Fehlerbehebung bei der Benutzeroberfläche von ISE 3.1 Anmeldung mit SAML SSO

Inhalt

Einleitung

In diesem Dokument werden die meisten Probleme beschrieben, die in ISE 3.1 mit der SAML-GUI-Anmeldung beobachtet wurden. Durch die Verwendung des SAML 2.0-Standards fügt SAML-basierte Admin-Anmeldung der ISE Single Sign-on (SSO)-Funktionen hinzu. Sie können jeden Identity Provider (IdP) wie Azure, Okta, PingOne, DUO Gateway oder jeden IdP verwenden, der SAML 2.0 implementiert.

Voraussetzungen

Anforderungen

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

1. Cisco ISE 3.1 oder höher
2. Grundlagen der SAML SSO-Einrichtung

Weitere Details zur Konfiguration und zum Ablauf finden Sie im ISE 3.1-Administrationsleitfaden für die SAML-Konfiguration und den ISE Admin Login Flow via SAML mit Azure AD.

> **Anmerkung:** Sie müssen mit dem Identity Provider-Dienst vertraut sein und sicherstellen, dass dieser ausgeführt wird.

Verwendete Komponenten

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

- ISE Version 3.1

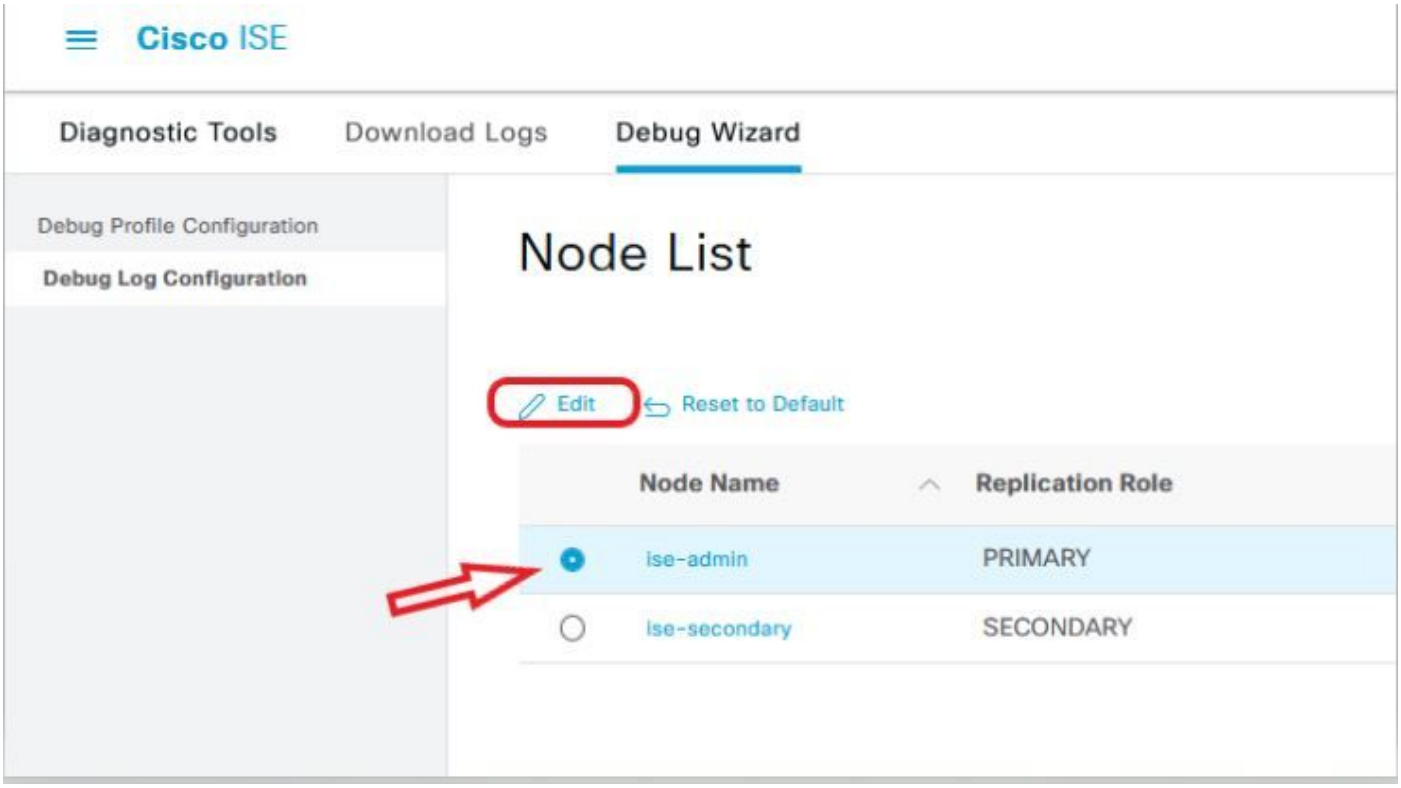
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

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

Aktivieren Sie die Fehlersuche.

