Probleemoplossing ISE 3.1 GUI-aanmelding met SAML SSO

Inhoud

Inleiding

Dit document beschrijft de meeste problemen die in ISE 3.1 met SAML GUI login zijn waargenomen. Door het gebruik van de SAML 2.0 standaard, op SAML-gebaseerde admin log-in voegt Single Sign-on (SSO) mogelijkheid toe aan ISE. U kunt elke Identity Provider (IDP) gebruiken zoals Azure, Okta, PingOne, DUO Gateway of elke IDP die SAML 2.0 implementeert.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

1. Cisco ISE-lijnkaart 3.1 of hoger
2. Begrijp de grondbeginselen van de opstellingen van SAML SSO

Raadpleeg de ISE 3.1 admin-handleiding voor SAML-configuratie en ISE Admin Login Flow via SAML met Azure AD voor meer informatie over de configuratie en flow.

> **Opmerking:** U moet bekend zijn met uw Identity Provider-service en ervoor zorgen dat deze actief is.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE, versie 3.1

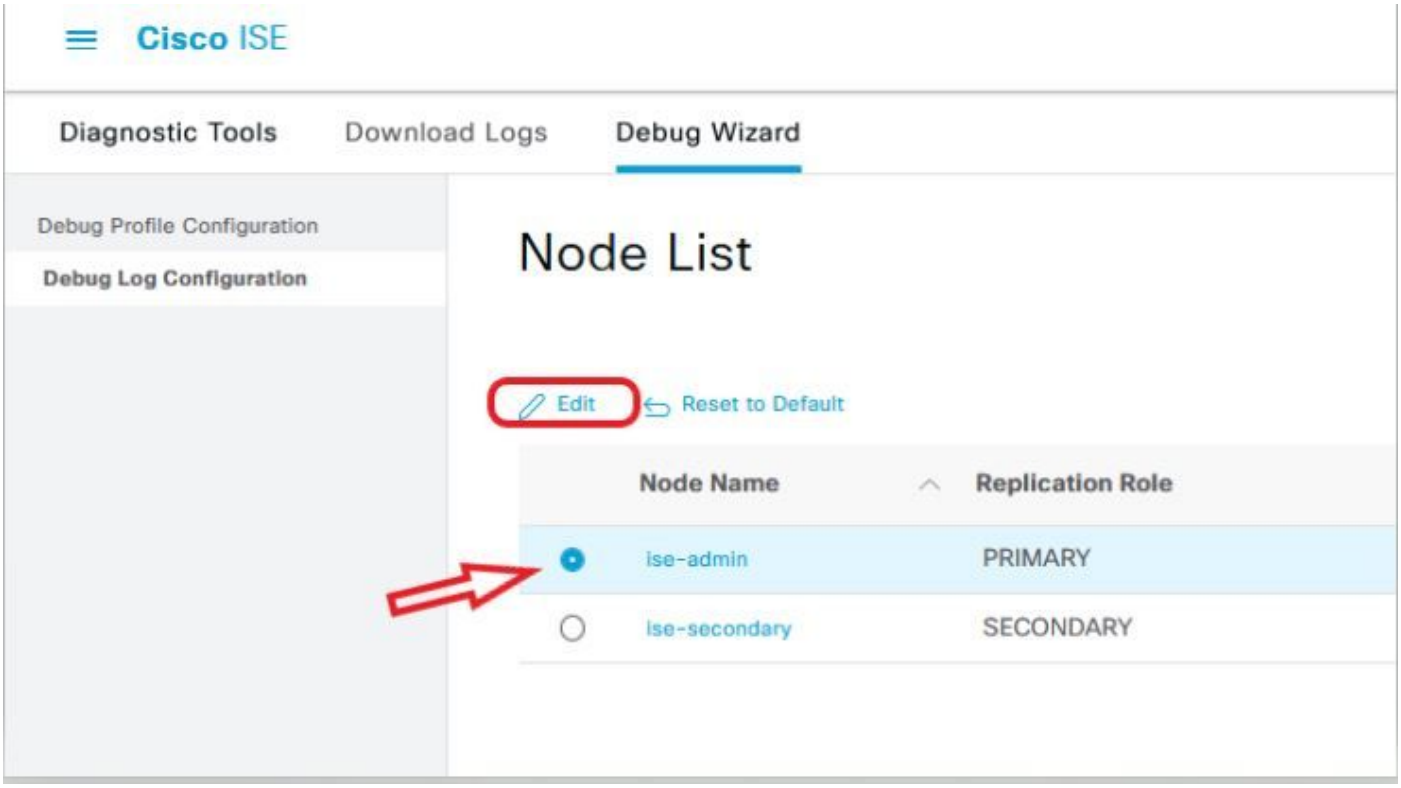
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Debugs inschakelen

