PingFederate SAML SSO の ISE 2.1 スポンサー ポータルを設定する

目次

概要

この資料にユーザを後援するためにサイン On（SSO）単一機能を提供するように Cisco 識別 サービス Engine（ISE） 2.1 で PingFederate SAML サーバ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あることが推奨されます。

- Cisco Identity Services Engine ゲスト サービス。
- SAML SSO 配備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
- PING 識別からの PingFederate 8.1.3.0 サーバ。
- アクティブ ディレクトリ ディレクトリー・ サービスを用いる Windows サーバ 2012 R2。

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、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークがライブである場合、あらゆるコマンドの潜在的影響を理解することを確かめて下さい。

表記法

文書 の 表記法に関する詳細については Ciscoテクニカル情報 規定を参照して下さい

フロー 外観

セキュリティ アサーション マークアップ言語（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（スポンサー ユーザ）、識別プロバイダ（IdP）（PING 連合したサーバ）、およびサービスプロバイダー（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 が政策決定の間に利用できる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。 最初の認証が行われればサービスにアクセスするためにアサーション セッションが IdP でそれでもアクティブである限り、ユーザは資格情報のために再度プロンプト表示するべきではありません。

これはこの使用例のための期待されたフローです:

1. 設定されたスポンサー ポータルのカスタム完全修飾ドメイン名 （FQDN）の起動によってスポンサー ポータルにログインするユーザ試み。
2. ISE は IdP ことをに速いリダイレクトの発行によっ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。
3. IdP は LDAP によってユーザを認証し、ISE（SP）に memberOf および電子メール属性を渡します。
4. ISE は IdP XML 応答を処理し、memberOf アトリビュートとスポンサー グループ設定に基づいてユーザは許可されるか、または拒否されます（設定されたスポンサー グループを一致する 団体会員状態点検）。
5. セッション 存続可能時間は各ソリューションで変わります。 この使用例では、（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 PING Federate 60 分の**セッション タイムアウト**（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）削除されますおよび 480 分の**セッション最大タイムアウト**で設定されます。 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。
6. セッションがまだアクティブな間、スポンサー ユーザは入力資格情報なしでポータルにブラウザおよびカムバックを閉じられますはずです。

設定

以降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スポンサー 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:** スポンサー 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. on Cisco ISE は、**Administration > アイデンティティ管理**へのナビゲート **> 外部識別 > SAML ID プロバイダ ソースをたどります。**
2. 『Add』 をクリック して下さい
3. General タブの下で、ID プロバイダー名を入力し、『SAVE』 をクリック して下さい。 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スポンサー 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 > 設定 > スポンサー ポータル**へのナビゲート
2. **門脈スポンサーを (デフォルト)** クリックして下さいまたは新しいポータルを作成して下さい。
3. **門脈設定**の下でこのスポンサー ポータルにリンクされるカスタム完全修飾ドメイン名 (FQDN) を入力して下さい。
4. 外部 SAML IdP が以前に定義した**識別出典 シーケンス**から選択して下さい。
5. 流れ図が次を表す確認し、『SAVE』 をクリック して下さいことを:

ステップ 3. ISE 認証要求を処理する IdP として設定 PingFederate

1. ISE **Administration > アイデンティティ管理**へのナビゲートは **> 外部識別 > SAML ID プロバイダ >** PingFederate **ソースをたどります**
2. **サービスプロバイダー Info タブを**クリックし、『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。 ここに含まれていた XML ファイルは PingFederate でプロファイルを作成している間使用されます。

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、以前に ISE からエクスポートされる XML ファイルを『File』 を選択 し、『File』 を選択 し、選択します。

9. **メタデータ要約**の下で、『Next』 をクリック して下さい。

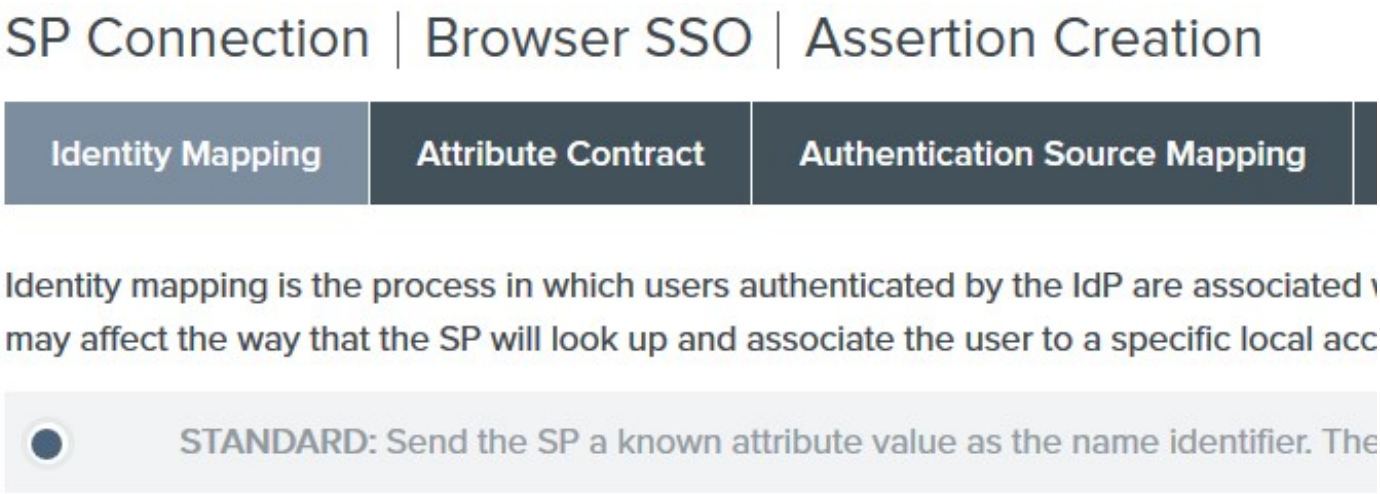
10. **接続名**の下の一般情報 ページで、名前 (IE を入力して下さい。 ISEsponsorPortal は) 『Next』 をクリック し。