Um mit der Fehlerbehebung zu beginnen, müssen Sie zunächst die Debugs wie unten beschrieben aktivieren.

Navigieren Sie zu **Operationen > Fehlerbehebung > Debugassistent > Debugprotokollkonfiguration.** Wählen Sie den Primärknoten Admin aus, und klicken Sie auf **Bearbeiten**, wie im nächsten Bild dargestellt.



- Legen Sie für die nächsten Komponenten die **DEBUG-**Stufe fest.

Komponentenname	Protokollstufe	Protokolldateiname
Portal	DEBUG	guest.log
opensaml	DEBUG	ise-psc.log
kleine	DEBUG	ise-psc.log

> **Anmerkung:** Wenn Sie mit der Fehlerbehebung fertig sind, denken Sie daran, die Debugs zurückzusetzen, indem Sie den Knoten auswählen und auf "Reset to Default" (Auf Standard zurücksetzen) klicken.

Protokolle herunterladen

Sobald das Problem reproduziert wurde, müssen Sie die erforderlichen Protokolldateien abrufen.

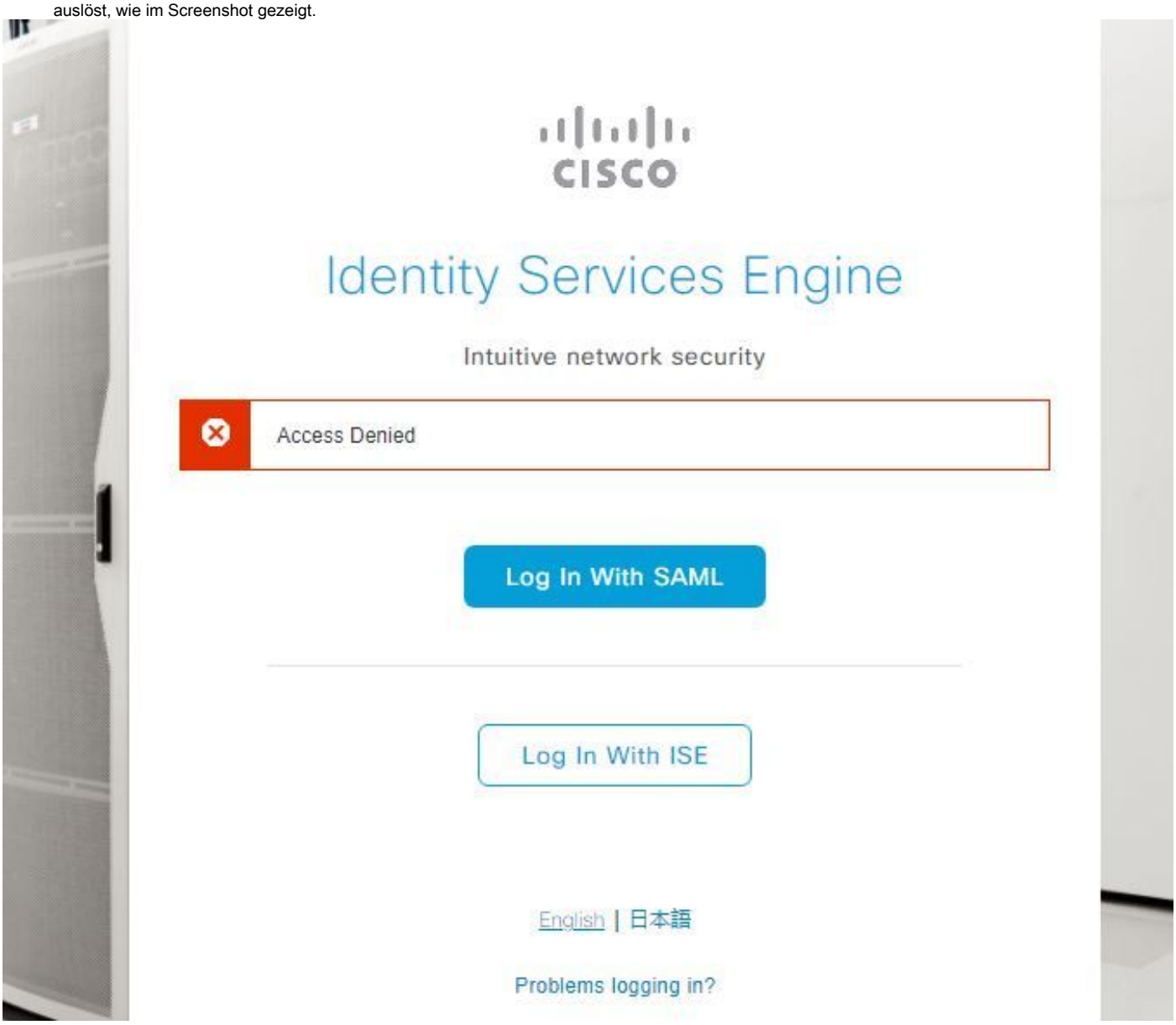
Schritt 1: Navigieren Sie zu Vorgänge > Fehlerbehebung > Protokolle herunterladen. Wählen Sie den primären Admin-Knoten unter 'Liste der Appliance-Knoten' > Debug-Protokolle aus.