Om het oplossen van problemen te starten moet u eerst de debugs inschakelen zoals hieronder beschreven.

Navigeer naar **Operations > Probleemoplossing > Wizard Debug > Configuratie debug log.** Selecteer de Primaire beheerknooppunt en klik op **Bewerken** zoals in de volgende afbeelding.



- Stel de volgende componenten op **DEBUG-**niveau in.

Naam van component	Logniveau	Logbestandsnaam
deuropening	DEBUGGEN	guest.log
opensaml	DEBUGGEN	ise-psc.log
klein	DEBUGGEN	ise-psc.log

> **Opmerking:** Wanneer u klaar bent met probleemoplossing, vergeet niet de debugs opnieuw in te stellen door de node te selecteren en klik op "Terugzetten op standaard".

De logbestanden downloaden

Nadat het probleem is gereproduceerd, dient u de benodigde logbestanden te verkrijgen.

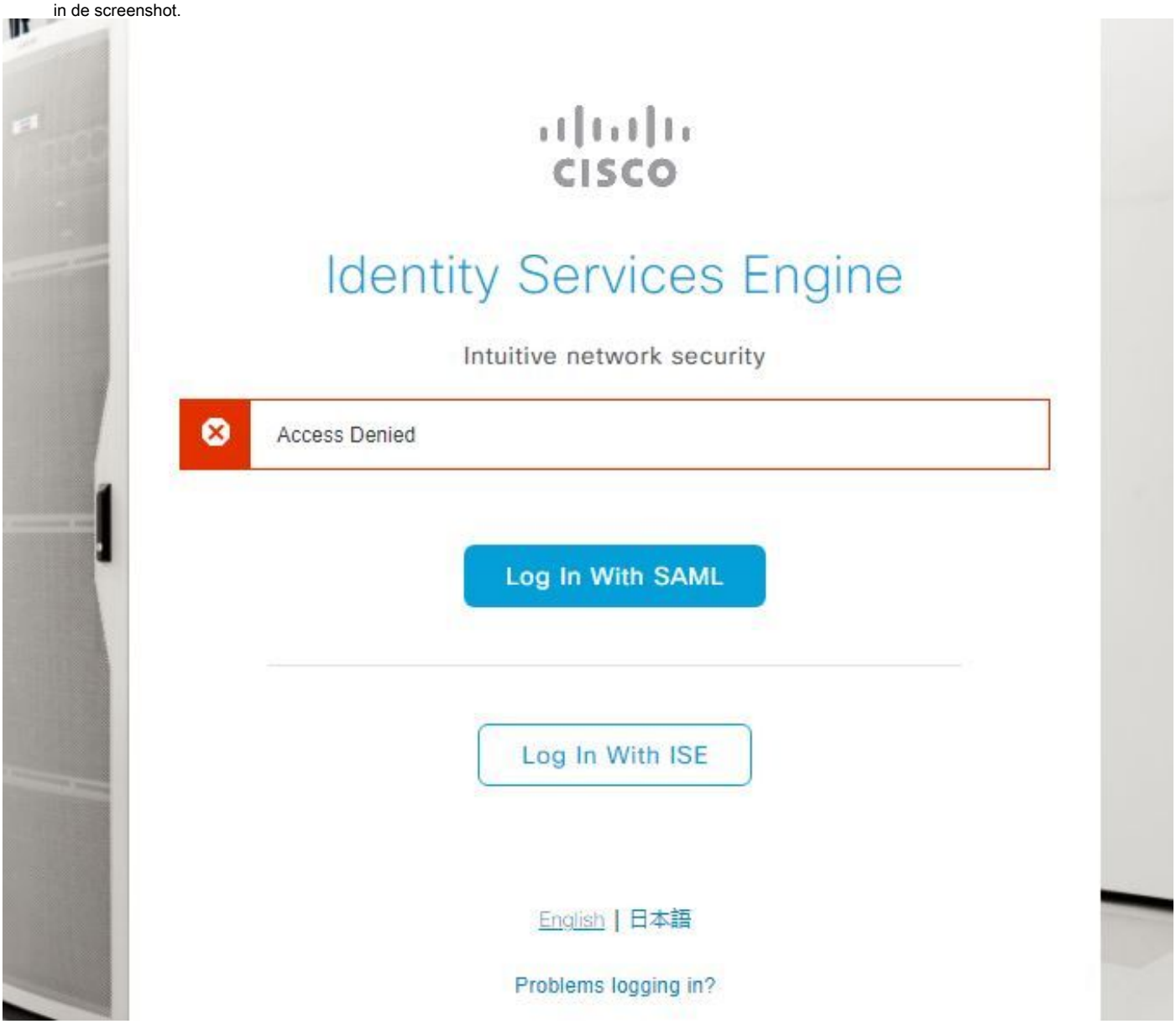
Stap 1. Navigeer naar Operations > Probleemoplossing > Logbestanden downloaden. Selecteer het primaire beheerknooppunt onder 'Applicatie knooppunt lijst' > Debug logs

