Troubleshoot ISE 3.1 GUI Log in with SAML SSO

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Enable Debugs

Download the Logs

- Problem 1a - "Access denied"
  - Cause
  - Solution
- Problem 1b - Multiple Groups in SAML Response ("Access denied")
- Problem 2 - "404 Resource not found"
  - Cause
  - Solution
- Problem 3 - Certificate Warning
  - Cause
  - Solution

Introduction

This document describes most issues that have been observed in ISE 3.1 with SAML GUI log-in.

Prerequisites

Through the use of the SAML 2.0 standard, SAML-based admin log-in adds Single sign-on (SSO) capability to ISE. You can use any Identity Provider (IdP) such as Azure, Okta, PingOne, DUO Gateway or any IdP that implements SAML 2.0.

Requirements

Cisco recommends that you have knowledge of these topics:

1. Cisco ISE 3.1 or higher
2. Understand the basics of SAML SSO setups.

Refer to the ISE 3.1 admin guide for SAML configuration and ISE Admin Login Flow via SAML with Azure AD for more details on the configuration and flow.

Note: You must be familiar with your Identity Provider service, and ensure that it is up and running.

Components Used

The information in this document is based on these software and hardware versions:

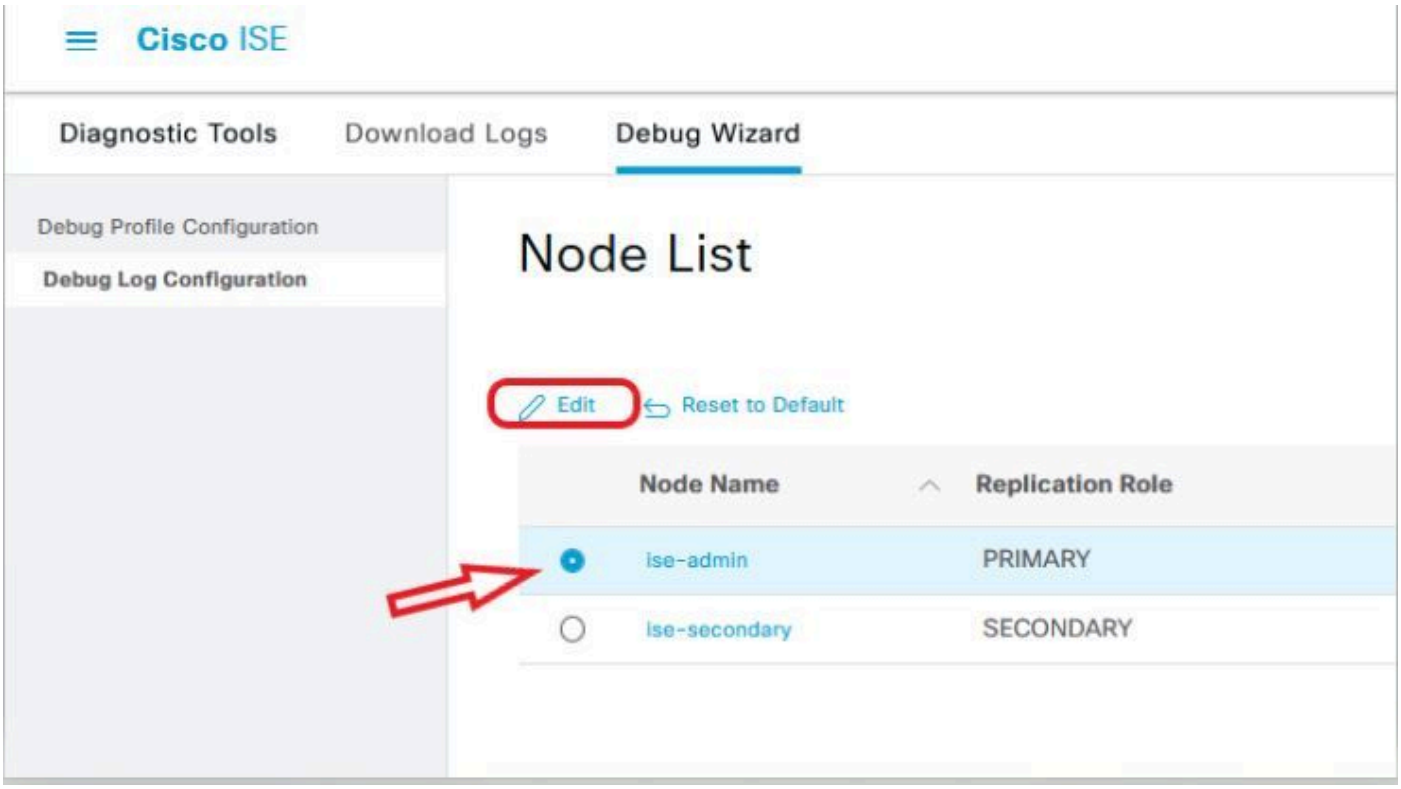
- ISE version 3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Enable Debugs

