PingFederate SAML SSO での ISE 2.1 ゲスト ポータルを設定する

内容

概要

このドキュメントでは、ゲストポータルのSecurity Assertion Markup Language(SAML)用にCisco Identity Services Engine(ISE)バージョン2.1シングルサインオン(SSO)機能を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine ゲスト サービス
- SAML SSO に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine バージョン 2.1
- SAML ID プロバイダー（IdP）として使用する Ping Identity の PingFederate 8.1.3.0 サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

フローの概要

SAML は、セキュリティ ドメイン間で認証および認可データを交換するための XML ベースの標準です。

SAML仕様では、プリンシパル（ゲストユーザ）、アイデンティティプロバイダー[IdP]（IPing Federateサーバ）、およびサービスプロバイダー[SP](ISE)の3つのロールが定義されています。

一般的な SAML SSO フローでは、SP が ID アサーションを要求して、IdP から取得します。ISE は、この結果に基づいてポリシー判断を実行できます。これは、ISE が使用できる設定可能な属性（つまり、AD オブジェクトに関連付けられたグループおよび電子メール アドレス）を IdP が含むことができるためです。

この使用例の予想されるフロー

1. ワイヤレス LAN コントローラ（WLC）またはアクセス スイッチが一般的な中央 Web 認証（CWA）フロー用に設定されます。

   ヒント:CWAフローの設定例については、記事の下部にある「関連情報」セクションを参照してください。

2.クライアントが接続し、セッションがISEに対して認証されます。ネットワーク アクセス デバイス（NAD）が、ISE によって返されたリダイレクト属性値ペア（url-redirect-acl および url-redirect）を適用します。

3.クライアントがブラウザを開き、HTTPまたはHTTPSトラフィックを生成し、ISEのゲストポータルにリダイレクトされます。

4.ポータルにログインすると、クライアントは以前に割り当てられたゲストのクレデンシャル(**スポンサーが作成**)を入力して新しいゲストアカウントをセルフプロビジョニングするか、ADクレデンシャルを使用してログイン(**従業員ログイン**)し、SAMLを介してシングルサインオン機能を提供できます。

5.ユーザが[Employee Login]オプションを選択すると（この例ではCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのCisco Unified Communications ManagerのUnified Communications Manager ManagerのEditionを使用）、ISEはこのクライアントののIdIdIdPPをををにします。アクティブ セッションがなければ、IdP はユーザ ログインを適用します。この時点で、ユーザは、AD クレデンシャルを IdP ポータルに直接入力することを求められます。

6. IdPはLDAPを介してユーザを認証し、設定可能な時間だけ有効な新しいアサーションを作成します。

   注：デフォルトでは、Ping Federateは**セッションタイムアウト**を60分（初期認証後60分でISEからのSSOログイン要求がない場合は、セッションが削除されます）、および**セッショ**

ン最大タイムアウトを480分（IdPがこのユーザに対してISEから一定のSSOログイン要求を受信した場合でも、セッションは8時間で期限切れになります）適用します。

アサーション セッションがアクティブであり続けている限り、従業員は、ゲスト ポータルの使用時に SSO を利用できます。セッションがタイムアウトになると、新しいユーザ認証が IdP によって実施されます。

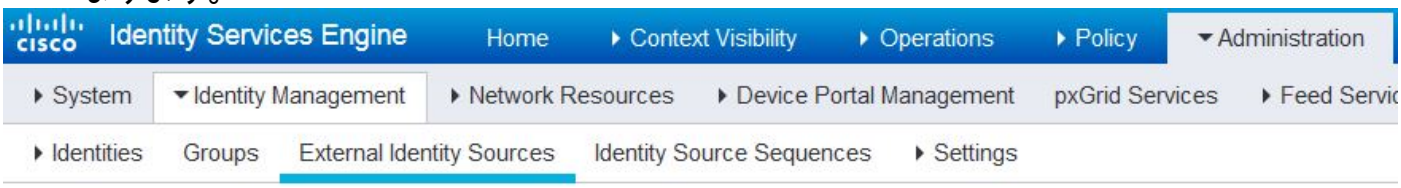
設定

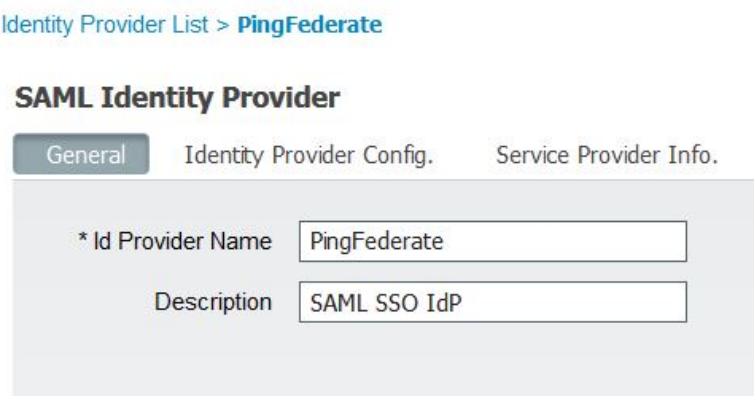
ここでは、ISE と PingFederate を統合するための設定手順と、ゲスト ポータルのブラウザ SSO を有効にする方法について説明します。

> **注**：ゲストユーザの認証時にはさまざまなオプションと可能性がありますが、このドキュメントでは、すべての組み合わせについて説明しているわけではありません。しかし、この使用例には、使用例を修正して目的の設定を正確に指定する方法について理解するのに必要な情報が含まれています。

ステップ 1：外部SAML IDプロバイダーを使用するためのISEの準備

1. Cisco ISEで、[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers] の順に選択します。
2. [Add] をクリックします。
3. [Genaral] **タブで、ID プロバイダー名**を入力します。[Save] をクリックします。 このセクションの残りの設定は、後の手順で IdP からインポートする必要があるメタデータによって異なります。





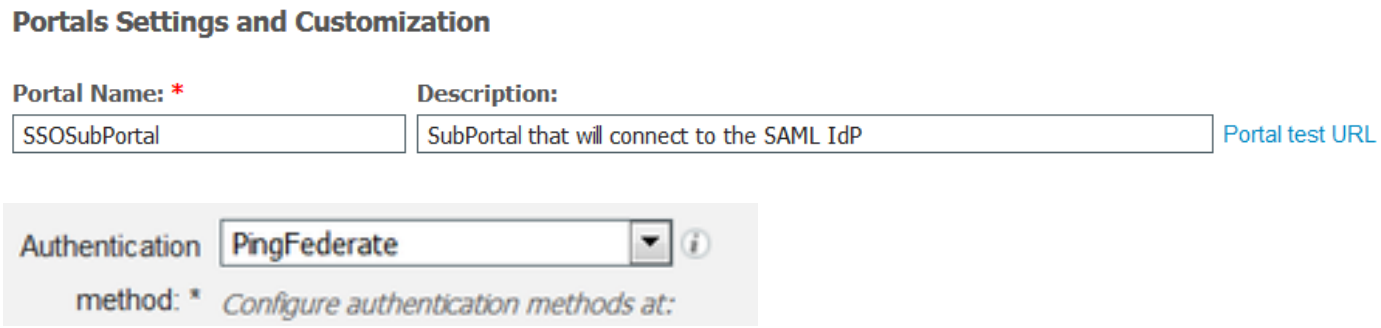
ステップ 2：外部アイデンティティプロバイダーを使用するためのゲストポータルの設定

1. [Work Centers] > [Guest Access] > [Configure] > [Guest Portals] **の順に選択します。**
2. 新しいポータルを作成し、[Self-Registered Guest Portal] を選択します。

注：これは、ユーザが体験するメインポータルではなく、セッションステータスを確認するためにIdPと対話するサブポータルです。このポータルは「SSOSubPortal」と呼ばれます。

3. [Portal Settings] を展開し、[Authentication Method] で[PingFederate] を選択します。

4. [Identity Source Sequence] から、以前に定義した外部SAML IdP(PingFederate)を選択します。



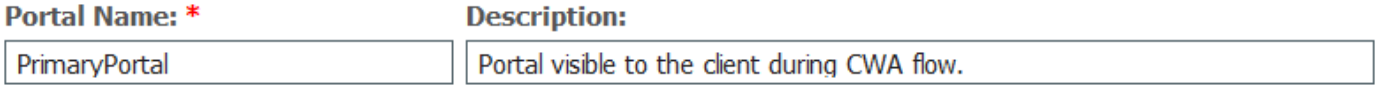
5. [Acceptable Use Policy(AUP)] セクションと[Post-Login Banner Page Settings] セクションを展開し、両方とも無効にします。

ポータル フローは次のとおりです。

6. [Save] をクリックして変更内容を保存します。

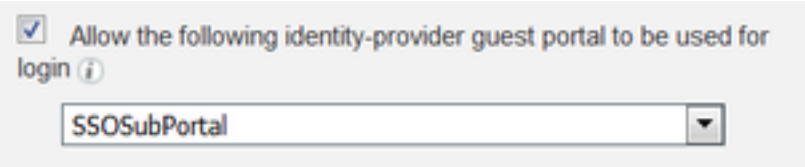
7. [Guest Portals]に戻り、[Self-Registered Guest Portal] オプションを使用して新しいポータルを作成します。

注：これはクライアントに表示されるプライマリポータルです。プライマリ ポータルは、SSOS サブポータルを ISE と IdP の間のインターフェイスとして使用します。 このポータルは「PrimaryPortal」と呼ばれます。



