SAML SSOでのISE 3.1 GUI口グインのトラブルシューティング

内容

概要

このドキュメントでは、SAML GUI口グインを使用したISE 3.1で観察されたほとんどの問題について説明します。SAML 2.0標準の使用により、SAMLベースの管理口グインにより、ISEにシングルサインオン(SSO)機能が追加されます。Azure、Okta、PingOne、DUO Gatewayなどの任意のIdentity Provider(IdP)、またはSAML 2.0を実装する任意のIdPを使用できます。

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。

1. Cisco ISE 3.1以降
2. SAML SSOセットアップの基本を理解する

設定とフローの詳細については、『SAML設定のISE 3.1管理者ガイド』および『Azure ADを使用したSAMLによるISE管理者口グインフロー』を参照してください。

> **注：**アイデンティティプロバイダサービスに精通し、サービスが稼働していることを確認する必要があります。

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。

- ISE バージョン 3.1

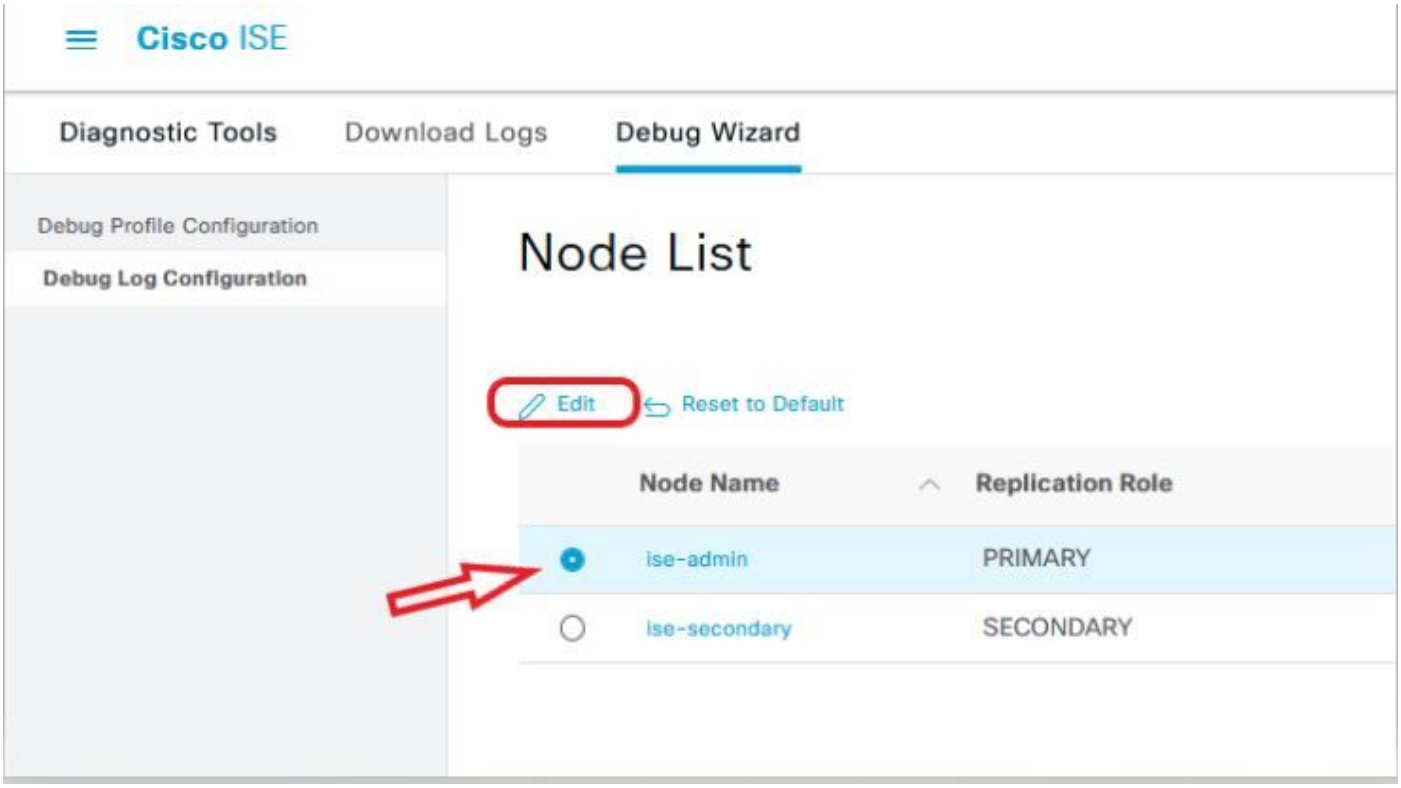
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