To start troubleshooting, you must first enable the debugs as described below.

Navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**. Select the Primary admin node and click on **Edit** as shown in the next image.



- Set the next Components to DEBUG level.

Component Name	Log Level	Log Filename
portal	DEBUG	guest.log
opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Note: When you are done troubleshooting, remember to reset the debugs by selecting the node and click **Reset to Default**.

Download the Logs

Once the issue has been reproduced, you must obtain the necessary log files.

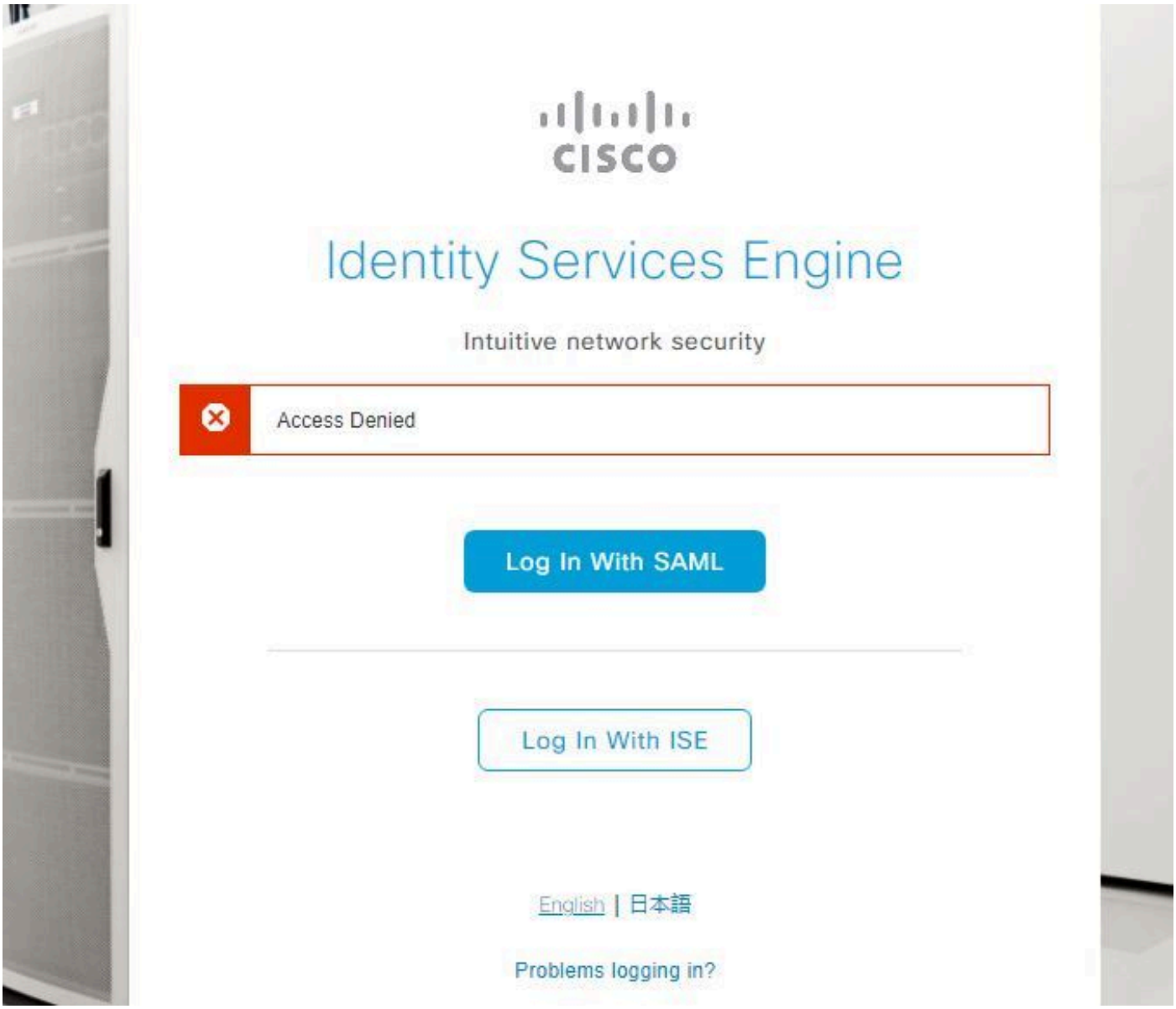
Step 1. Navigate to **Operations > Troubleshoot > Download logs**. Select the primary admin node under **Appliance node list > Debug Logs**.

