

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

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[フロー概要](#)

[この使用例のための期待されたフロー](#)

[設定](#)

[ステップ 1. 外部 SAML 識別プロバイダを使用するために ISE を準備して下さい](#)

[ステップ 2. 外部識別プロバイダを使用するためにゲストポータルを設定して下さい](#)

[ステップ 3. ISE ゲストポータルのための識別プロバイダとして機能するために PingFederate を設定して下さい](#)

[ステップ 4. ISE 外部 SAML IdP プロバイダ プロファイルに IdP メタデータをインポートして下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この文書にセキュリティ表明マークアップ言語 (SAML) によってゲスト門脈ユーザ向けにサイン On (SSO) 単一機能を提供するために Cisco Identity Services Engine (ISE) バージョン 2.1 を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Identity Services Engine ゲスト サービス。
- SAML SSO についての基本的な知識。

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くものです。

- Cisco Identity Services Engine バージョン 2.1
- SAML 識別 Provider (IdP) として Ping 識別からの PingFederate 8.1.3.0 サーバ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。ネットワークがライブである場合、適用されるあらゆる設定の潜在的影響を理解することをお勧めします。

フロー概要

SAML はセキュリティドメイン間の認証 および 権限データを交換するための XML ベース規格です。

SAML 仕様は 3 つのロールを定義します: プリンシパル (ゲストユーザ)、識別プロバイダ [IdP] (IPing 連合したサーバ)、およびサービスプロバイダ [SP] (ISE)。

典型的な SAML SSO フローでは、SP は IdP からの識別アサーションを要求し、得ます。この結果に基づいて、ISE は IdP が ISE は使用できるという設定可能な属性を含むことができると同時に政策決定を行うことができます (AD オブジェクトに関連付けられるすなわちグループおよび e メールアドレス)。

この使用例のための期待されたフロー

1. ワイヤレス LAN コントローラ (WLC) またはアクセス スイッチは典型的な中央 Web 認証 (CWA) フローのために設定されます。

ヒント: 技術情報の下部の関連情報セクションの CWA フローのための設定例を見つけ下さい。

2. クライアントは接続し、セッションは ISE に対して認証されます。ネットワーク アクセス Device (NAD) は ISE によって戻るリダイレクト Attributes 値ペア (AVP) を適用します (URL リダイレクト ACL および URL リダイレクト)。

3. クライアントはブラウザを開いたり、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. ポータルでクライアントが事前に割り当てられたゲスト信任状ログイン (従業員ログオン) 単一への AD 信任状に提供する SAML によって機能で署名して下さい (作成されるスポンサー) および自己プロビジョニングするを新しいゲスト アカウント入力してまたは使用できれば。

5. ユーザが「従業員ログオン」のオプションを選択すれば、ISE は IdP に対してこのクライアントのブラウザー セッションに関連付けられるアクティブなアサーションがあるかどうか確認します。アクティブセッションがない場合、IdP はユーザ ログインを実施します。このステップでユーザは IdP ポータルで AD 信任状を直接入力するためにプロンプト表示されます。

6. IdP は LDAP によってユーザを認証し、設定可能な時間の間稼働しているとどまる新しいアサーションを作成します。

注: 連合した Ping はデフォルトで (IdP がセッションが 8 時間以内に切らす) このユーザ向けの ISE から一定した SSO Login 要求を受け取っても 60 分の ISE から SSO Login 要求が最初の認証の後になければセッションは削除されることを 60 分 (これは意味しますことを) のセッション タイムアウトおよび 480 分のセッション最大タイムアウトを適用します。

アサーション セッションがそれでもアクティブである限り、従業員は彼がゲスト ポータルを使用

する場合 SSO を経験します。セッションタイム、新規 ユーザ 認証が IdP によって実施されれば。

設定

このセクションは連合した Ping と ISE を統合ためにコンフィギュレーションのステップをゲストポータルのためのブラウザ SSO を有効にする方法を論議し。

注: ゲストユーザを認証するとさまざまなオプションおよび可能性があるが、この資料にすべての組み合わせが説明がありません。ただし実現させたいと思う精密な設定に例を修正する方法を、この例は理解するのに必要な情報を与えたものです。