デバッグをイネーブルにする

トラブルシューティングを開始するには、まず次の説明に従ってデバッグを有効にする必要があります。

[Operations] > [Troubleshoot] > [Debug Wizard] > [Debug Log Configuration] に移動します。**プライマリ管理ノードを選択し、次の図に示すように[Edit]** をクリックします。



- 次のコンポーネントを**DEBUG**レベルに設定します。

コンポーネント名	ログ レベル	ログファイル名
ポータル	デバッグ	guest.log
opensaml	デバッグ	ise-psc.log
saml	デバッグ	ise-psc.log

> **注：** トラブルシューティングが完了したら、ノードを選択してデバッグをリセットし、[Reset to Default]をクリックします。

ログのダウンロード

問題が再現されたら、必要なログファイルを取得する必要があります。

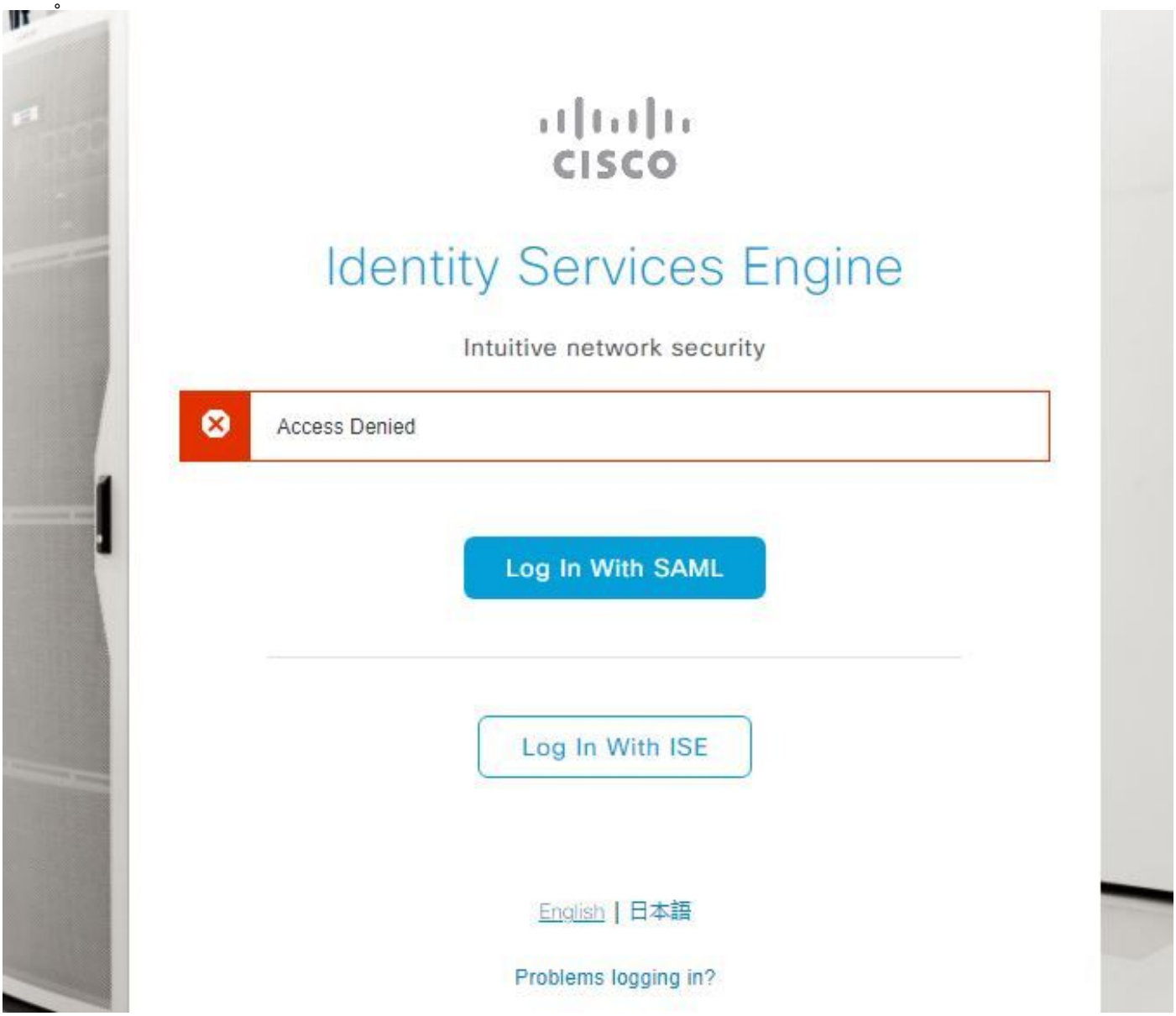
ステップ1:[Operations] > [Troubleshoot] > [Download logs] に移動します。[Appliance node list] > [Debug Logs]でプライマリ管理ノードを選択します。