Schritt 2: Suchen und Erweitern der übergeordneten Guest- und ise-psc-Ordner

Schritt 3: Herunterladen guest.log und ise-psc.log Dateien.

Problem 1a: Zugriff verweigert

- Nachdem Sie Ihre SAML-basierte Admin-Anmeldung konfiguriert haben,
- Wählen Sie Mit SAML anmelden.
- Die Umleitung zur IDp-Anmeldung auf der Seite funktioniert wie erwartet.
- Die Authentifizierung ist gemäß SAML/IdP-Antwort erfolgreich.
- IdP sendet Gruppenattribut, und es wird dieselbe Gruppen-/Objekt-ID angezeigt, die in ISE konfiguriert wurde.
- Wenn die ISE dann versucht, ihre Richtlinien zu analysieren, löst sie eine Ausnahme aus, die die Meldung "Access Denied" (Zugriff verweigert) auslöst, wie im Screenshot gezeigt.



Meldet sich in ise-psc.log an

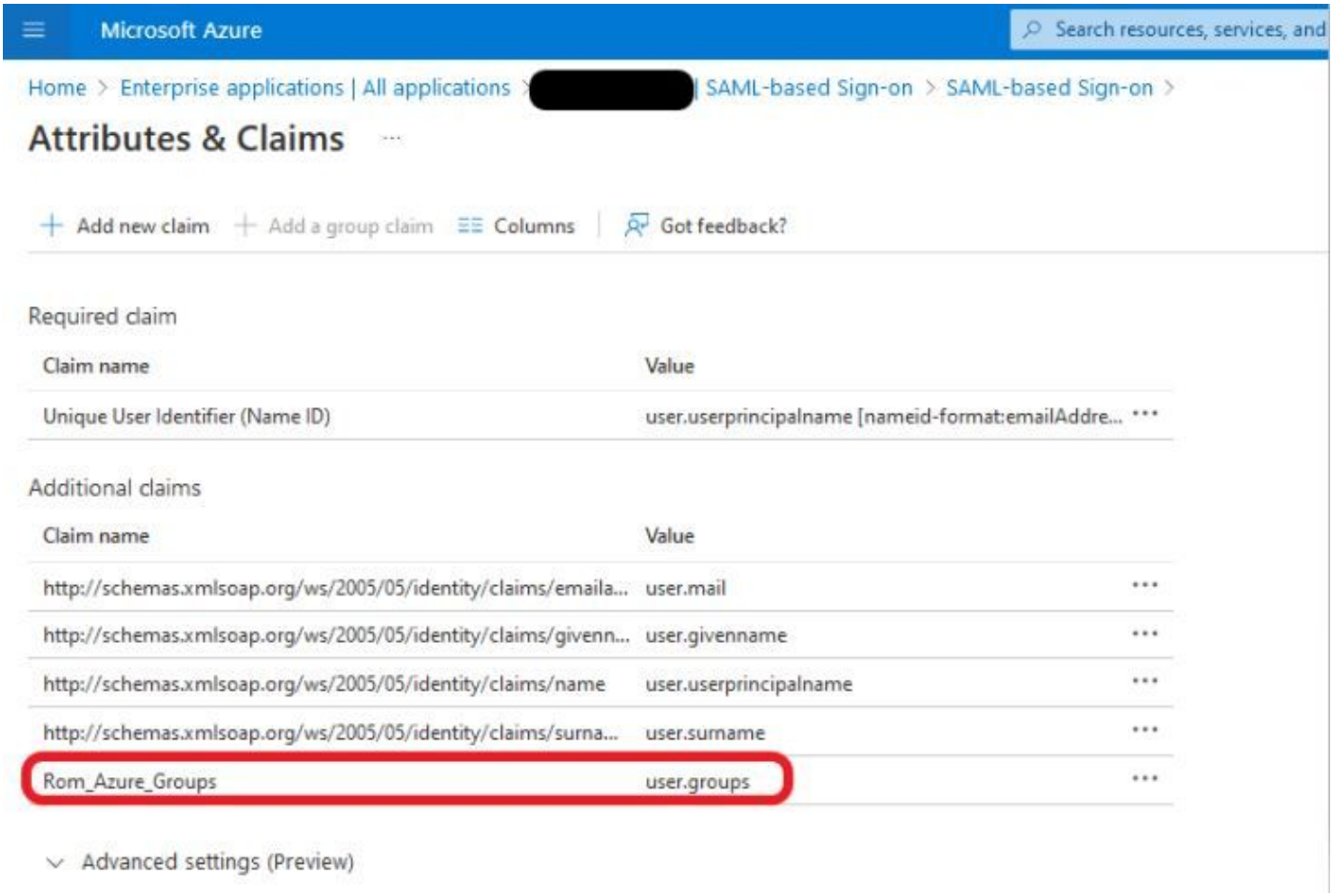
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true 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
```

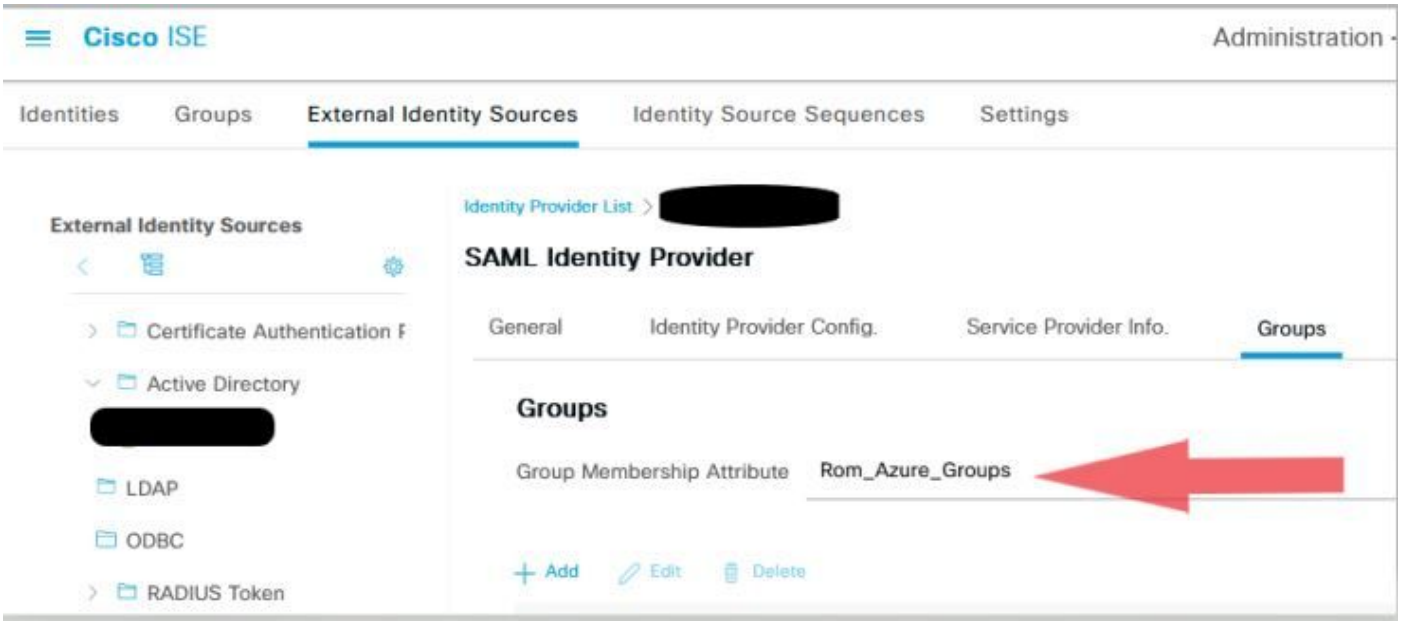