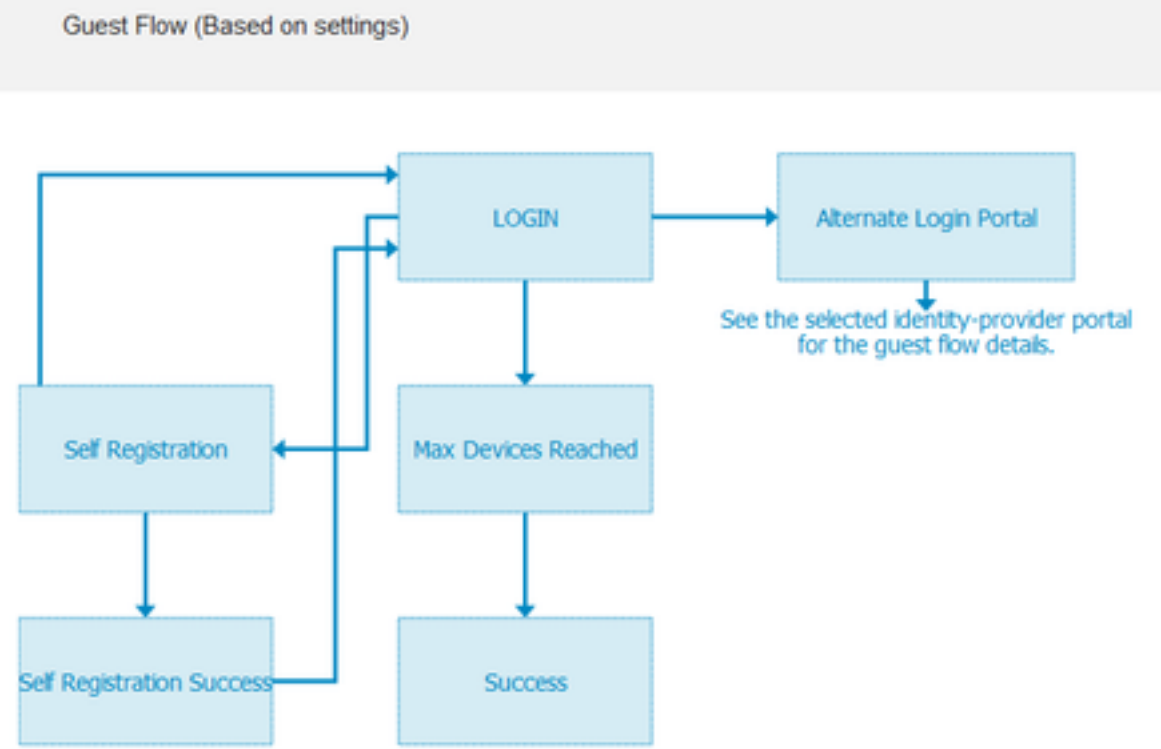
8. [Login Page Settings] を展開し、[Allow the following identity-provider guest portal to be used

for login] で以前に作成した**SSOSubPortal**を選択します。

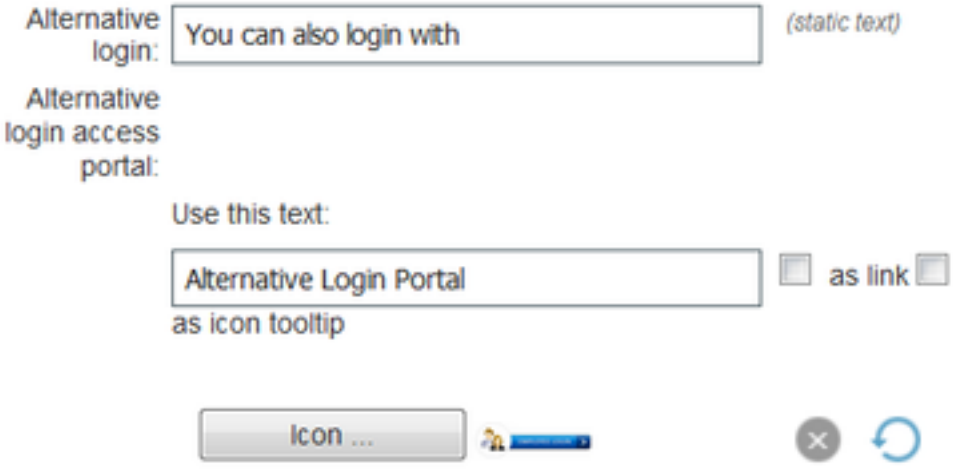


9. [Acceptable Use Policy] の[AUP]と[Post-login Banner Page Settings]を展開し、これらのチェックボックスをオフにします。

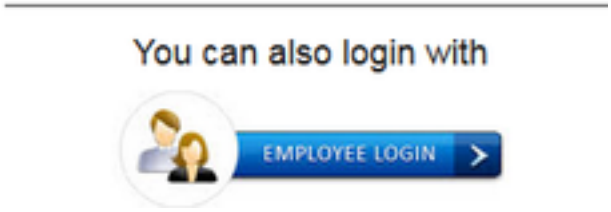
この時点で、ポータルフローは次のようになります。



10. [Portal Customization] > [Pages] > [Login] を選択します。**代替ログインオプション**（アイコン、テキストなど）をカスタマイズするオプションが必要になりました。

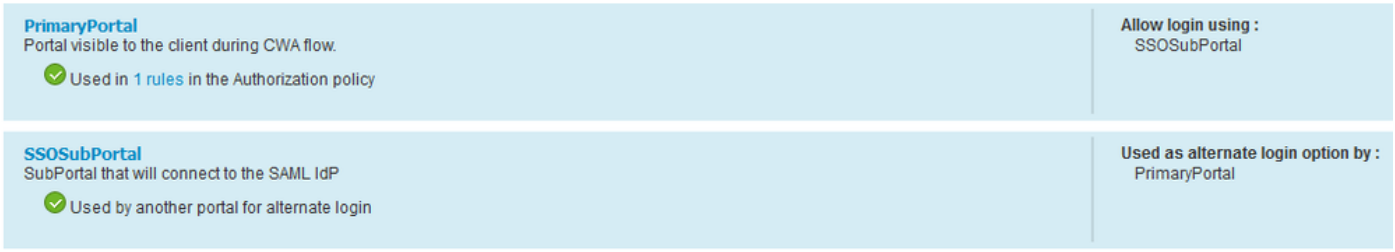


注：右側のポータルプレビューの下に、追加のログインオプションが表示されていることに注意してください。



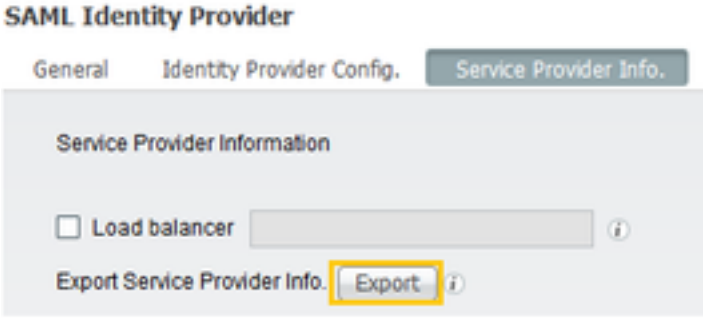
11. [Save] をクリックします。

以上で、両方のポータルがゲスト ポータル リストに表示されます。



ステップ 3：ISEゲストポータルのアイデンティティプロバイダーとして機能するようにPingFederateを設定する

1. ISE で、[Administration] > [Identity Management] > [External identity Sources] > [SAML Id Providers] > [PingFederate] の順に選択し、[Service Provider Info] をクリックします。
2. [Export Service Provider Info] **で、[Export] をクリックします。**



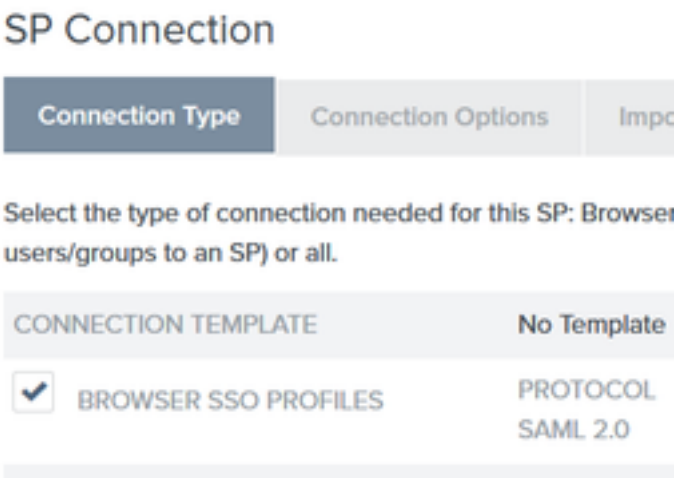
3. 生成されたzipファイルを保存して解凍します。そこに含まれている XML ファイルは、後の手順で、PingFederate でプロファイルを作成するために使用されます。

注：これ以降、このドキュメントではPingFederateの設定について説明します。この設定は、スポンサー ポータル、MyDevices、BYOD ポータルなどの複数のソリューションで同じです（これらのソリューションについては、このドキュメントでは説明していません）。