ステップ2:guestおよびise-pscの親フォルダを見つけて展開します

ステップ3:ダウンロード guest.log と ise-psc.log ファイルが削除されます。

問題1a:アクセス拒否

- SAMLベースの管理者ログインを設定した後、
  - [Log in With SAML]を選択します。
  - IdPログインページへのリダイレクトは正常に機能します
  - SAML/IdP応答ごとの認証が成功しました
  - IdPの送信グループ属性と、ISEで設定されている同じグループ/オブジェクトIDを確認できます。
  - 次に、ISEがポリシーを分析しようとすると、スクリーンショットに示すように、「Access Denied」メッセージを引き起こす例外がスローされます
    。



ise-psc.logのログ

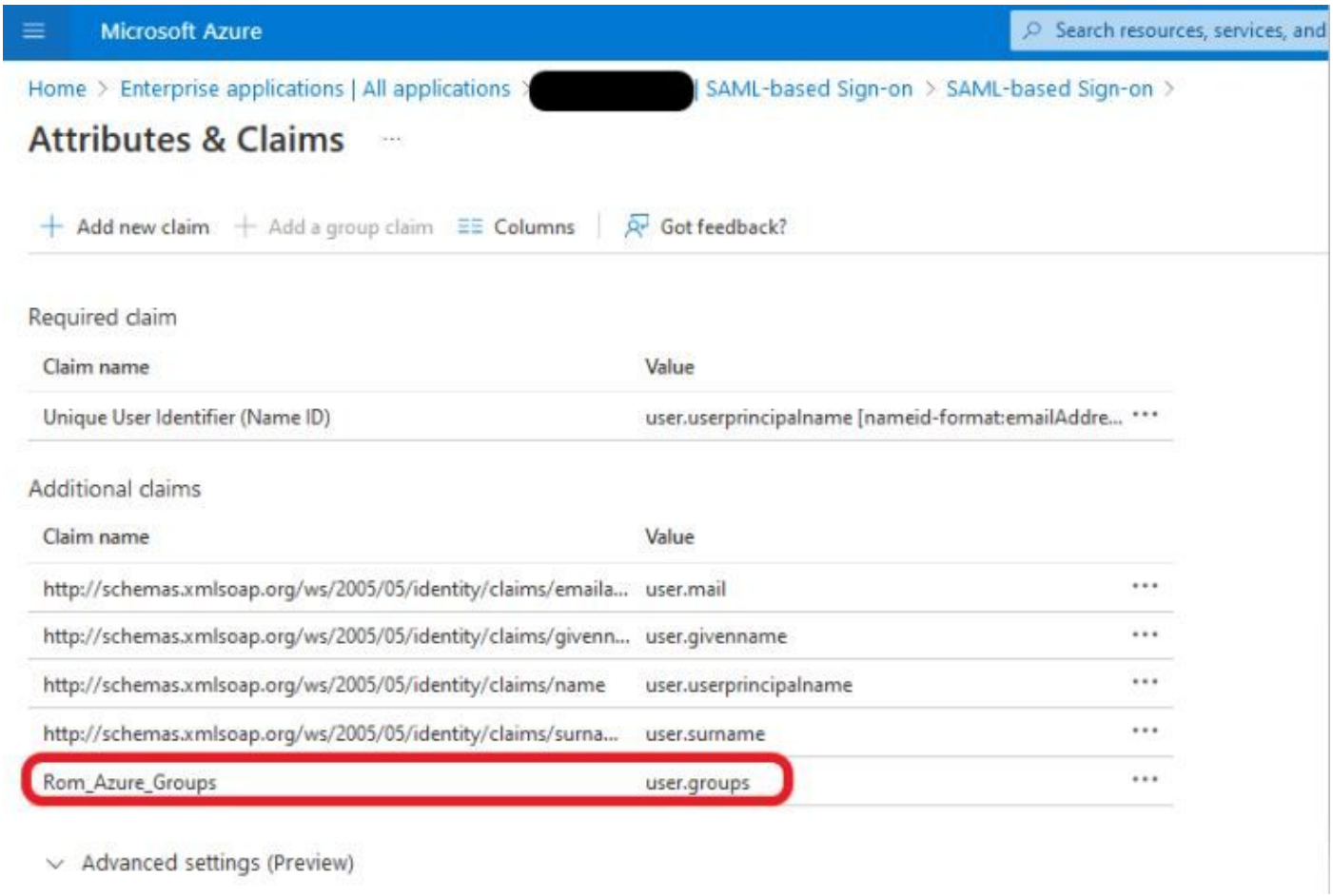
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true SAML Status Message:null SAML
email: SAML Exception:nullUserRole : NONE 2021-09-27 17:16:18,218 DEBUG [https-jsse-nio-
10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser
- about to call authenticateSAMLUser messageCode:null subject: ise.test 2021-09-27 17:16:18,225
DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::-
Authenticate SAML User - result:PASSED 2021-09-27 17:16:18,390 INFO [admin-http-pool5][]
ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl -::::- **********Rbac Log
Summary for user samlUser********** 2021-09-27 17:16:18,392 INFO [admin-http-
pool5][] com.cisco.ise.util.RBACUtil -::::- Populating cache for external to internal group
linkage. 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][]
```