Stap 2. Zoek en vouw gast- en ISE-psc-oudermappen uit

Stap 3. Downloaden guest.log en ise-psc.log bestanden.

Probleem 1a: Toegang geweigerd

- Nadat u uw op SAML gebaseerde Admin-aanmelding hebt geconfigureerd,
  - Selecteer Inloggen met SAML.
  - Omleiding naar IDp inlogpagina werk zoals verwacht
  - Verificatie is een succes per SAML/IDP-respons
  - IdP verzend groepsattributen en u kunt de zelfde groep/de objecten ID zien die in ISE wordt gevormd.
  - Vervolgens, terwijl ISE probeert om haar beleid te analyseren, wordt er een uitzondering geworpen die een "Access Denied"-bericht veroorzaakt, zoals in de screenshot.



Logs in ise-psc.log

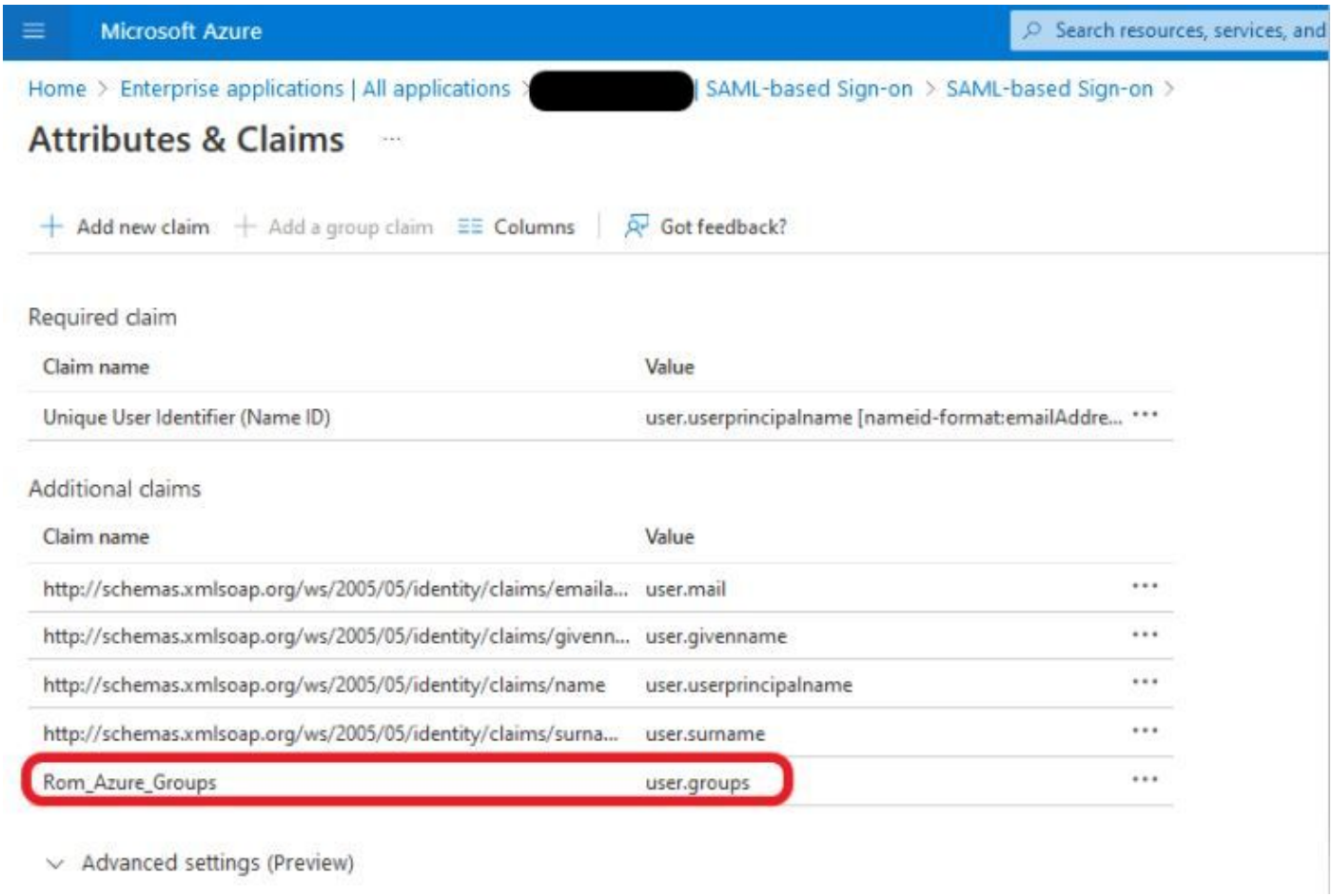
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true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