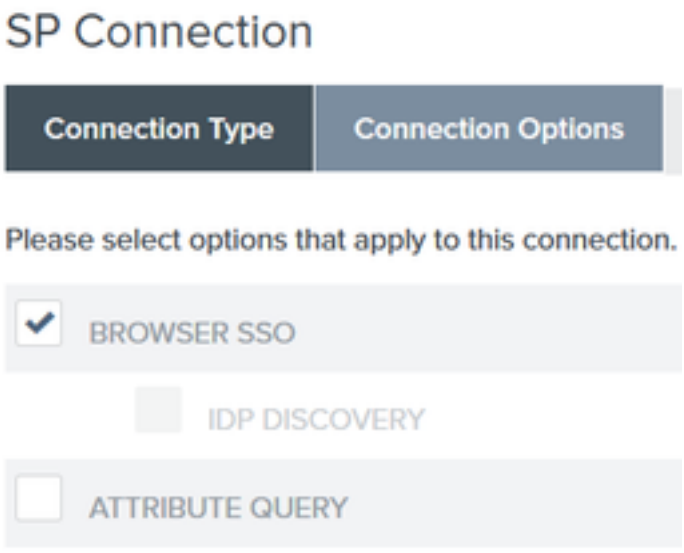
4. PingFederate管理ポータル(通常はhttps://ip:9999/pingfederate/app)を開きます。

5. [IdP Configuration] タブ> [SP Connections] セクションで、[Create New] を選択します。

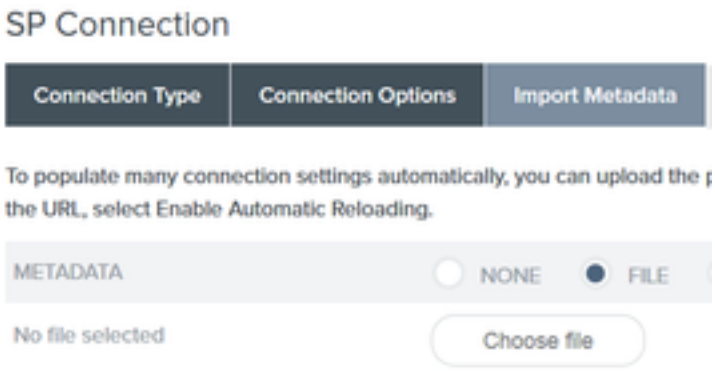
6. [Connection Type] で、[Next] をクリックします。



7. [Connection Options] で、[Next] をクリックします。

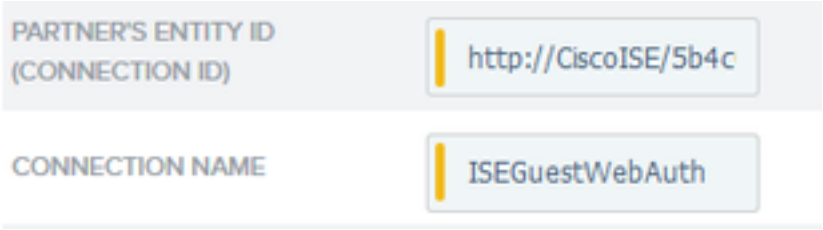


8. [Import Metadata] で、[File] オプションボタンをクリックし、[Choose file] をクリックして、以前にISEからエクスポートしたXMLファイルを選択します。

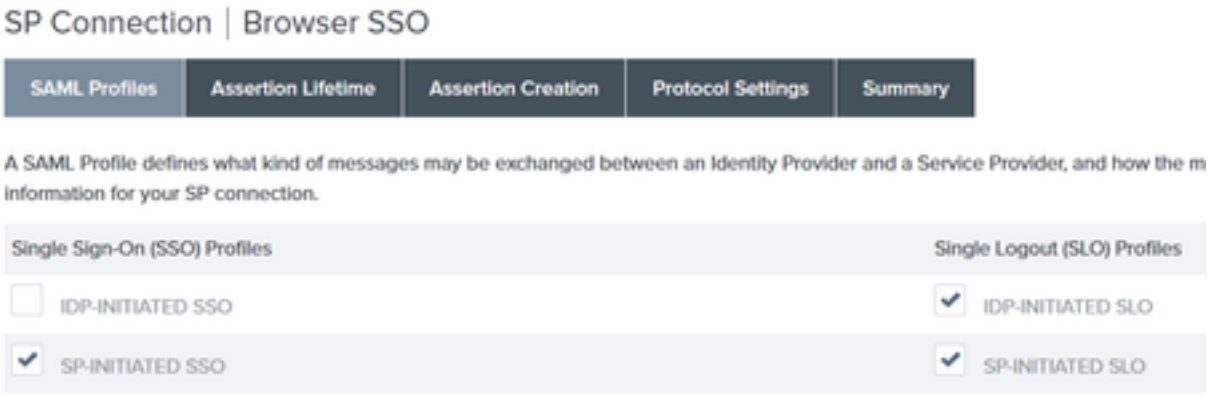


9. [Metadata Summary] で、[Next] をクリックします。

10. [General Info] ページで、[Connection Name] に名前（ISEGuestWebAuth など）を入力し、[Next] をクリックします。



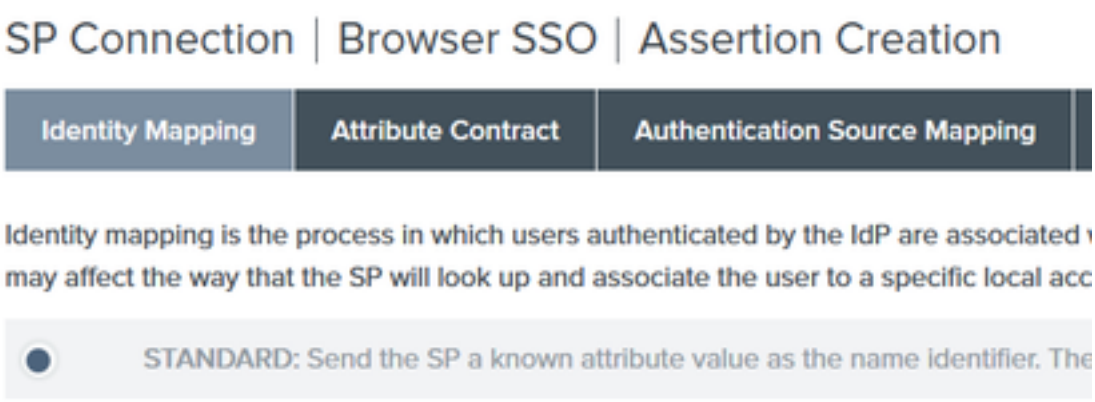
11. [Browser SSO] で[Configure Browser SSO] をクリックし、[SAML Profiles] でオプションを確認して[Next] をクリックします。



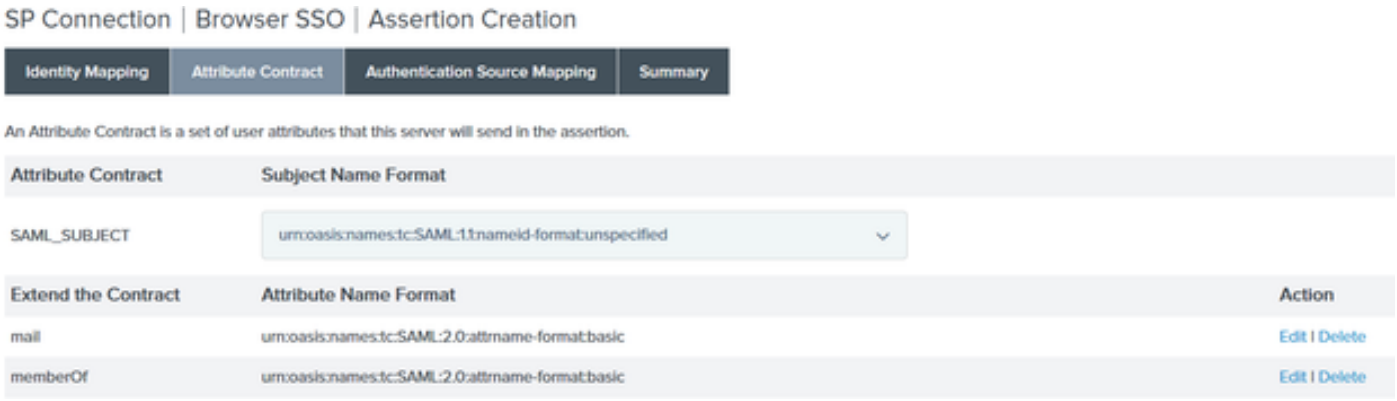
12. [Assertion lifetime] **で、[Next] をクリックします。**

13. [Assertion Creation] **で、[Configure Assertion Creation] をクリックします。**

14. [Identity Mapping] で、[Standard] **を選択し、[Next] をクリックします。**



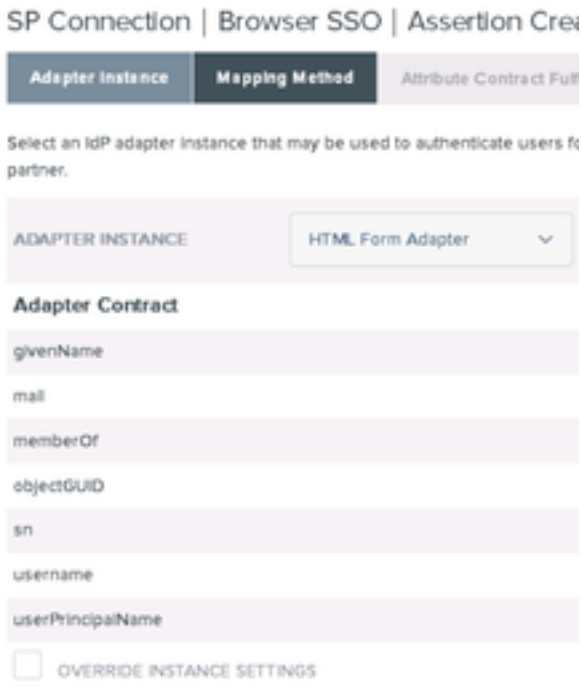
15. [Attribute Contract] > [Extend Contract] で、属性**mail**および**memberOf**を入力し、[add] をクリックします。[next] をクリックします。