ステップ 1.外部 SAML 識別プロバイダを使用するために ISE を準備して下さい

1. Cisco ISE で、> **アイデンティティ管理** > **外部識別ソースをたどります** > **SAML ID プロバイダ** 『管理』 を選択して下さい。
2. [Add] をクリックします。
3. **General** タブの下で、**ID プロバイダ名**を入力して下さい。 [Save] をクリックします。 後の手順の IdP からインポートされる必要があるこのセクションの設定の他はメタデータによって決まります。

ステップ 2.外部識別プロバイダを使用するためにゲストポータルを設定して下さい

1. **作業センター** > **ゲストアクセスを** > **設定します** > **ゲストポータル**選択して下さい。
2. 新しい門脈を作成し、自己登録された**ゲストポータル**を選択して下さい。

注: これはその主要なポータル ユーザ エクスペリエンス セッションステータスを確認するために IdP と相互に作用している subportal ではないですが。 このポータルは SSOSubPortal と呼ばれます。

3. **門脈設定を**拡張し、**認証方式のための PingFederate** を選択して下さい。
4. **識別ソース シーケンス**から、**外部 SAML IdP defined (PingFederate)** を以前に選択して下さい。
5. **Acceptable Use Policy (AUP)** および**後ログオン バナーページ設定**セクションを拡張し、両方を**ディセーブル**にして下さい。

門脈フローは次のとおりです:

6. 変更を保存します。
7. **ゲストポータル**に戻り、自己登録された**ゲストポータル オプション**を使用して新しいものを作成して下さい。

注: これはクライアントへプライマリ門脈目に見えます。プライマリ ポータルは ISE と IdP 間のインターフェイスとして SSOSubportal を使用します。このポータルは PrimaryPortal と呼ばれます。

8. Login ページ設定を拡張し、以前にの下で「作成される SSOSubPortal をログインに」使用するようになります。次の識別プロバイダ ゲスト ポータルが選択して下さい。

9. インターネット接続規定 AUP および後ログオン バナーページ設定を拡張し、チェックを外して下さい。

この時点で門脈フローはこのようになる必要があります:

10. 門脈カスタマイゼーション > ページ > ログオンを選択して下さい。等) を今代替ログオン オプション (アイコン、テキスト カスタマイズするオプションがあるはず) です。

注: 、門脈プレビューの下で、右側でそれに追加 Login オプション目に見えます注意して下さい。

11. [Save] をクリックします。

この場合ポータルは両方ともゲスト ポータル リストの下で現われます。

ステップ 3. ISE ゲスト ポータルのための識別プロバイダとして機能するために PingFederate を設定して下さい

1. ISE で、> アイデンティティ管理 > 外部識別ソースをたどり、> SAML ID プロバイダ > PingFederate をクリックします。サービスプロバイダー ヒントを『管理』を選択して下さい。
2. エクスポート サービスプロバイダー ヒントの下で、『Export』 をクリックして下さい。
3. 生成される ZIP ファイルを保存し、抽出して下さい。ここに含まれている XML ファイルが後の手順の PingFederate のプロファイルを作成するのに使用されています。

注: ここから先は、この資料は PingFederate 設定を取り扱っています。この設定はスポンサー ポータル、MyDevices および BYOD ポータルのような多様なソリューションのため同じです。(それらのソリューションはこの技術情報でカバーされません)。

4. PingFederate admin ポータル (一般的に <https://ip:9999/pingfederate/app>) を開いて下さい。
5. IdP Configuration タブ > SP Connections セクションの下で新しい『Create』を選択して下さい。
6. 接続タイプの下で、『Next』 をクリックして下さい。
7. 接続オプションの下で、『Next』 をクリックして下さい。
8. インポート メタデータの下で、File オプション・ ボタンをクリックして下さい、『File』を選択し、選択します以前に ISE からエクスポートされる XML ファイルをクリックして下さい。
9. Under メタデータ要約は、『Next』 をクリックします。

