Sign On".

3. Geben Sie die AD-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
4. Der IDp-Anmeldebildschirm leitet den Benutzer auf die Erfolgsseite des Gastportals um.



5. Zu diesem Zeitpunkt wird der Benutzer jedes Mal, wenn er zum Gastportal zurückkehrt und "Employee Login" (Mitarbeiteranmeldung) wählt, im Netzwerk zugelassen, solange die Sitzung im IdP noch aktiv ist.

Fehlerbehebung

Jedes SAML-Authentifizierungsproblem wird unter ise-psc.log protokolliert. Es gibt eine dedizierte Komponente (SAML) unter **Administration > Logging > Debug log Configuration > Select the node in question > Set SAML component to debug level**.

Sie können über die CLI auf ISE zugreifen und den Befehl **show logging application ise-psc.log tail** eingeben und die SAML-Ereignisse überwachen. Sie können auch ise-psc.log für weitere Analysen unter **Operationen > Fehlerbehebung > Protokolle herunterladen > ISE-Knoten auswählen > Registerkarte Debug Logs herunterladen > auf ise-psc.log klicken**, um die Protokolle herunterzuladen.

```
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

```

Zugehörige Informationen

- [Zentrale Web-Authentifizierung am Konfigurationsbeispiel des Cisco WLC und der ISE.](#)
- [Konfigurationsbeispiel für die zentrale Webauthentifizierung mit einem Switch und einer Identity Services Engine.](#)
- [Versionshinweise für Cisco Identity Services Engine, Version 2.1](#)
- [Administratorleitfaden für die Cisco Identity Services Engine, Version 2.1](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.