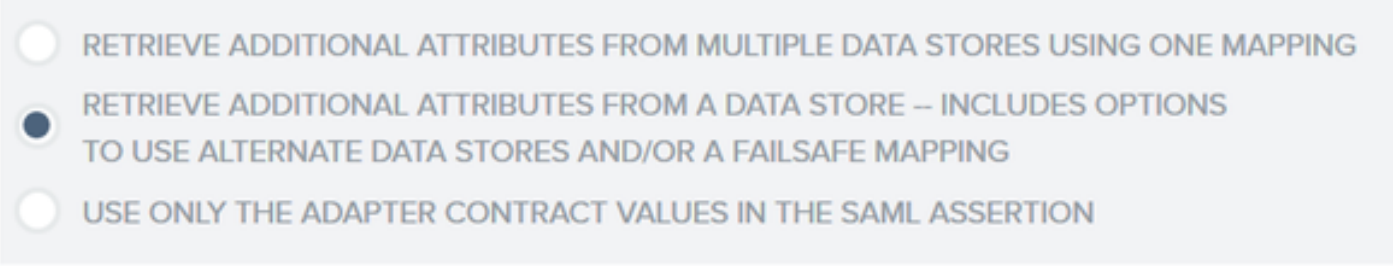
このオプションの設定により、ID プロバイダーは、Active Directory によって提供される **MemberOf 属性と Email 属性を ISE に渡すことができます。ISE は、後でポリシー判定時にこれを条件として使用できます。**

16. [Authentication Source Mapping] **で、[Map New Adapter Instance]** をクリックします。

17. [Adapter Instance] **で、[HTML Form Adapter]** を選択します。[Next] をクリックします。

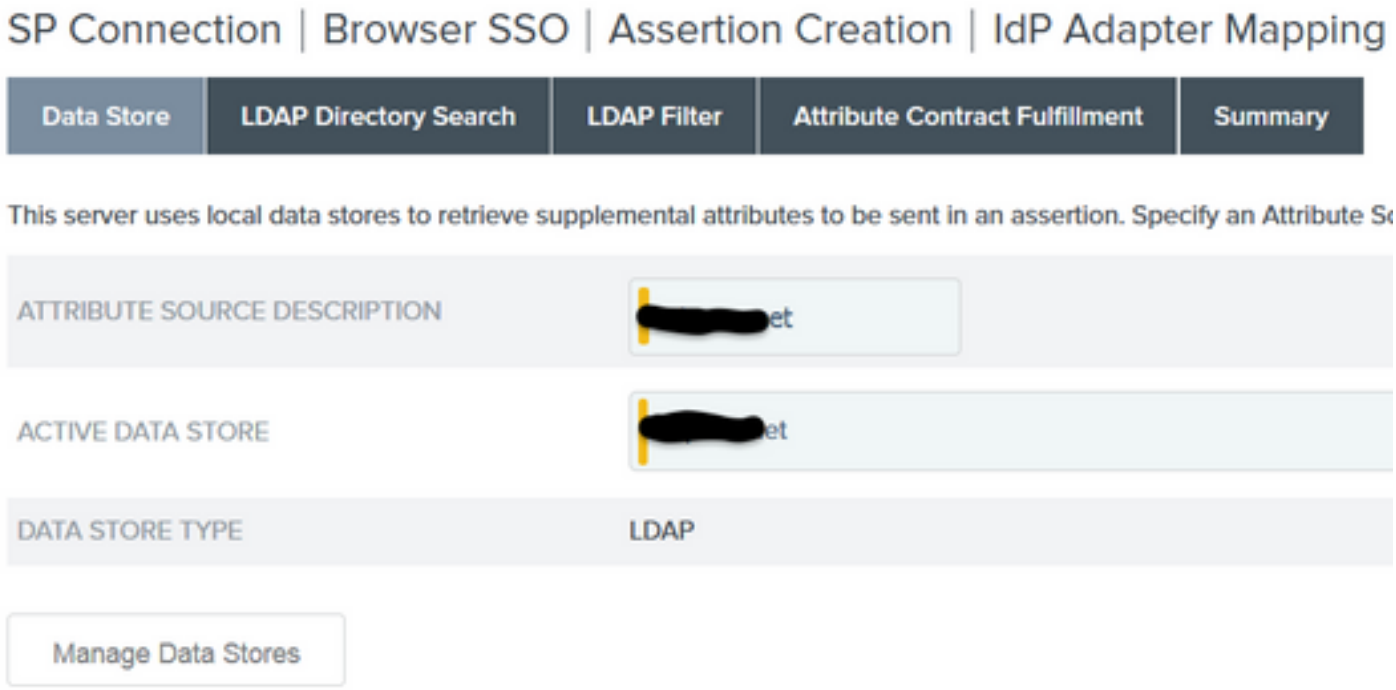


18. [Mapping methods] で2番目のオプションを選択し、[Next] をクリックします。

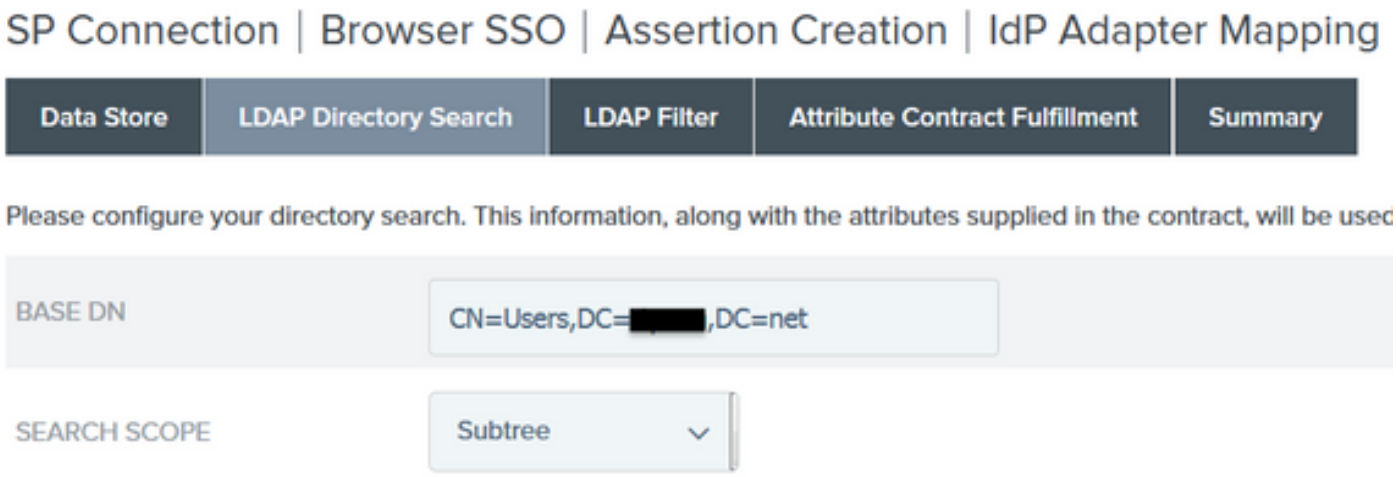


19. [Attribute Sources & User Lookup] で、[Add Attribute Source] ボックスをクリックします。

20. [Data Store] で説明を入力し、[Active Data Store] から[LDAP connection instance]を選択して、このディレクトリサービスのタイプを定義します。まだ**データ ストアを設定していない場合は、[Manage Data Stores] をクリックして新しいインスタンスを追加します。**