```
cpm.admin.infra.utils.PermissionEvaluationUtil -:::::- Exception in login action
java.lang.NullPointerException 2021-09-27 17:16:18,402 INFO [admin-http-pool5][]
cpm.admin.infra.action.LoginAction -:::::- In Login Action user has Menu Permission: false 2021-
09-27 17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login
action, user has no menu permission 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][]
cpm.admin.infra.action.LoginAction -:::::- Can't save locale. loginSuccess: false 2021-09-27
17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginActionResultHandler -:::::-
Redirected to: /admin/login.jsp?mid=access_denied
```

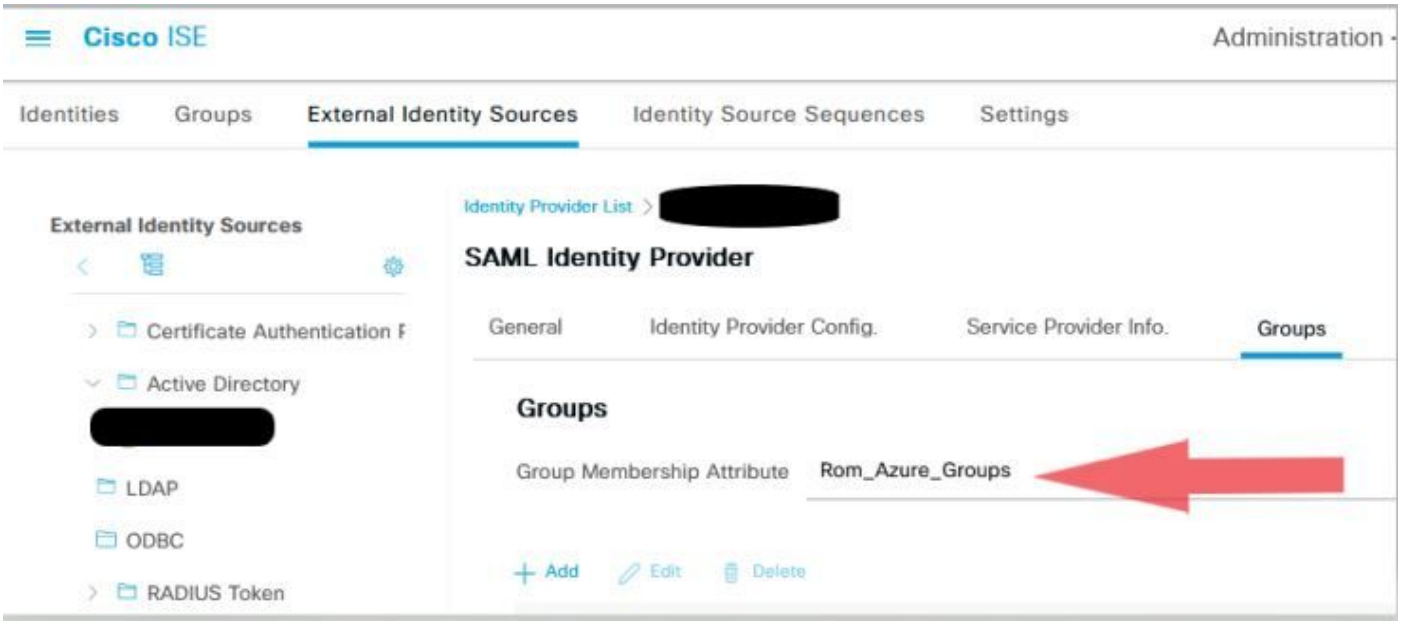
原因/ソリューション

IdP設定のグループ要求名がISEで設定されているものと同じであることを確認します。

次のスクリーンショットはAzure側から撮影したものです。