Ursache/Lösung

Stellen Sie sicher, dass der Gruppenname in den IdP-Konfigurationen mit dem in der ISE konfigurierten Namen übereinstimmt.

Der nächste Screenshot stammt von Azure-Seite.



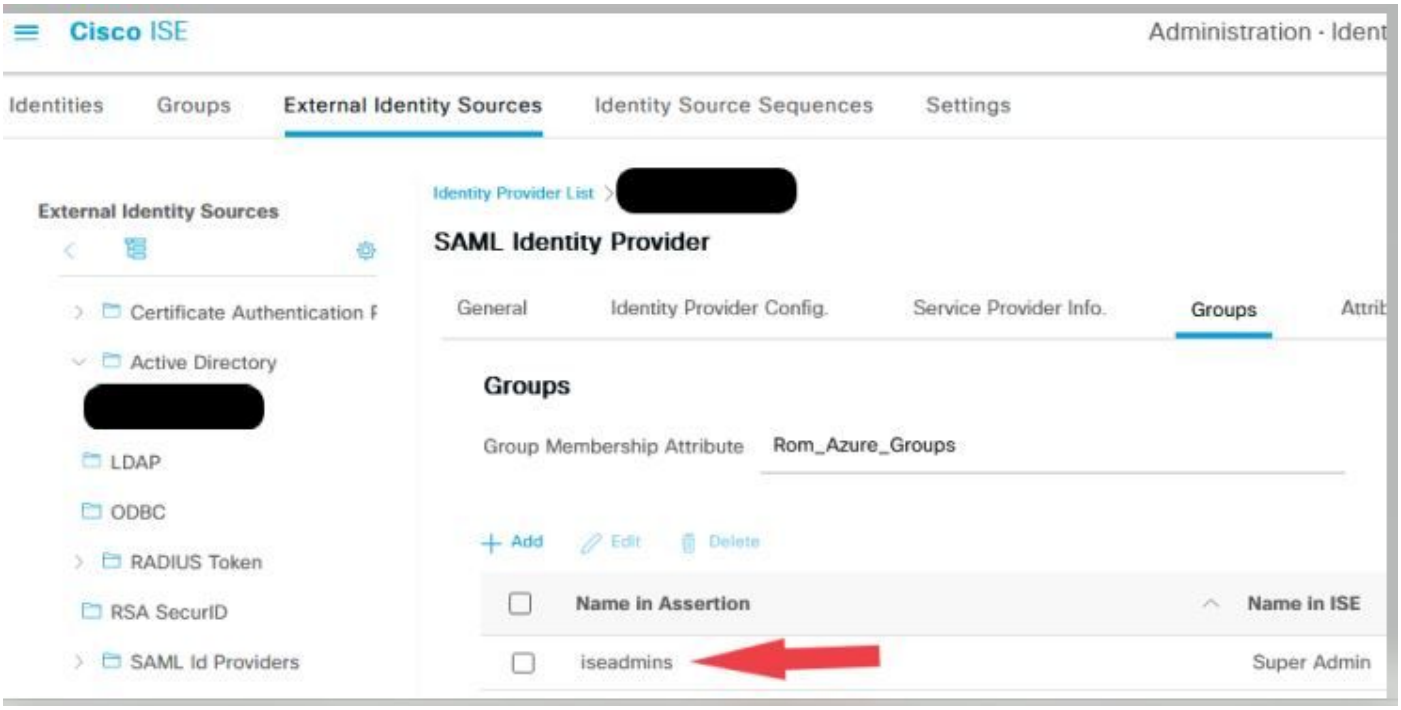
Screenshot der ISE-Seite.



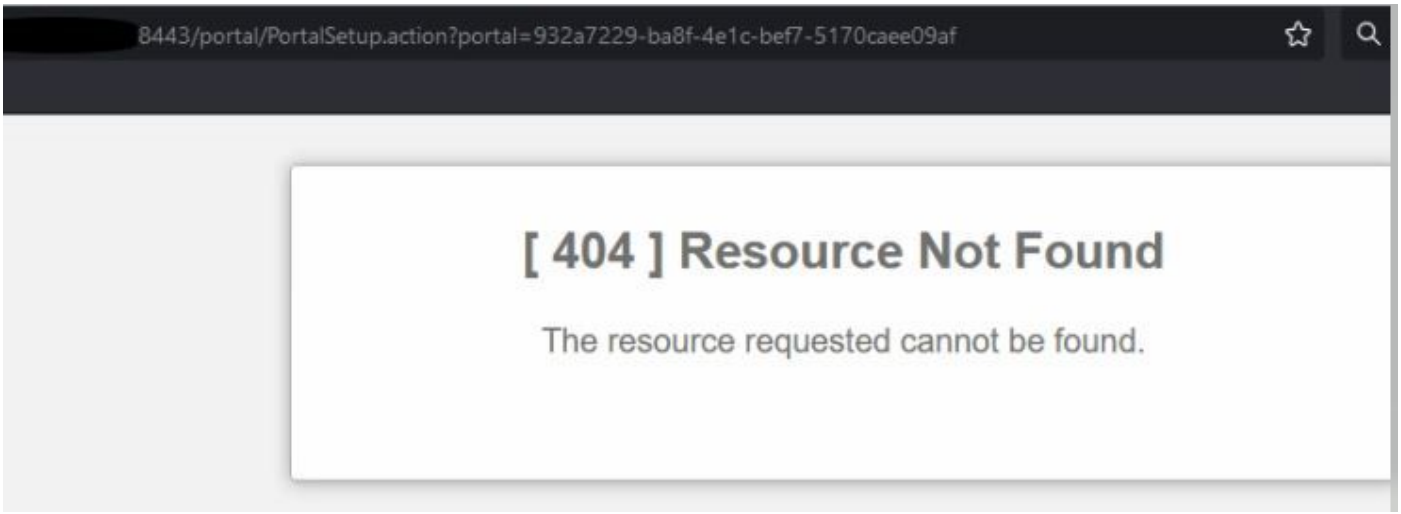
Problem 1b: Mehrere Gruppen in SAML-Antwort (Zugriff verweigert)

Wenn der vorherige Fix das Problem nicht löst, stellen Sie sicher, dass der Benutzer nicht Mitglied mehrerer Gruppen ist. In diesem Fall müssen Sie auf die Cisco Bug-ID CSCwa17470 gestoßen sein, wobei ISE nur dem ersten Wert (Gruppenname/ID) in der Liste aus der SAML-Antwort entspricht. Dieser Fehler wurde in 3.1 P3 behoben

Gemäß der zuvor angegebenen IdP-Antwort muss die ISE-Zuordnung für die **iseadmins**-Gruppe konfiguriert werden, damit die Anmeldung erfolgreich ist.



Problem 2: 404 Ressource nicht gefunden



Sie sehen einen Fehler in **guest.log**