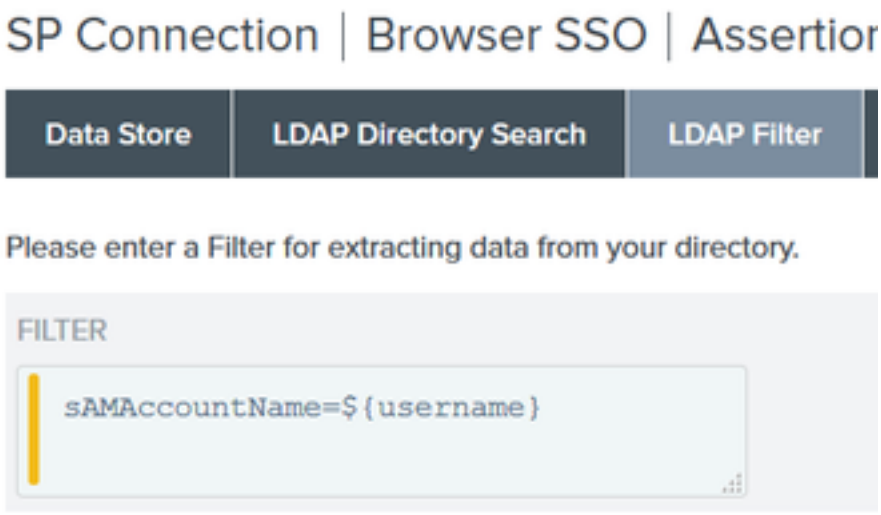


21. [LDAP Directory Search] で、ドメイン内のLDAPユーザルックアップの**ベースDN**を定義し、[Next] をクリックします。

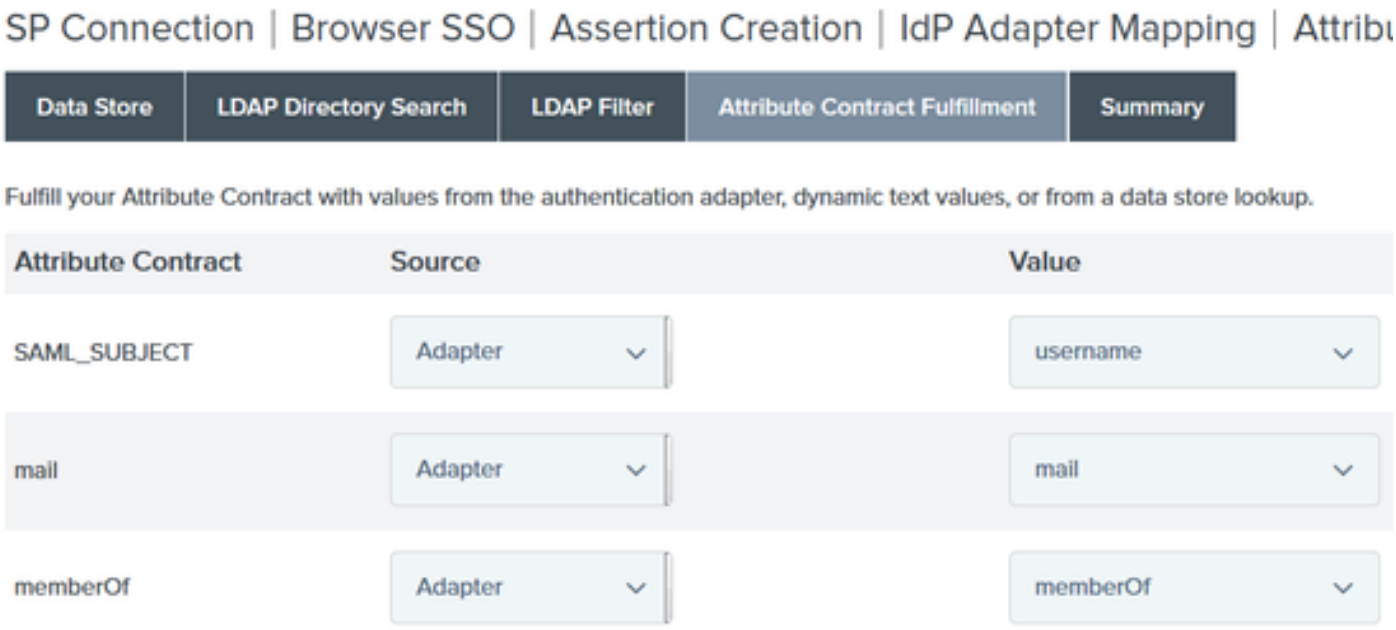


注：これは、LDAPユーザのルックアップ時にベースDNを定義するため、重要です。ベースDN が正しく定義されない場合、 LDAP スキーマでオブジェクトが検出されません。

22. [LDAP Filter] で、「sAMAccountName=${username}」という文字列を追加し、[Next] をクリックします。



23. [Attribute Contract Fulfillment] でオプションを選択し、[Next] をクリックします。

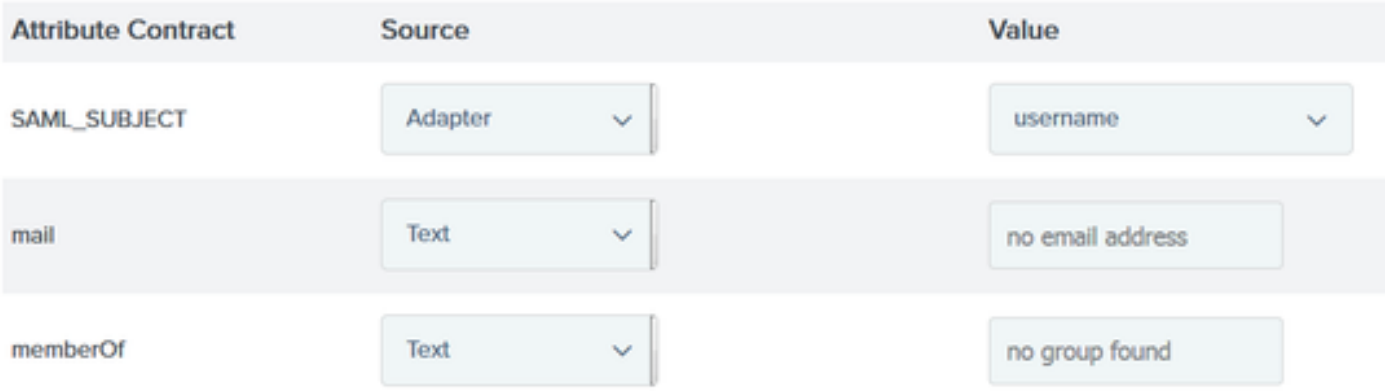


24.サマリーセクションで設定を確認し、Doneをクリックします。

25. [Attribute Sources & User lookup] に戻り、[Next] をクリックします。

26. [Failsafe Attribute Source] で、[Next] をクリックします。

27. [Attribute Contract Fulfillment] で、次のオプションを選択し、[Next] をクリックします。



28. [Summary]セクションの設定を確認し、[Done] をクリックします。

29. [Authentication Source Mapping] に戻り、[Next] をクリックします。

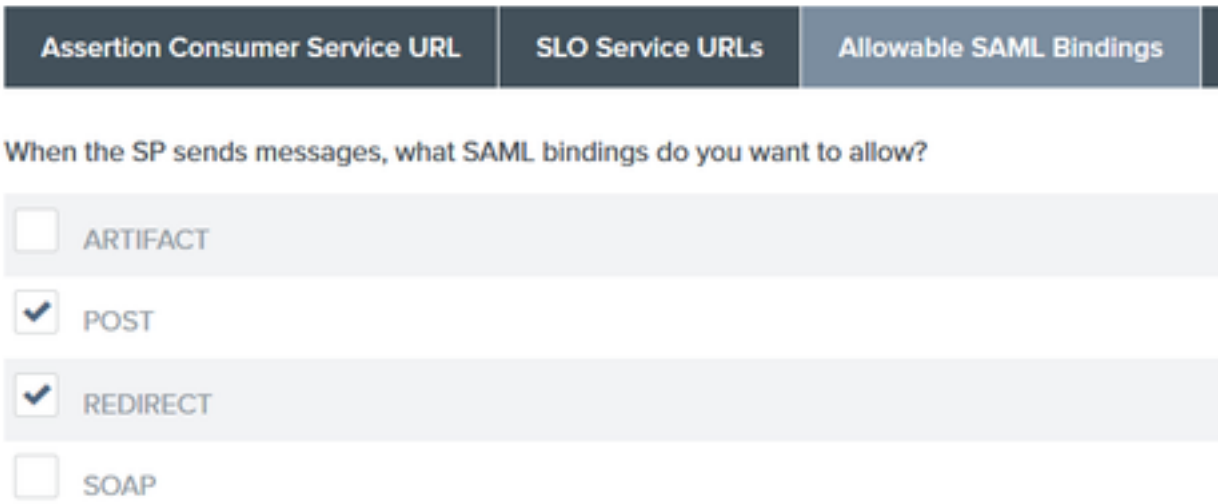
30. [Summary] ページで設定を確認したら、[Done] をクリックします。

31. [Assertion Creation] に戻り、[Next] をクリックします。

32. [Protocol Settings] で、[Configure Protocol Settings] をクリックします。この時点で、すでに2つのエントリが入力されている必要があります。[next] をクリックします。

33. [SLO Service URLs]で[**Next**]をクリックします。

34. [Allowable SAML Bindings]で、オプション[ARTIFACT]と[SOAP]のチェックマークを外し、[**Next**]をクリックします。