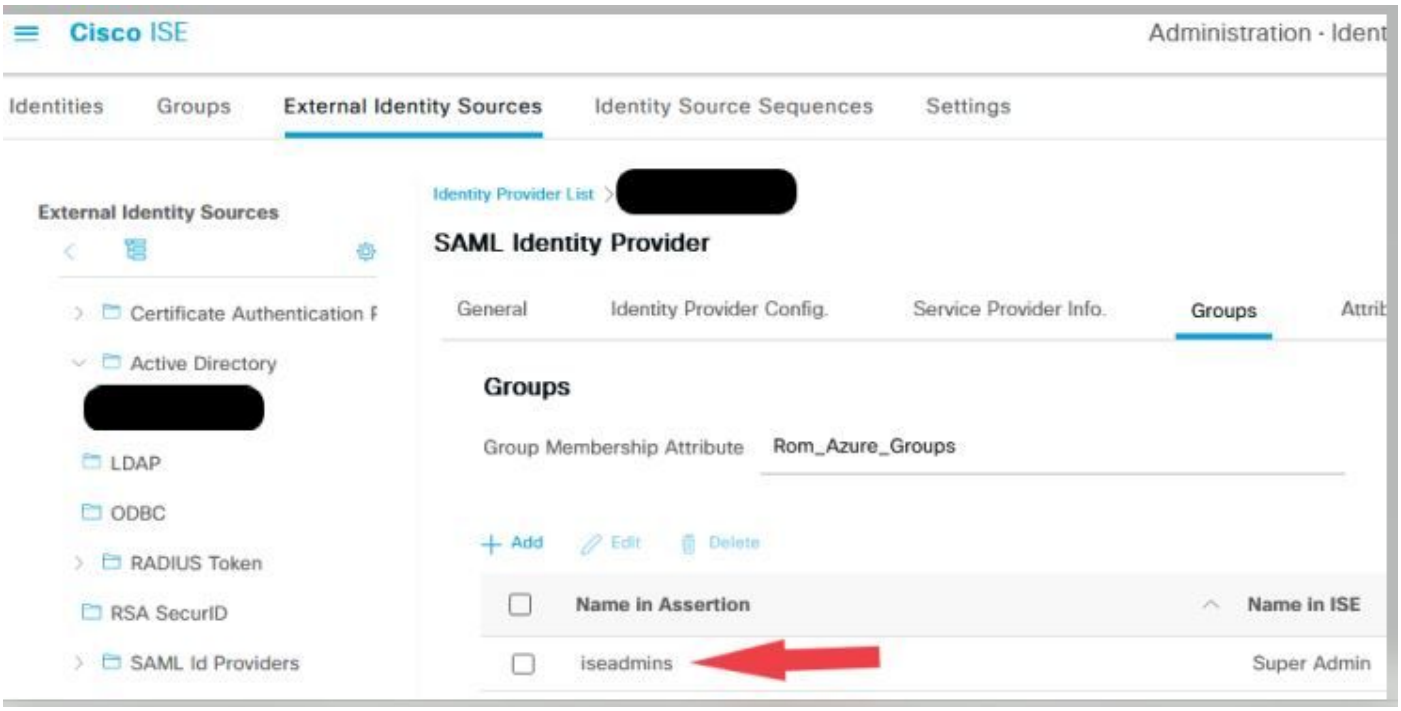
ISE側のスクリーンショット。



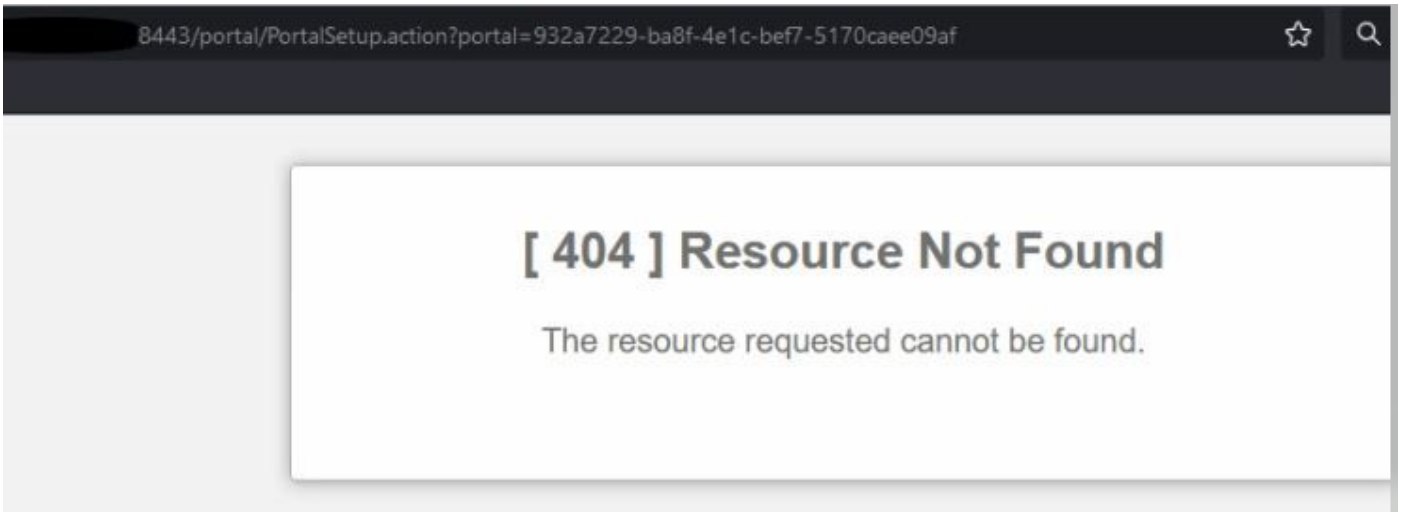
問題1b:SAML応答の複数のグループ（アクセス拒否）

前の修正で問題が解決しない場合は、ユーザが複数のグループのメンバでないことを確認します。この場合は、Cisco Bug ID CSCwa17470が発生している必要があります。ISEはSAML応答のリストの最初の値（グループ名/ID）にのみ一致します。このバグは3.1 P3で解決されています

前に示したIdP応答に従って、ログインを成功させるには、**isedms**グループのISEマッピングを設定する必要があります。



問題 2：404 Resource not found



guest.logにエラーが表示されます