Step 2. Locate and expand guest and ise-psc parent folders

Step 3. Download guest.log and ise-psc.log files.

Problem 1a - "Access denied"

- After you have configured your SAML-Based Admin Login.
- Select **Log in With SAML**.
- Redirection to IdP log in page work as expected.
- Authentication is success per SAML/IdP response.
- IdP send group attribute and you can see the same group/object ID configured in ISE.
- Then, as ISE tries to analyze its policies, it throws an exception that causes an "Access Denied" message, as shown in the 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.SAML

                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.SAML
2021-09-27 17:16:18,225 DEBUG  [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAML
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
```

```
2021-09-27 17:16:18,402 ERROR  [admin-http-pool5][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::

java.lang.NullPointerException

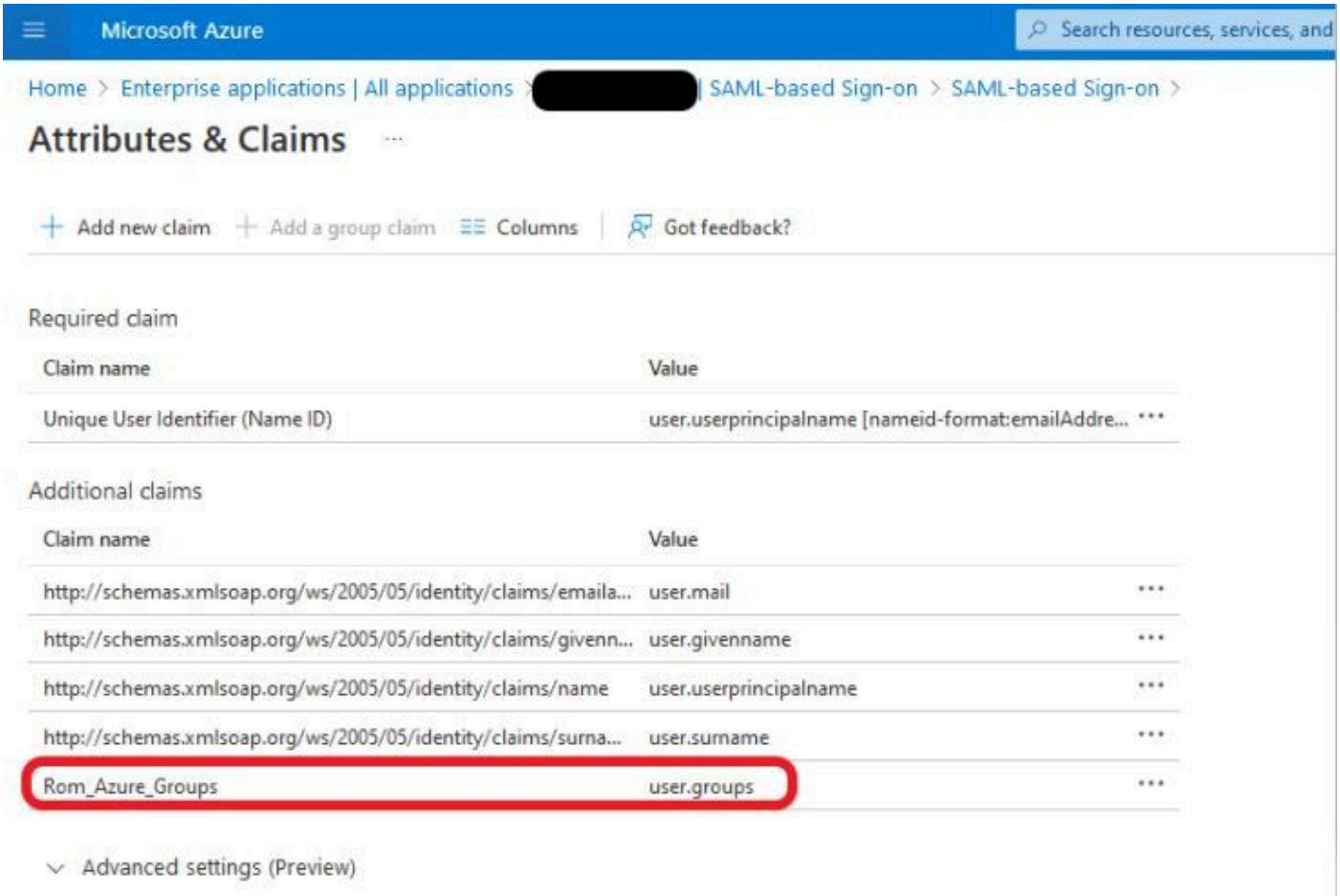