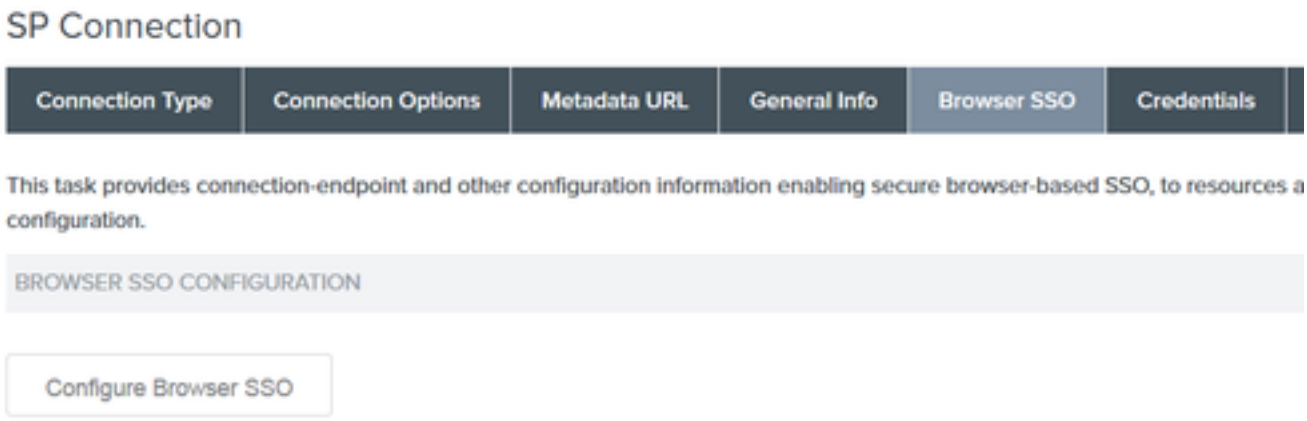
35. [Signature Policy]で[Next] をクリックします。

36. [Encryption Policy]で[Next] をクリックします。

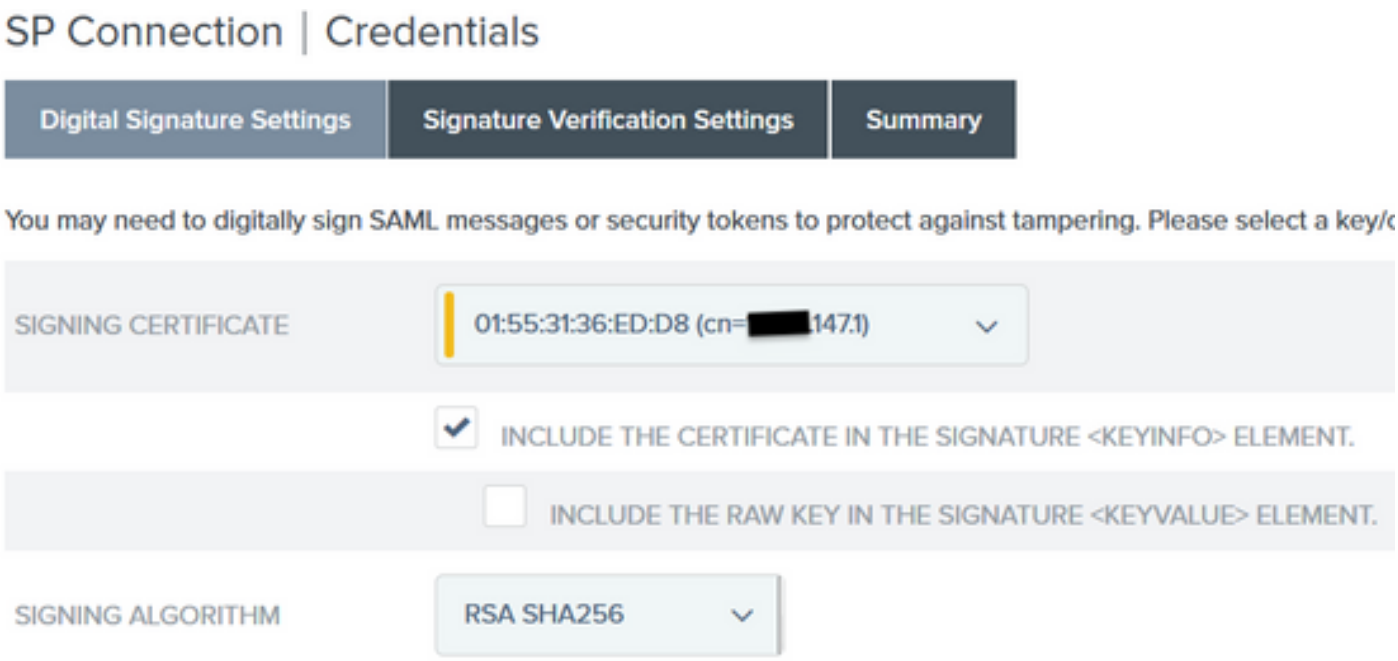
37. [Summary]ページで設定を確認し、[Done] をクリックします。

38. [Browser SSO] > [Protocol settings]に戻り、[Next] をクリックして設定を検証し、[Done] をクリックします。

39.ブラウザの[SSO]タブが表示されます。[next] をクリックします。



40. [Credentials] で[Configure Credentials] をクリックし、IdPからISEへの通信中に使用する署名証明書を選択して、[Include the certificate in the signature] オプションをオンにします。次に、[Next] をクリックします。



> **注**：設定されている証明書がない場合は、[Manage Certificates] をクリックし、プロンプトに従って、IdPからISEへの通信の署名に使用する**自己署名証明書**を生成します。

41.サマリーページで設定を検証し、[Done] をクリックします。

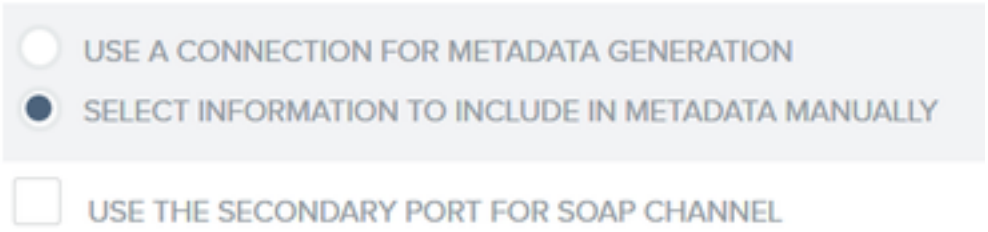
42. [Credentials] タブに戻り、[Next] をクリックします。

43. [Activation & Summary] の [Connection Status] で [ACTIVE] を選択し、残りの設定を確認し

て、[Done] をクリックします。

ステップ 4：ISE外部SAML IdPプロバイダープロファイルへのIdPメタデータのインポート

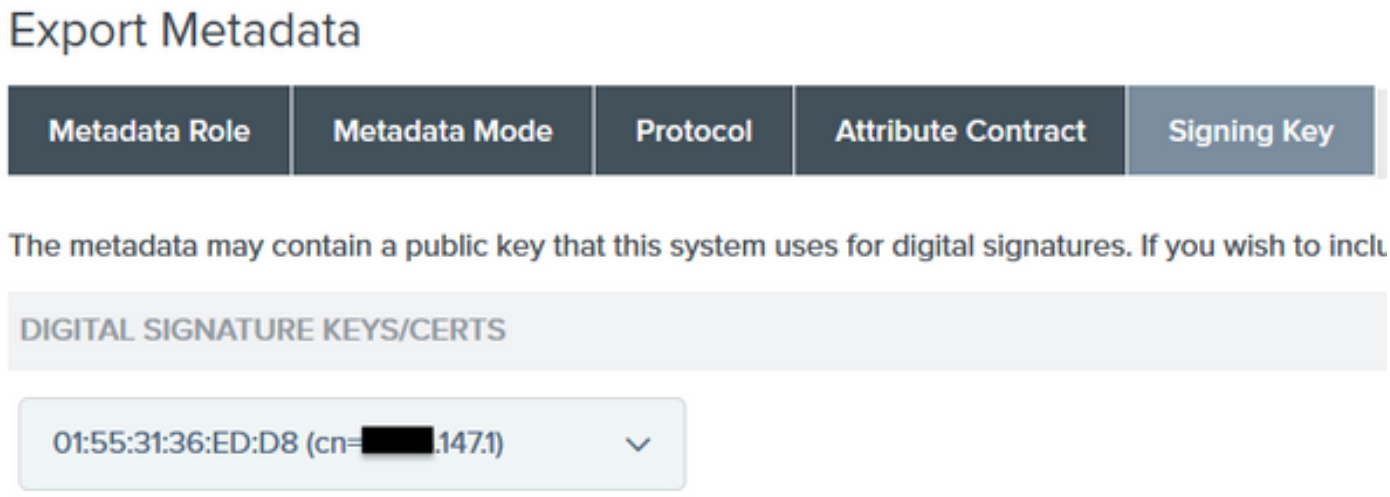
1. PingFederate 管理コンソールで、[Server Configuration] > [Administrative Functions] > [Metadata Export] の順に選択します。 サーバが複数の役割（IdP と SP）用に設定されている場合は、[I am the Identity Provider(IdP)] **オプションを選択します。**[next] をクリックします。
2. [Metadata] モードで [Select Information to Include In Metadata Manually] を選択します。[next] をクリックします。