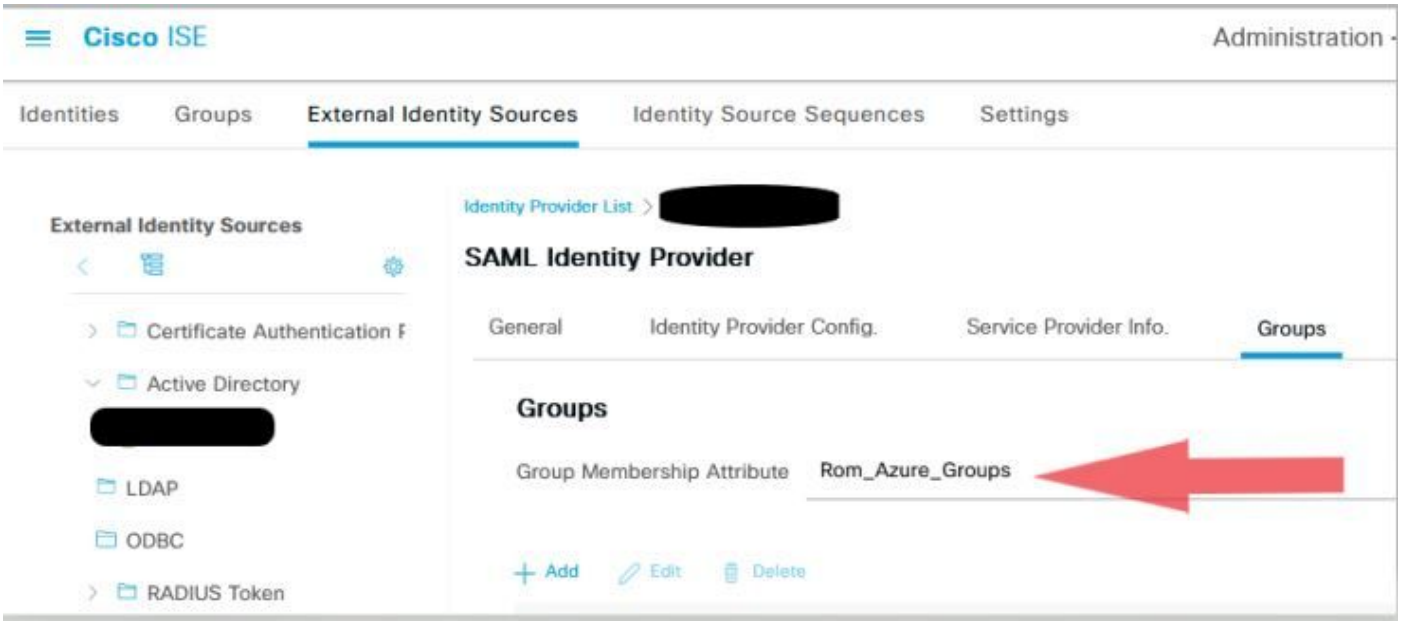
Oorzaak/oplossing

Zorg ervoor dat de naam van de groepsclaim in de IDp-configuraties hetzelfde is als wat