10. On は一般的な情報ページ、接続名の下で、名前を (ISEGuestWebAuth のような) 入力し、『Next』 をクリックします。
11. ブラウザ SSO の下で、**ブラウザ SSO を SAML プロファイル チェック**の下でオプション『Configure』 をクリックし、『Next』 をクリックして下さい。
12. On **アサーション ライフタイム**は『Next』 をクリックします。
13. On **アサーション作成**は**アサーション作成**を『Configure』 をクリックします。
14. Under **識別マッピング**は**規格**を選択し、『Next』 をクリックします。
15. **属性契約**で > **契約**を入力し、属性メールおよび memberOf を『Add』 をクリック します**拡張**して下さい。 [Next] をクリックします。

このオプションの設定は識別プロバイダが提供される MemberOf を渡し、アクティブ ディレクトリによって属性を ISE が政策決定の間に条件として以降を使用できる ISE に **E-メールを送る**ことを可能にします。
16. Under **認証ソース マッピング**は**新しいアダプター インスタンス**を『Map』 をクリック します。
17. On **アダプター インスタンス**は **HTML 形式アダプタ**を選択します。『Next』 をクリック して下さい
18. **マッピング方式**の下で第 2 オプションを選択し、『Next』 をクリック して下さい。
19. **属性ソース及びユーザ ルックアップ**で**属性ソース ボックス**を『Add』 をクリック して下さい。
20. **データ ストア**の下で説明を入力し、**アクティブなデータ ストア**から LDAP conection 例を選択し、どのようなディレクトリ サービスこれがであるか定義して下さい。設定される**データ ストア**がけれども新しいインスタンスを追加するためになかったら**データ ストア**を『Manage』 をクリック して下さい。
21. **LDAP ディレクトリの検索**の下でドメインの LDAP ユーザ ルックアップのための**ベース DN**を定義し、『Next』 をクリック して下さい。

注: これは LDAP ユーザ ルックアップの間にベース DN を定義するので重要です。 不正確に定義されたベース DN は LDAP スキーマで見つけられなかったオブジェクトという結果に終わります。
22. Under **LDAP フィルタ**は**ストリング sAMAccountName=\${username}**を追加し、『Next』 をクリック します。
23. **属性契約達成**の下であられたオプションを選択し、『Next』 をクリック して下さい。
24. 設定を Summary セクションで確認し、『Done』 をクリック して下さい。
25. **属性ソース**で支持して下さい**及びユーザ ルックアップ**は『Next』 をクリック します。
26. **フェイル・セーフ属性ソース**の下で『Next』 をクリック して下さい。

27. 属性契約達成の下でこれらのオプションを選択し、『Next』をクリックして下さい。
28. 設定セクションを要約すると確認し、『Done』をクリックして下さい。
29. 認証ソース マッピングで『Next』をクリックします支持して下さい。
30. 設定が要約 ページの下で確認されたら『Done』をクリックして下さい。
31. アサーション作成で『Next』をクリックします支持して下さい。
32. プロトコル 設定の下で、プロトコル 設定を『Configure』をクリックして下さい。この時点で既に読み込まれる 2 つのエントリがあるはずで、[Next] をクリックします。
33. SLO の下で URL を『Next』をクリックします保守して下さい。
34. 正当な SAML バインディングで、オプション アーティファクトおよび石鹸のチェックを外し、『Next』をクリックして下さい。
35. シグニチャ ポリシーの下で『Next』をクリックして下さい。
36. 暗号化ポリシーの下で『Next』をクリックして下さい。
37. 要約 ページの設定を検討し、『Done』をクリックして下さい。
38. ブラウザで SSO > プロトコル 設定 『Next』をクリックし、検証し設定を、『Done』をクリックします支持して下さい。
39. ブラウザ SSO タブは現われます。[Next] をクリックします。
40. 信任状の下で信任状を『Configure』をクリックし、ISE コミュニケーションに IdP の間に使用されるべき署名証明書を選択し、オプションを含めずシグニチャに証明書をチェックして下さい。次に [Next] をクリックします。

注: あれば設定される証明書は証明書を『Manage』をクリックしないし、ISE コミュニケーションに IdP に署名するのに使用されるべき自己署名証明書を生成するためにプロンプトに従います。

41. 設定を要約 ページの下で検証し、『Done』をクリックして下さい。
42. タブが『Next』をクリックする信任状で支持して下さい。
43. アクティベーション及び要約の下でステータス アクティブを『Connection』を選択し、設定の他を検証し、『Done』をクリックして下さい。