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login A
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login A
2021-09-27 17:16:18,402 ERROR  [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- Can't save
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginActionResultHandler -:::
```

Cause

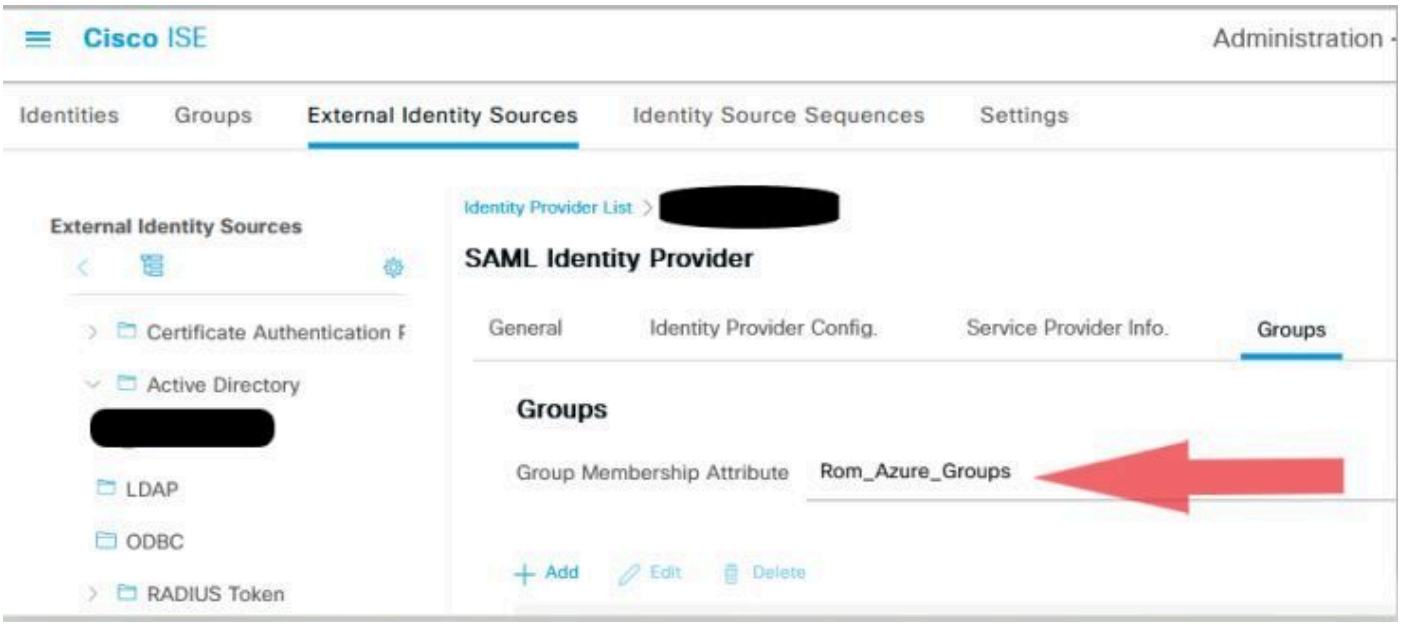
Ensure the group claim name in IdP configs is the same as what is configured in ISE.

Solution

The next screenshot was taken from Azure side:



Screenshot from the ISE side:

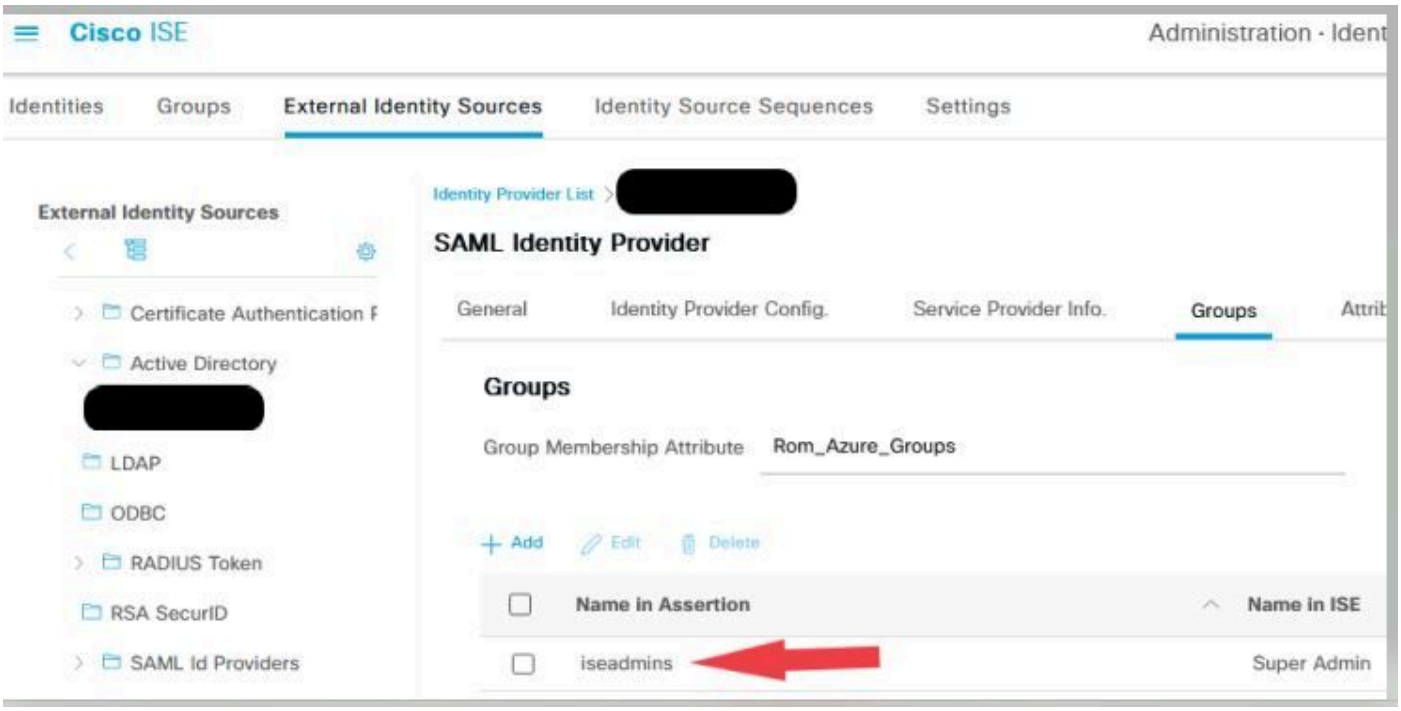


Problem 1b - Multiple Groups in SAML Response ("Access denied")

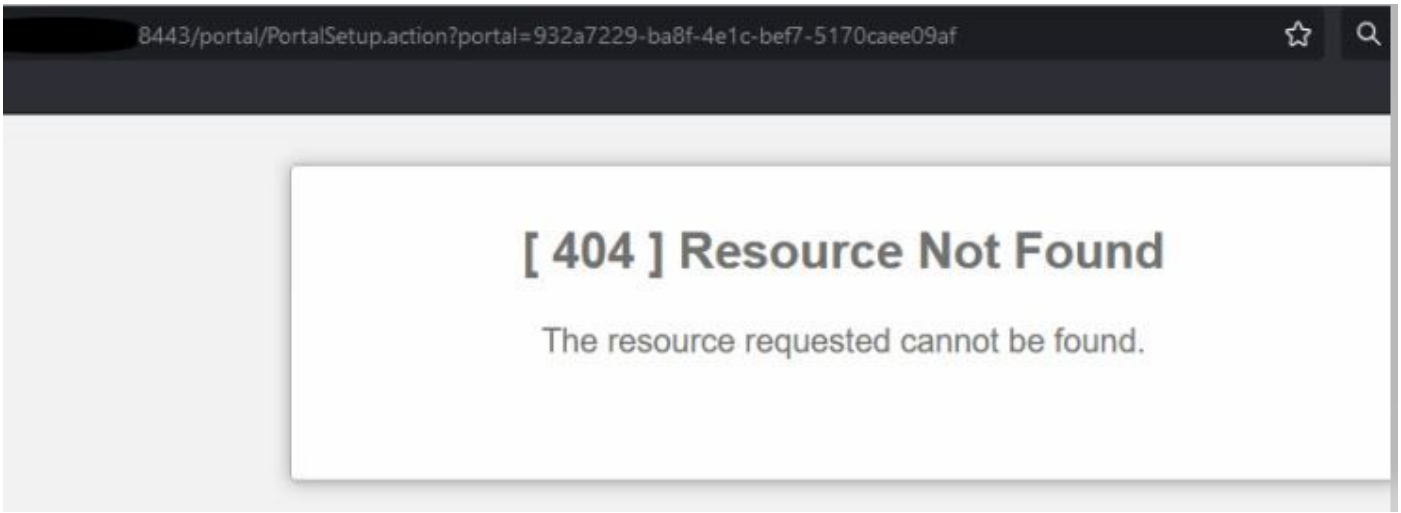
If the previous fix does not resolve the issue, make sure the user is not a member of more than one Group. If this is the case, you must have encountered Cisco bug ID CSCwa17470 where ISE only match the first value (group name / ID) in the list from SAML response. This bug is resolved in 3.1 P3.