in ISE is geconfigureerd.

De volgende screenshot werd genomen van Azure kant.



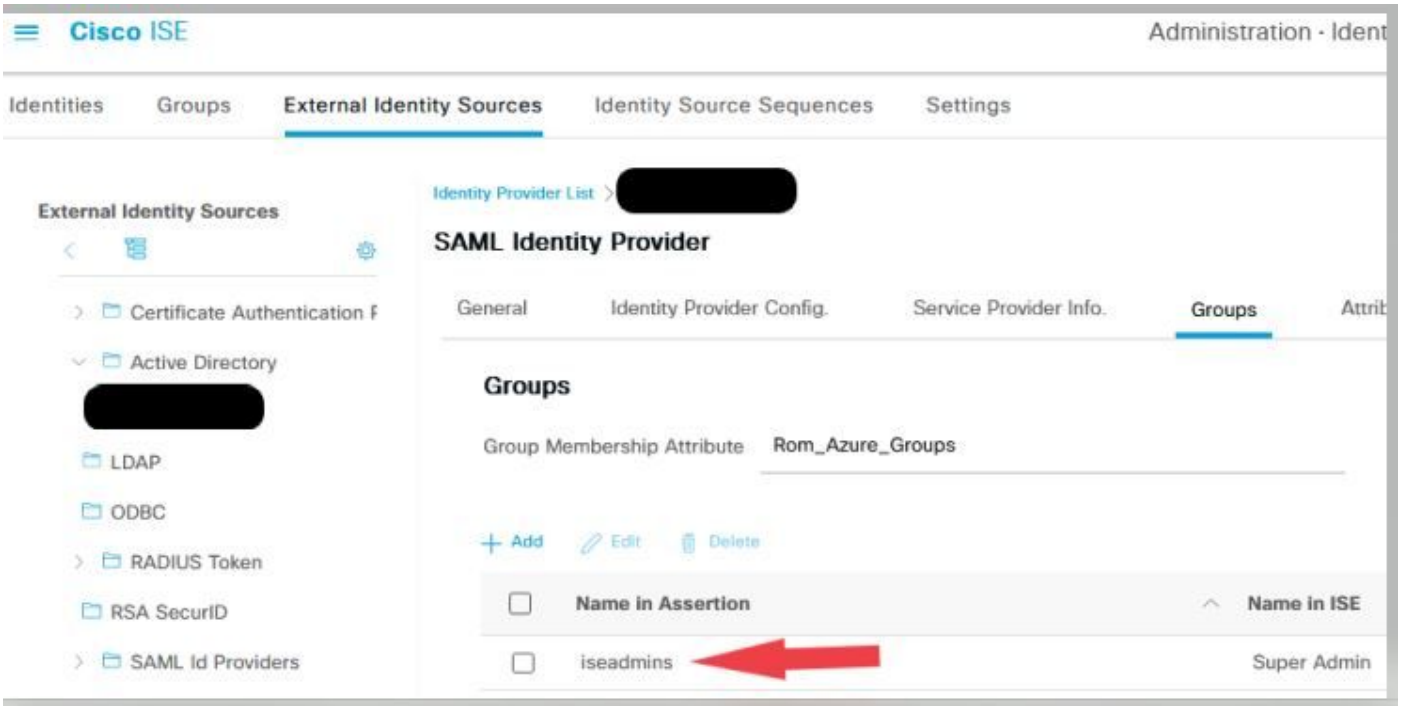
Screenshot van ISE Side.