ステップ 4. ISE 外部 SAML IdP プロバイダ プロファイルに IdP メタデータをインポートして下さい

1. PingFederate マネジメントコンソールの下で、設定 > 管理機能 > メタデータ エクスポートを『Server』を選択して下さい。サーバが複数のロールのために (IdP および SP) 設定されたら、によって識別 Provider (IdP) であるオプションを選択して下さい。[Next] をクリックします。

2. モードが「メタデータで」手動で含むために選択するメタデータの下で情報を選択して下さい。 [Next] をクリックします。
3. プロトコルの下で『Next』 をクリックして下さい。
4. 属性契約で『Next』 をクリックして下さい。
5. 署名キーの下で接続プロファイルで前もって設定される証明書を選択して下さい。 [Next] をクリックします。
6. メタデータ署名の下で署名証明書を選択すればチェックはキー情報要素この証明書の公開キーが含まれています。 [Next] をクリックします。
7. XML 暗号化証明の下で『Next』 をクリックして下さい。

注: ここの暗号化を実施するオプションはネットワーク Admin まであります。

8. Summary セクションの下で『Export』 をクリックして下さい。 生成されるメタデータ ファイルを保存し、次に『Done』 をクリックして下さい。
9. ISE の下で、Administration > アイデンティティ管理に > 外部識別ソースをたどります > SAML ID プロバイダ > PingFederate 選択して下さい。
10. プロバイダ構成を > 参照し、PingFederate メタデータ エクスポート オペレーションから保存されるメタデータをインポートすることを続行します 『Identity』 をクリックして下さい。
11. タブを『Groups』 を選択して下さい団体会員属性の下で memberOf を追加し、次に『Add』 をクリックして下さい

アサーションでという名で memberOf 属性が取得された形式 LADP 認証のとき戻す IdP が必要がある識別名を追加して下さい。 この場合設定されるグループは TOR のスポンサー グループにリンクされ、このグループのための DN は次の通りです:

DN をおよび追加すれば「ISE の名前」は説明『OK』 をクリックします。

12. タブを『Attributes』 を選択し、『Add』 をクリックして下さい。

このステップで、LDAP 上の Ping のクエリに基づいていた IdP から渡される SAML トークンで、それぞれのオブジェクトのための電子メール属性が含まれているべきである含まれていること属性「メール」を追加して下さい。

注: ISE が AD オブジェクト電子メールを受信し、IdP を通した MemberOf が属性操作をログインするようにステップ 11 および 12 はします。

検証

1. 門脈テスト URL を使用してゲスト ポータルを起動させて下さいまたは CWA に続くことによってフローして下さい。 ユーザにゲスト信任状を入力するオプションがありましたり自身のアカウントおよび従業員ログオンを作成します。
2. 従業員ログオンをクリックして下さい。 アクティブセッションがないのでユーザは IdP ログオ

ンポータルにリダイレクトされます。

3. AD 信任状を入力し、**サイン**をクリックして下さい。

4. IdP ログオン画面はゲスト門脈成功ページにユーザをリダイレクトします。

5. この時点でユーザが門脈ゲストに戻り、"Employee Login"を選択する度に、それらはネットワークでセッションが IdP でそれでもアクティブである限り許可されます。

トラブルシューティング

SAML ise-psc.log Administration > > SAML > > SAML

ISE CLI show logging ise-psc.log SAML > > > ISE > > ise-psc.log ise-psc.log

```
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-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-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- ResponseValidationContext:
    IdP URI: PingFederate
    SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
    Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action
    Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210
    Client Address: 14.0.25.62
    Load Balancer: null
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Validate signature to SAML standard
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
org.opensaml.xml.signature.SignatureValidator -:::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG [http-bio-14.36.157.210-8443-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-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.AssertionValidator -:::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.AssertionValidator -:::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][[]
cpm.saml.framework.validators.AssertionValidator -:::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-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@rtpaaa.net
SAML Exception:null

```
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-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-14.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED
```

関連情報

- [Cisco WLC および ISE 設定例の中央 Web 認証。](#)
- [スイッチおよび Identity Services Engine 設定例の中央 Web 認証。](#)
- [Cisco Identity Services Engine に関するリリース ノート、リリース 2.1](#)
- [Cisco Identity Services Engine 管理者ガイド、リリース 2.1](#)