```
<samlp:Response ID="######"
                Version="2.0"
      <Attribute Name="Groups">
       <AttributeValue>iseadmins </AttributeValue>
      <AttributeValue>Sysadmins</AttributeValue>
      <AttributeValue>domain admins</AttributeValue>
       <AttributeValue>change-esc</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

Per the IdP response given previously, ISE mapping for the iseadmins group must be configured for log-in to be successful.



Problem 2 - "404 Resource not found"



You see error in guest.log:

<#root>

```
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=PROC
```

Cause

This issue is observed after creates the first ID store only.

Solution

To resolve this, try the next in the same order:

Step 1. Create a new SAML IdP in your ISE (Do not remove the current one just yet.).

Step 2. Go to admin access page and assign your admin access to this new IdP.

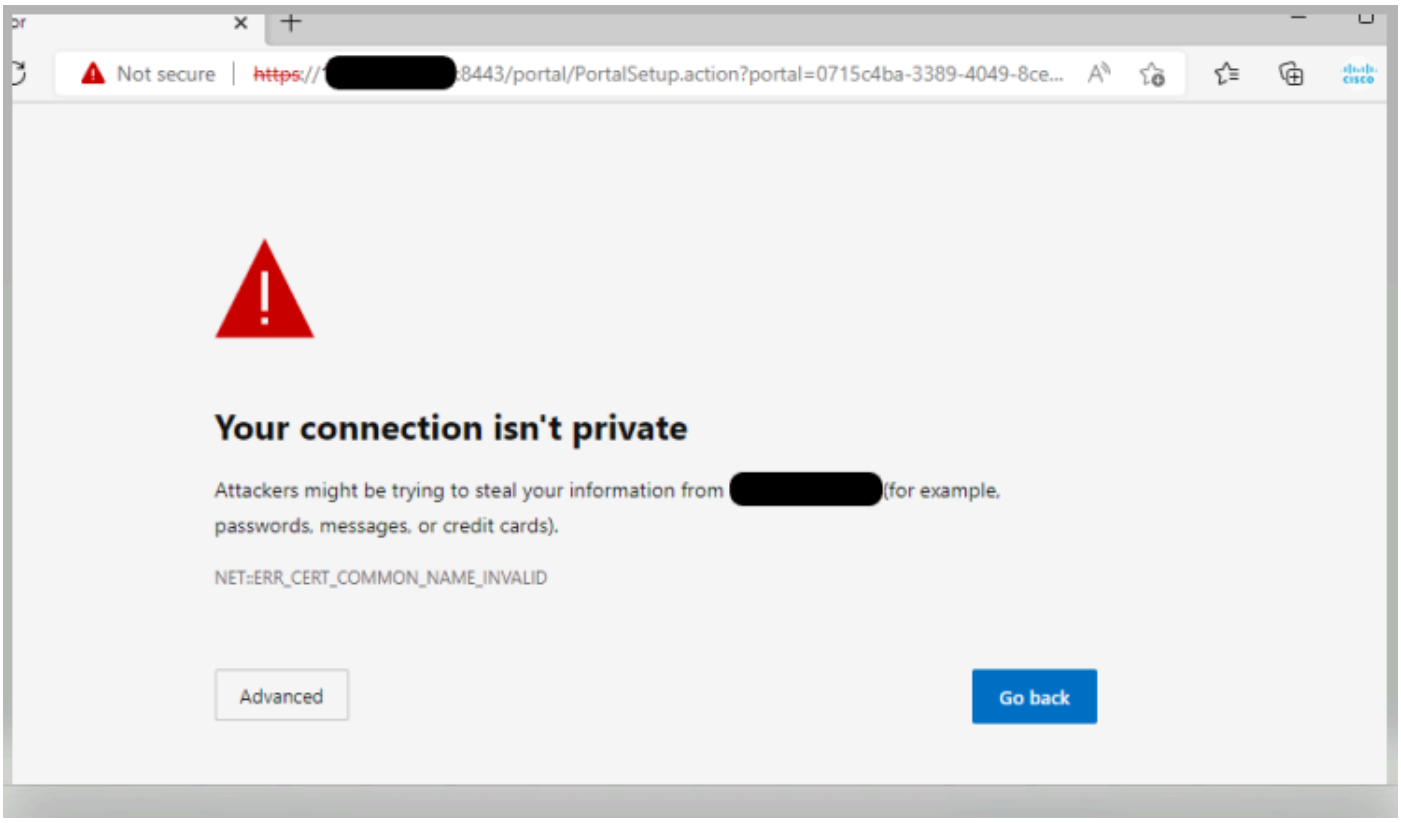
Step 3. Delete the old IdP in External Identity Providers page.

Step 4. Import the current IdP metadata into the new IdP created in step 1 and perform any necessary group mappings.

Step 5. Now try SAML log in and ensure it works.

Problem 3 - Certificate Warning

In a multi-node deployment, when you click on **Log In with SAML**, you can see the un-trusted certificate warning in the browser:



Cause

In some cases, pPAN redirects you to the Active PSNs IP, not FQDN. This cause a certificate warning in some PKI deployment, if there is no IP address in the SAN field.

Solution

The workaround is to add IP in the SAN field of the certificate.

Cisco bug ID CSCvz89415. This is resolved in 3.1p1.