```
2021-10-21 13:38:49,308 ERROR  [https-jsse-nio-10.200.50.44-8443-exec-3][]
cpm.guestaccess.flowmanager.step.StepExecutor -::-
Can not find the matched transition step on Step=id: 51d3f147-5261-4eb7-a1c9-ce47ec8ec093,
tranEnum=PROCEED_SSO.
```

原因/ソリューション

この問題は、が最初のIDストアを作成した後にのみ発生します。

この問題を解決するには、次の手順を同じ順序で実行します。

ステップ1:ISEに新しいSAML IdPを作成します（現在のSAML IdPはまだ削除しないでください）。

ステップ2:admin accessページに移動し、この新しいIdPにadminアクセス権を割り当てます。

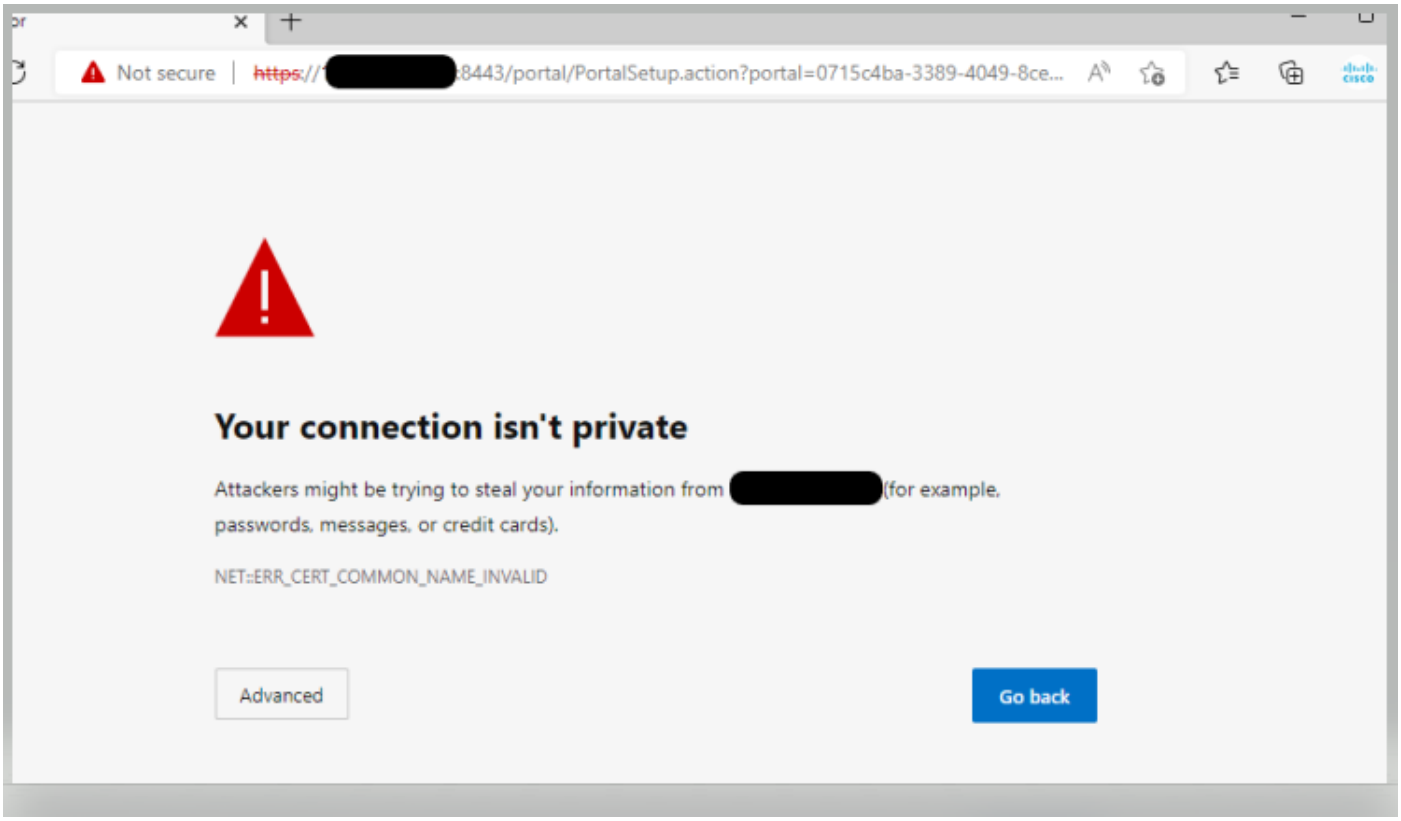
ステップ3:[External Identity Providers] ページで古いIdPを削除します。

ステップ4:現在のIdPメタデータをステップ1で作成した新しいIdPにインポートし、必要なグループマッピングを実行します。

ステップ5:SAMLログインを試してください。動くでしょう

問題 3：証明書の警告

マルチノード展開では、[Log In with SAML]をクリックすると、ブラウザに[Un-trusted certificate warning]が表示されます



原因/ソリューション

場合によっては、pPANはユーザをFQDNではなくアクティブPSNのIPにリダイレクトします。これにより、SANフィールドにIPアドレスがない場合、一部のPKI展開で証明書の警告が発生します。

回避策は、証明書のSANフィールドにIPを追加することです。

Cisco Bug ID CSCvz89415。これは3.1p1で解決されています。

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。