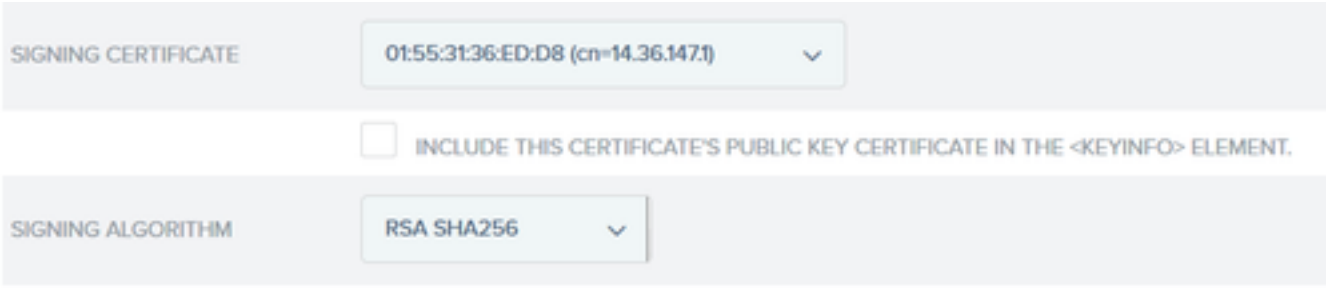
3. [Protocol] で[Next] をクリックします。

4. [Attribute Contract] で、[Next] をクリックします。

5. [Signing Key] で、以前に接続プロファイルで設定した証明書を選択します。[next] をクリックします。



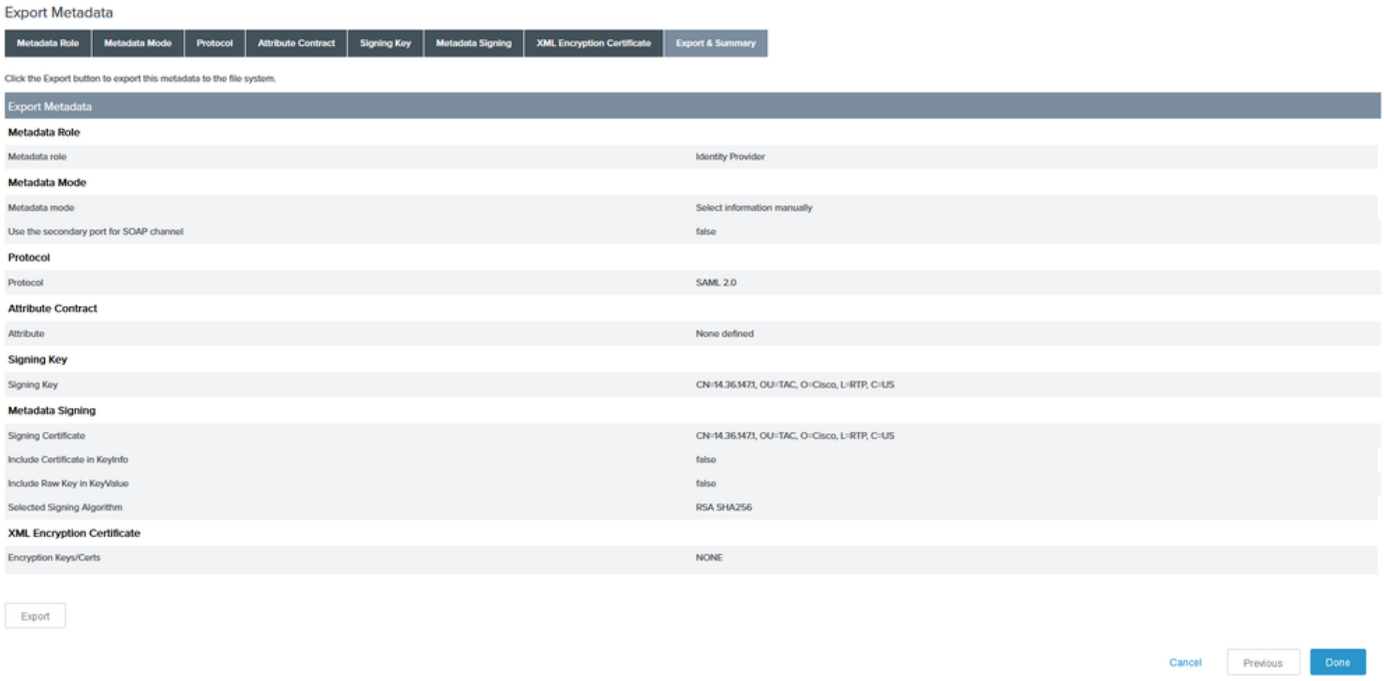
6. [Metadata Signing] で署名証明書を選択し、[Include this certificate's public key in the key info element] をオンにします。[next] をクリックします。



7. [XML encryption certificate] で [Next] をクリックします。

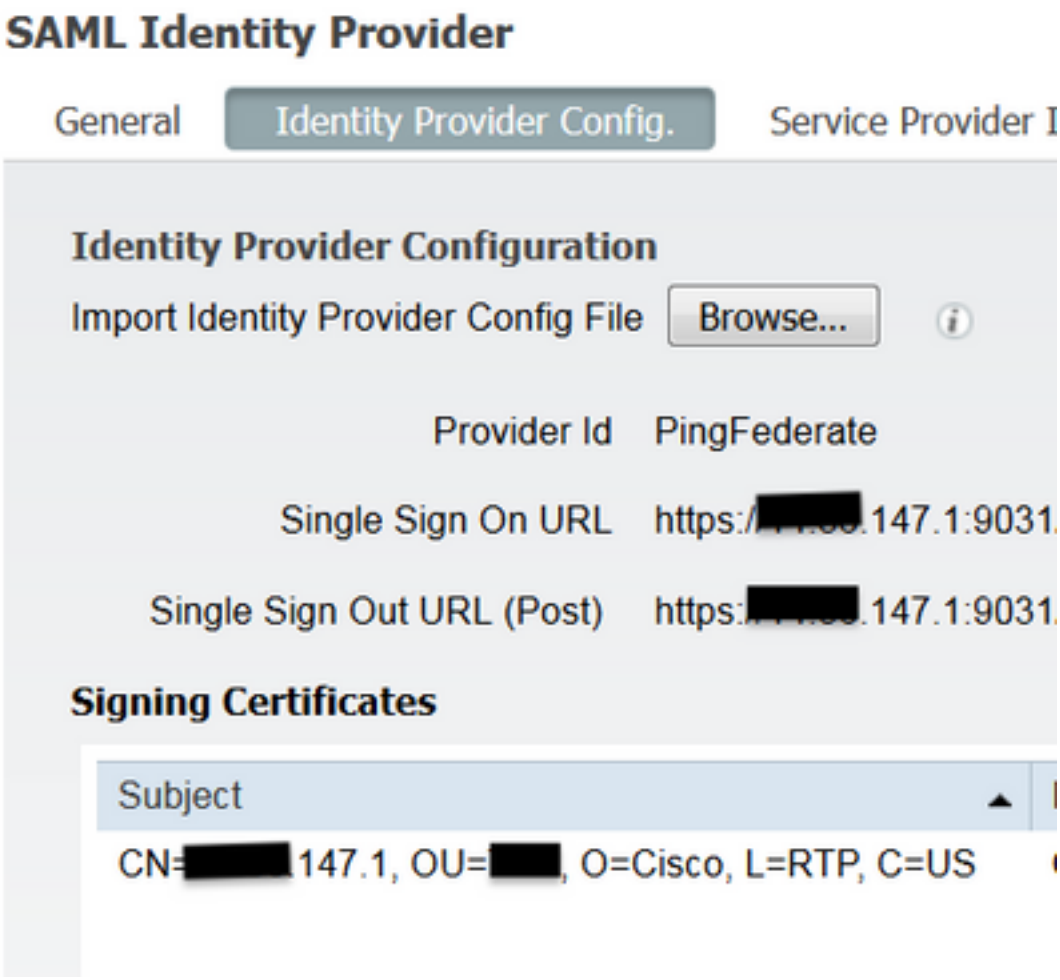
注：ここで暗号化を適用するオプションは、ネットワーク管理者が設定します。

8. [Summary] セクションで、[Export] をクリックします。生成されたメタデータ ファイルを保存し、[Done] をクリックします。



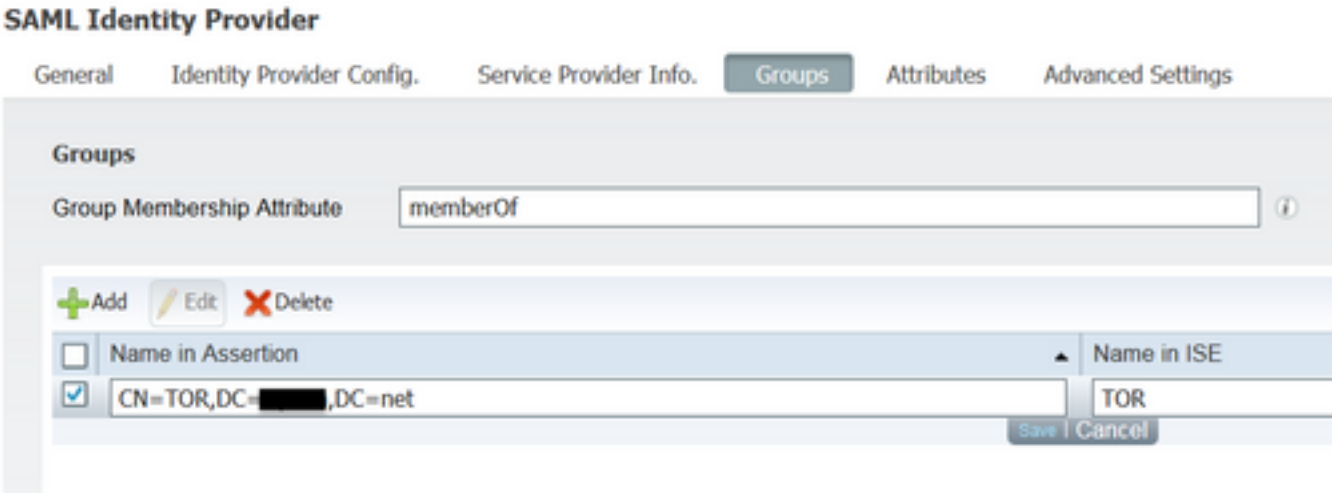
9. ISEで、[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers] > [PingFederate] を選択します。