```
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.
```

Ursache/Lösung

Dieses Problem tritt auf, nachdem nur der erste ID-Speicher erstellt wurde.

Führen Sie zur Behebung dieses Problems den nächsten Schritt in derselben Reihenfolge aus:

Schritt 1. Erstellen Sie eine neue SAML-IDp in Ihrer ISE (entfernen Sie die aktuelle noch nicht).

Schritt 2: Gehen Sie zur Admin-Zugriffsseite, und weisen Sie Ihren Admin-Zugriff dieser neuen IdP zu.

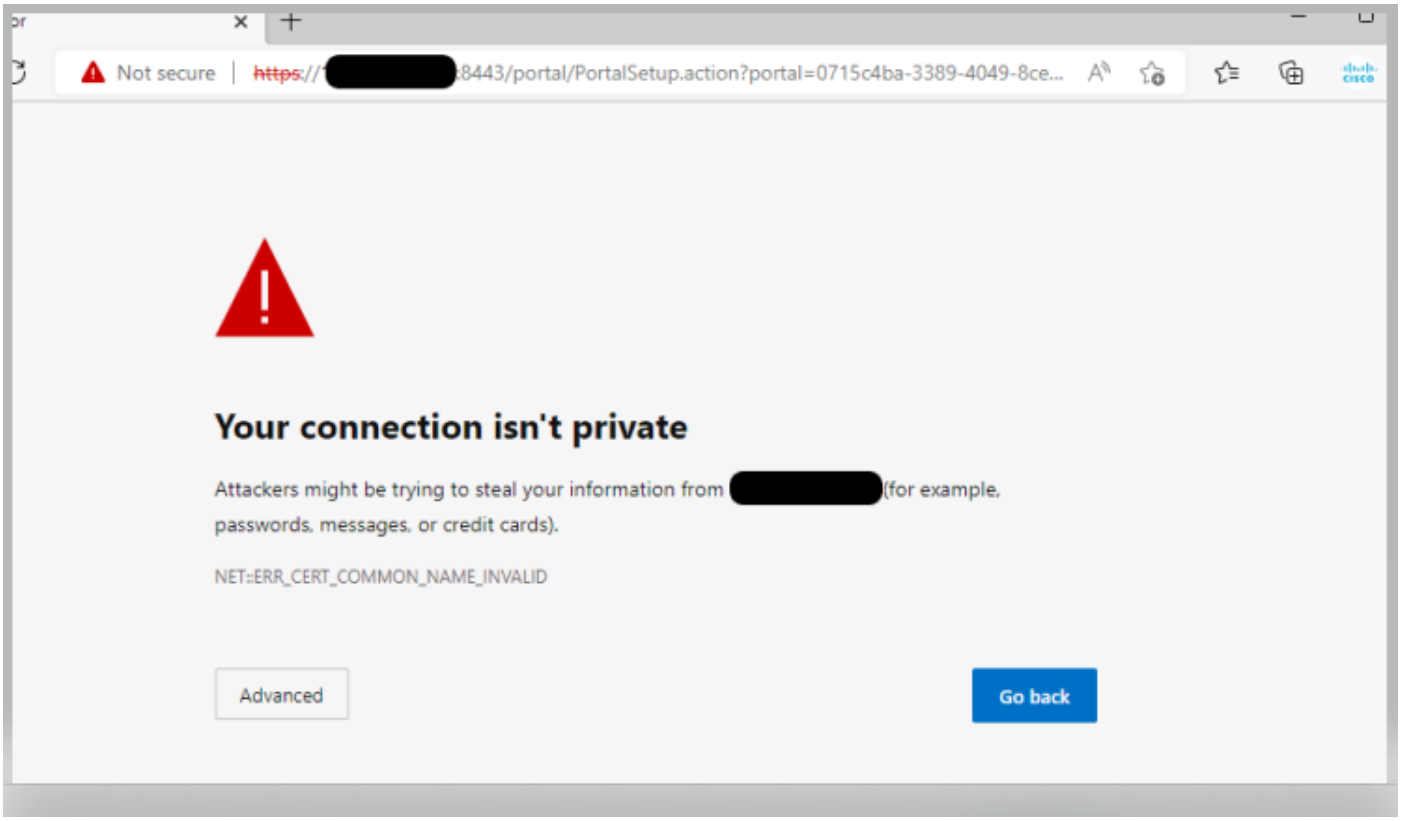
Schritt 3: Löschen Sie die alte IDp in External Identity Providers.

Schritt 4: Importieren Sie die aktuellen IdP-Metadaten in die in Schritt 1 erstellte neue IdP, und führen Sie alle erforderlichen Gruppenzuordnungen durch.

Schritt 5. Versuchen Sie nun SAML-Login; wird es funktionieren.

Problem 3: Zertifikatswarnung

Wenn Sie in einer Multi-Node-Bereitstellung auf "Log In with SAML" (Anmelden mit SAML) klicken, wird im Browser eine Warnung vor nicht vertrauenswürdigem Zertifikat angezeigt.



Ursache/Lösung

In einigen Fällen leitet pPAN Sie zur IP der aktiven PSNs um, nicht zu FQDN. Dies führt bei einigen PKI-Bereitstellungen zu einer Zertifikatwarnung, wenn im SAN-Feld keine IP-Adresse angegeben ist.

Die Problemumgehung besteht darin, IP im SAN-Feld des Zertifikats hinzuzufügen.

Cisco Bug-ID CSCvz89415. Dies wird in 3.1p1 behoben.

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.