11. **ブラウザ SSO** の下で**ブラウザ SSO を SAML プロファイル** チェックの下でこれらのオプション 『Configure』 をクリック し、『Next』 をクリック して下さい:

12. **アサーション ライフタイム**で『Next』 をクリック して下さい

13. **アサーション作成**で**アサーション作成を**『Configure』 をクリック して下さい

14. **識別マッピング**の下で**規格を**選択し、『Next』 をクリック して下さい



15. **アトリビュート契約**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。** 次に [Next] をクリックします。

> **注:** これは ISE がマッピング する正しいスポンサー グループのためのこれらの属性に頼る で、またです正しい通知関数に必要 E-メールを送りますので極めて重要な手順。

16. **認証 出典マッピング**の下で**新しいアダプター インスタンスを**『Map』 をクリック して下さい。

17. **アダプター インスタンス**で **HTML 形式アダプタを**選択して下さい。 [Next] をクリックします。

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. アトリビュートで**出典及びユーザ ルックアップはアトリビュート 出典** ボックスを『Add』 をクリック します。

20. **データ ストア**の下で説明を入力し、そして**アクティブなデータ ストア**から LDAP 接続 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。 設定されるデータ記憶装置がけれども新しい例を追加するためになかったら**データ記憶装置を**『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 はエラー「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ります。

22. **LDAP フィルタ**の下でストリング **sAMAccountName=$ {username}を**追加し、『Next』 をクリック して下さい。

23. **アトリビュート契約達成**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

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. **アトリビュート 出典**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・ セイフ アトリビュート 出典**の下で『Next』 をクリック して下さい。

27. **アトリビュート契約達成**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:

27. 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。

28. **認証 出典マッピング**で『Next』 をクリック します支持して下さい。

29. 設定が **Summary セクション**の下で確認されたら『Done』 をクリック して下さい。

30. **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。

31. **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 3 エントリがあるはずです。 『Next』 をクリック して下さい

32. SLO の下で **URL を**『Next』 をクリック します**保守して下さい**

33. **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。

34. **シグニチャ ポリシー**の下で『Next』 をクリック して下さい。

35. **暗号化ポリシー**の下で『Next』 をクリック して下さい。

36. **要約 ページ**の設定を検討し、『Done』 をクリック して下さい。

37. **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。 これは**ブラウザ SSO** タブを持ち帰ります。 [Next] をクリックします。

38. **資格情報**の下で**資格情報を**『Configure』 をクリック し、ISE 通信に 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**含めますシグニチャに認証を**チェックして下さい。 次に [Next] をクリックします。

注: 設定される認証がない場合**認証を**『Manage』 をクリック し、ISE 通信に 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って下さい。

39. 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。

40. タブが『Next』 をクリック する **資格情報**で支持して下さい。

41. **接続ステータス アクティブ**で選り抜き**アクティベーション及び要約**の下で設定の他を検証し、『SAVE』 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、サーバが複数のロールのために設定されたら**サーバコンフィギュレーション > 管理機能 > メタデータ エクスポート**へのナビゲートは (IdP および SP) によって**識別 Provider (IdP) である**オプションを選択します。 『Next』 をクリック して下さい

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. **アトリビュート契約**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認証を選択して下さい。 [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 ヒント要素この認証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。 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「Save」を生成されるメタデータ ファイル『Export』 をクリック し、次に『Done』 をクリック して下さい。

9. ISE の下で、**> 外部識別は Administration > アイデンティティ管理にソースをたどります > SAML ID プロバイダ > PingFederate** ナビゲート します。

10. **プロバイダを Config** >Click が**参照する**『Identity』 をクリック 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て下さい。

11. タブを『Groups』 を選択 すれば **団体会員 アトリビュート**の下で **memberOf を**追加し、次に『Add』 をクリック して下さい