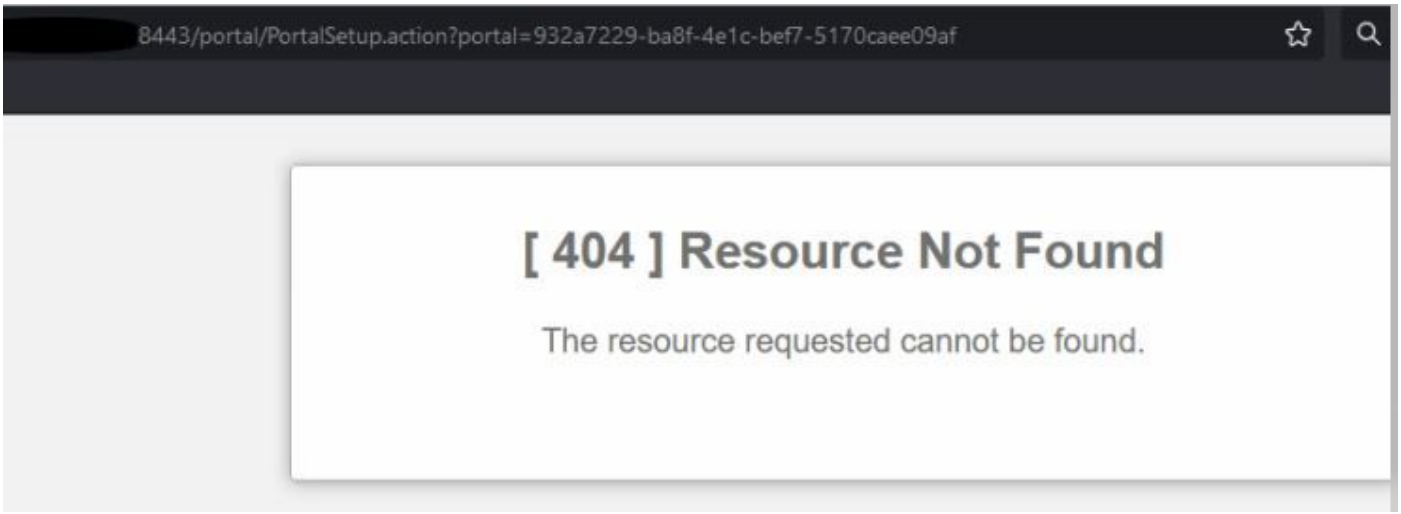
Probleem 1b: Meervoudige groepen in SAML-respons (toegang geweigerd)

Als de vorige oplossing het probleem niet oplost, zorg er dan voor dat de gebruiker geen lid is van meer dan één groep. Als dit probleem zich voordoet, moet u Cisco bug-id CSC17470 hebben aangetroffen, waar ISE alleen de eerste waarde (groepsnaam / ID) in de lijst met SAML-respons overeenkomt. Deze bug is opgelost in 3.1 P3

Per de eerder gegeven IdP-respons moet ISE-mapping voor de groep **iseadmins** worden geconfigureerd voor aanmelding om succesvol te zijn.