10. [Identity Provider Config] > [Browse] をクリックし、PingFederateのメタデータエクスポート操作で保存されたメタデータのインポートに進みます。



11. [Groups] タブを選択し、[Group Membership Attribute] で[memberOf] を追加して、[Add] をクリックします

[Name in Assertion] で、LADP認証からmemberOf属性を取得するときにIdPが返す必要がある識別名を追加します。 今回の場合は、設定済みのグループが TOR のスポンサー グループにリンクされており、このグループの DN は次のとおりです。

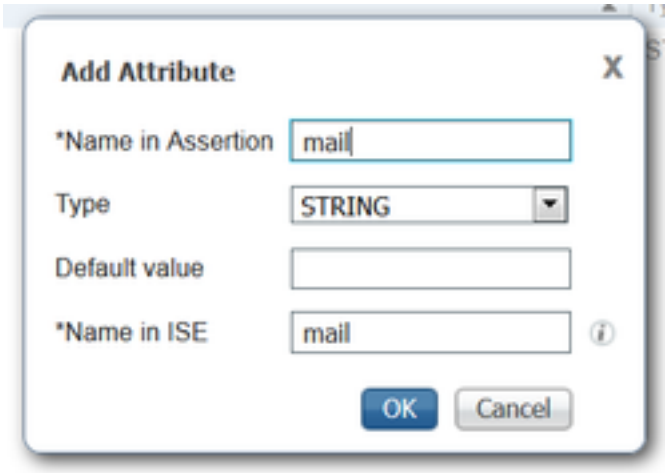


DN と [Name in ISE] を追加したら、[OK] をクリックします。

12. [Attributes] タブを選択し、[Add] をクリックします。

このステップでは、LDAPを介したPingのクエリーに基づいてIdPから渡されるSAMLトークンに含まれる属性「mail」を追加します。この属性には、そのオブジェクトの電子メール属性が含ま

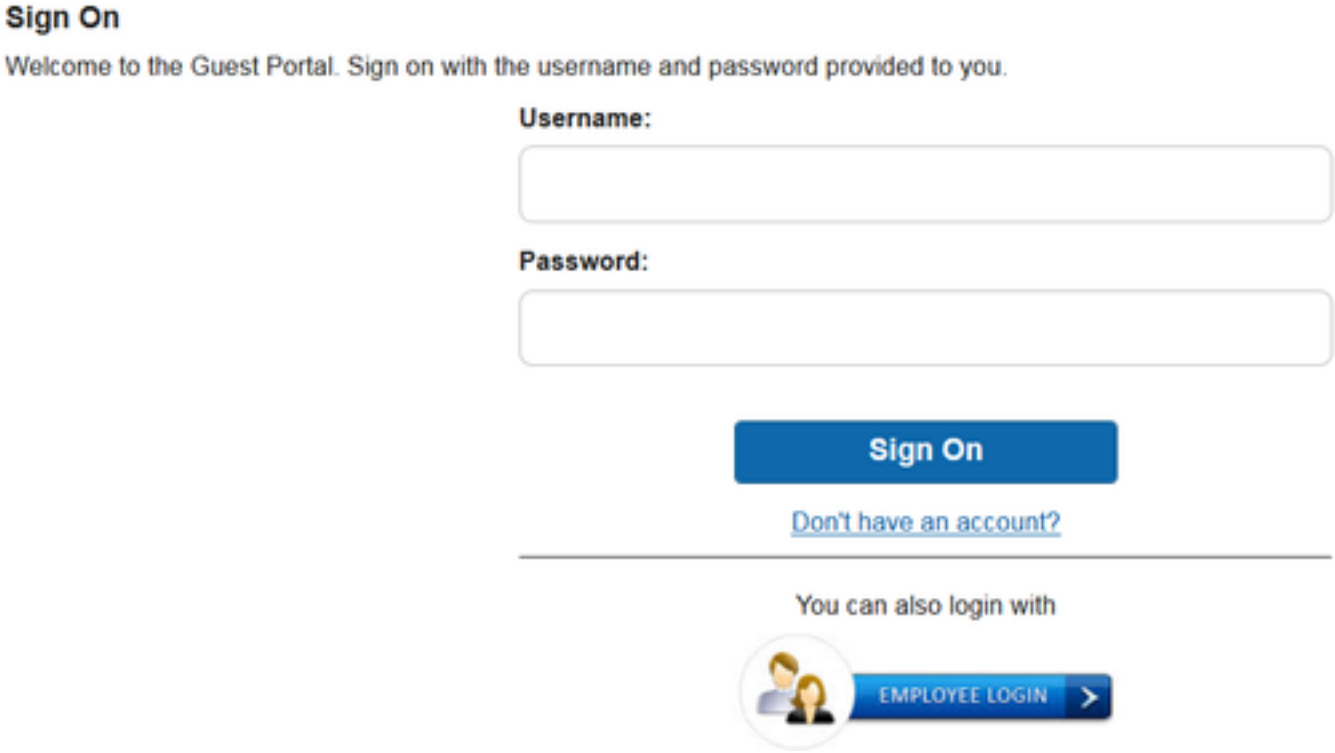
れている必要があります。



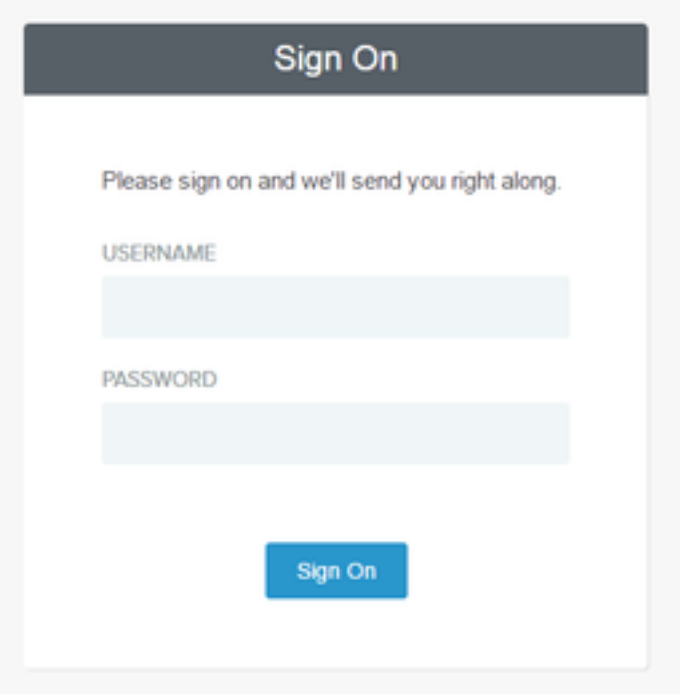
注：ステップ11と12では、ISEがIdPログインアクションを通じてADオブジェクトのEmail属性とMemberOf属性を受信することを確認します。

確認

1. ポータル テスト URL を使用するか、CWA フローに従って、ゲスト ポータルを起動します。ユーザは、ゲスト クレデンシャルを入力するか、独自のアカウントを作成するか、従業員ログインを実行することができます。

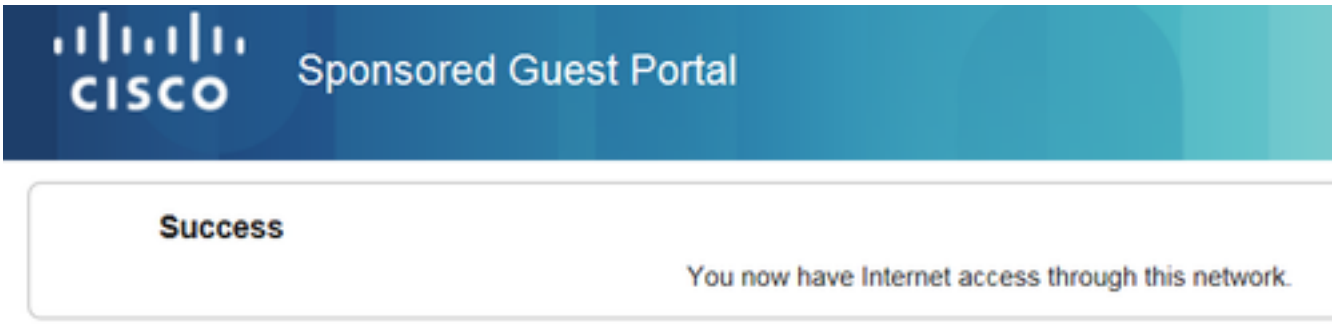


2. [Employee Login] をクリックします。アクティブなセッションがないため、ユーザは IdP ログイン ポータルにリダイレクトされます。



3. ADクレデンシャルを入力し、[Sign On] をクリックします。

4. IdPログオン画面は、ユーザーをゲストポータルの成功ページにリダイレクトします。



5.この時点で、ユーザがゲストポータルに戻って[Employee Login] を選択するたびに、IdPでセッションがアクティブである限り、ネットワークで許可されます。

トラブルシュート

SAML ise-psc.log SAML[Administration] > [Logging] > [Debug log Configuration] **SAML**

CLI ISE **show logging application ise-psc.log tail SAML [Operations] > [Troubleshoot] > [Download Logs] ISE [Debug Logs] ise-psc.log**

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

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

関連情報

- WLC と ISE での中央 Web 認証の設定例
- スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例
- Cisco Identity Services Engine, Release 2.1 のリリース ノート
- Cisco Identity Services Engine 管理者ガイド リリース 2.1

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。