12. **アサーションで**という名で **memberOf** アトリビュートが取得された形式 LDAP認証のとき IdP が戻す必要がある**識別名を**追加して下さい。このグループはスポンサー グループにリンクされます。

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。

13. タブを『Attributes』 を選択 し、『Add』 をクリック して下さい。 このステップでアトリビュート**「メール」を**追加します。 これは SAML 認証で含まれています; IdP から (アクティブ ディレクトリのそのユーザ オブジェクトのための電子メール アトリビュートに基づく) 渡される結果。

> **注:** このステップは重要自己登録済みのフローからの保留中のステータスのアカウントをマッピング できるスポンサーのセッションにリンクされる電子メールを処理できるはずであ

る ISE はです。 他ではアカウントはリンボー状態を参照された」電子メールである「人が有効なスポンサー セッションにマッピング されないので維持します。 それは電子メール通知のためにまた重要提案しますです。

14. **Advanced タブ**の下で次の設定を選択して下さい:

注: このセクションは IdP サーバに Logout 要求に電子メール アトリビュートを含めるように ISE に指示します。 これはスポンサー ユーザがポータルから手動で口グオフするとき重要です。

15. [Save] をクリックします。

16. このステップで管理者はスポンサー グループに IdP によって取得されたアクティブ ディレクトリ グループをマッピング します。 **作業センター > ゲスト アクセス > 設定 > スポンサー**へのナビゲートは > **ALL_ACCOUNTS グループ化します** (または適切なグループを選択して下さい) 。 **メンバーを**クリックし、**PingFederate を**選択して下さい: 私達をマッピング し、前のステップで選択したユーザ Groups カラムに追加しますそれを**グループ化して下さい**。 次に [OK] をクリックします。

17. 自己によって登録されているフローが設定される場合、アカウントは承認迄あります。 この場合オブジェクト Eメールアドレスを確認する簡単な方法が AD **割り当てられ、**である**メール** アトリビュートを使用して IdP サーバによって ISE のスポンサー識別に選択して下さいので、**「承認し、自己登録済みのゲストからの View 要求」**選択します**このスポンサーに」**転送される**アカウント迄「だけ**。

18. [Save] をクリックします。 これは ISE の設定を終了します。

確認

1. 設定されたカスタム FQDN を使用してスポンサー ポータルを起動させて下さい。 ISE は PingFederate ユーザ認証ポータルにユーザをリダイレクトする必要があります。

2. アクティブ ディレクトリ 資格情報およびヒット サインを入力して下さい。 IdP ログオン画面は ISE のスポンサー ポータルの最初の AUP にユーザをリダイレクトします。

この時点でスポンサー ユーザはポータルにフルアクセスがあるはずです。

3. 単一 サインを確認して下さい。 「**門脈テスト URL**」機能が使用されるとき ISE はスポンサー資格情報を SSO が設定されない場合毎回頼む必要があります。

門脈テスト URL リンクのスポンサー ポータルを起動させて下さい。 ISE スポンサー URL は IdP URL にセッションステータスが資格情報を入力する必要なしでスポンサー ポータルに戻ってセッション トークンが確認されればクライアント リダイレクトされる確認するためにすぐに切り替え。

4. 電子メール アトリビュートがアクティブ ディレクトリ オブジェクトから IdP ISE にに正しく通じることを確認して下さい。 テストする最も簡単な方法は門脈スポンサーの新しいアカウントを作成し、**呼出** オプションを選択することによって行います。 電子メールが正しく取得されればスポンサーの **eメールアドレス** フィールドの下で現われます。

5. **ログアウト**機能を確認して下さい。 これはスポンサー ログアウトがトークン セッションを終わるべき識別サーバ側で引き起こすことを確認して統合で重大です。 ユーザがスポンサー ポータルにアクセスすることを試みる時次に門脈スポンサーから署名し、IdP 認証 画面に戻ってリダイレクトされることを確かめて下さい。

トラブルシューティング

どの SAML 認証 トランザクションでも **ise-psc.log** の下にログオンされた ISE 側です。 **Administration > ロギング > デバッグ ログ 設定**の下に専用コンポーネント（**SAML**）が > 選択します**デバッグ レベル**に > 設定 された **SAML** コンポーネント疑わしいノードをあります。

ISE によって CLI にアクセスでき、「show logging アプリケーション ise-psc.log 末尾」を発行し、SAML イベントを監視するために住めば、**オペレーション**の下で **> 解決します > ダウンロード ログ** > 選択します ISE ノード > **デバッグ ログ** タブを > クリックしますログをダウンロードするために **ise-psc.log を**更なる分析のための **ise-psc.log を**ダウンロードできます。

通常最初の認証 ログはこのようになります:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>


2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

トークンはまだアクティブであることを最初のログイン イベントの後、確認するためにユーザアクセスはスポンサー ポータル私達 ISE がアサーション情報を検索することを見るたびに。 結果はこのようになる必要があります:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>
```

```
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

関連情報

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