Probleem 2: 404 Resource niet gevonden



Je ziet fout 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.
```

Oorzaak/oplossing

Dit probleem wordt geobserveerd nadat de eerste ID-winkel wordt gemaakt.

Probeer de volgende oplossing in dezelfde volgorde:

Stap 1. Maak een nieuwe SAML IDp in uw ISE (verwijder de huidige nog niet.)

Stap 2. Ga naar de pagina voor beheerderstoegang en wijs uw beheerderstoegang toe aan deze nieuwe IDp.

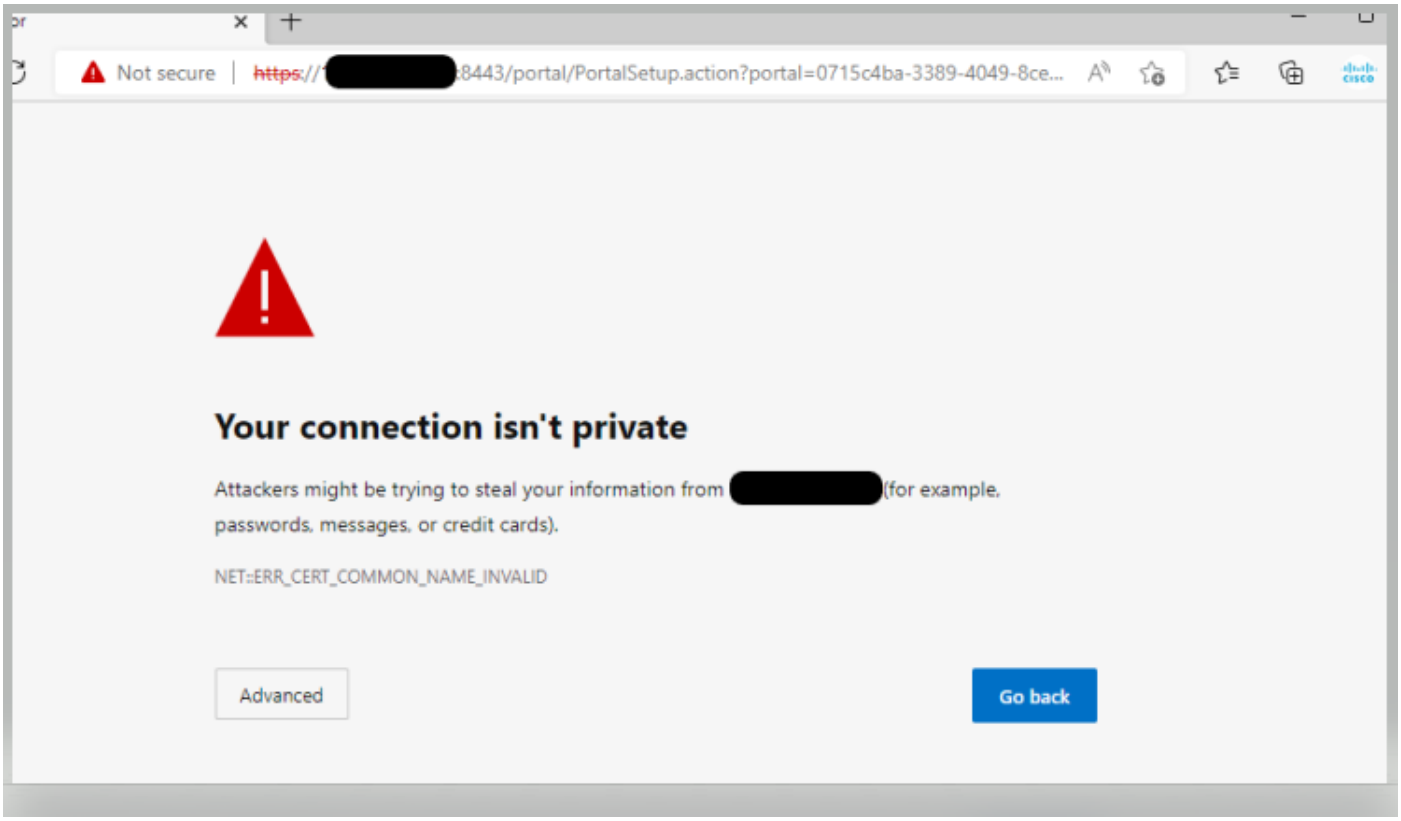
Stap 3. Verwijder de oude IDp op de pagina Externe Identity Providers.

Stap 4. Importeer de huidige IDp-metagegevens in de nieuwe IDp die in stap 1 is gemaakt en voer alle nodige groepstoewijzingen uit.

Stap 5. Probeer nu SAML-aanmelding. het zal werken.

Probleem 3: Waarschuwing certificaat

In een multi-node-implementatie, wanneer u op "Inloggen met SAML" klikt, kunt u niet-vertrouwde certificaatwaarschuwing in de browser zien



Oorzaak/oplossing

In sommige gevallen wordt u door pPAN omgeleid naar de actieve PSN IP en niet naar FQDN. Dit veroorzaakt een certificaatwaarschuwing bij sommige PKI-implementatie, als er geen IP-adres in het SAN-veld is.

De tijdelijke oplossing is om IP toe te voegen aan het SAN-veld van het certificaat.

Cisco bug-id CSCvz89415. Dit wordt opgelost in 3.1p1

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.