# 使用SAML SSO排除ISE 3.1 GUI登录故障

## 目录


简介

先决条件

- 要求
- 使用的组件

启用调试

下载日志

- 问题1a — “Access denied”
  - 原因
  - 解决方案
- 问题1b - SAML响应中的多个组（“访问被拒绝”）
- 问题2 — “404资源未找到”
  - 原因
  - 解决方案
- 问题3 — 证书警告
  - 原因
  - 解决方案


## 简介

本文档介绍在使用SAML GUI登录的ISE 3.1中观察到的大多数问题。

## 先决条件

通过使用SAML 2.0标准，基于SAML的管理员登录向ISE添加单点登录(SSO)功能。您可以使用任何身份提供程序(IdP)，例如Azure、Okta、PingOne、DUO Gateway或实施SAML 2.0的任何IdP。

### 要求

Cisco 建议您了解以下主题：

1. Cisco ISE 3.1或更高版本
2. 了解SAML SSO设置的基础知识。

有关配置和流程的详细信息，请参阅ISE 3.1管理员指南，了解SAML配置和通过SAML使用Azure AD的ISE管理员登录流程。

注意：您必须熟悉身份提供程序服务，并确保其已启动并正在运行。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

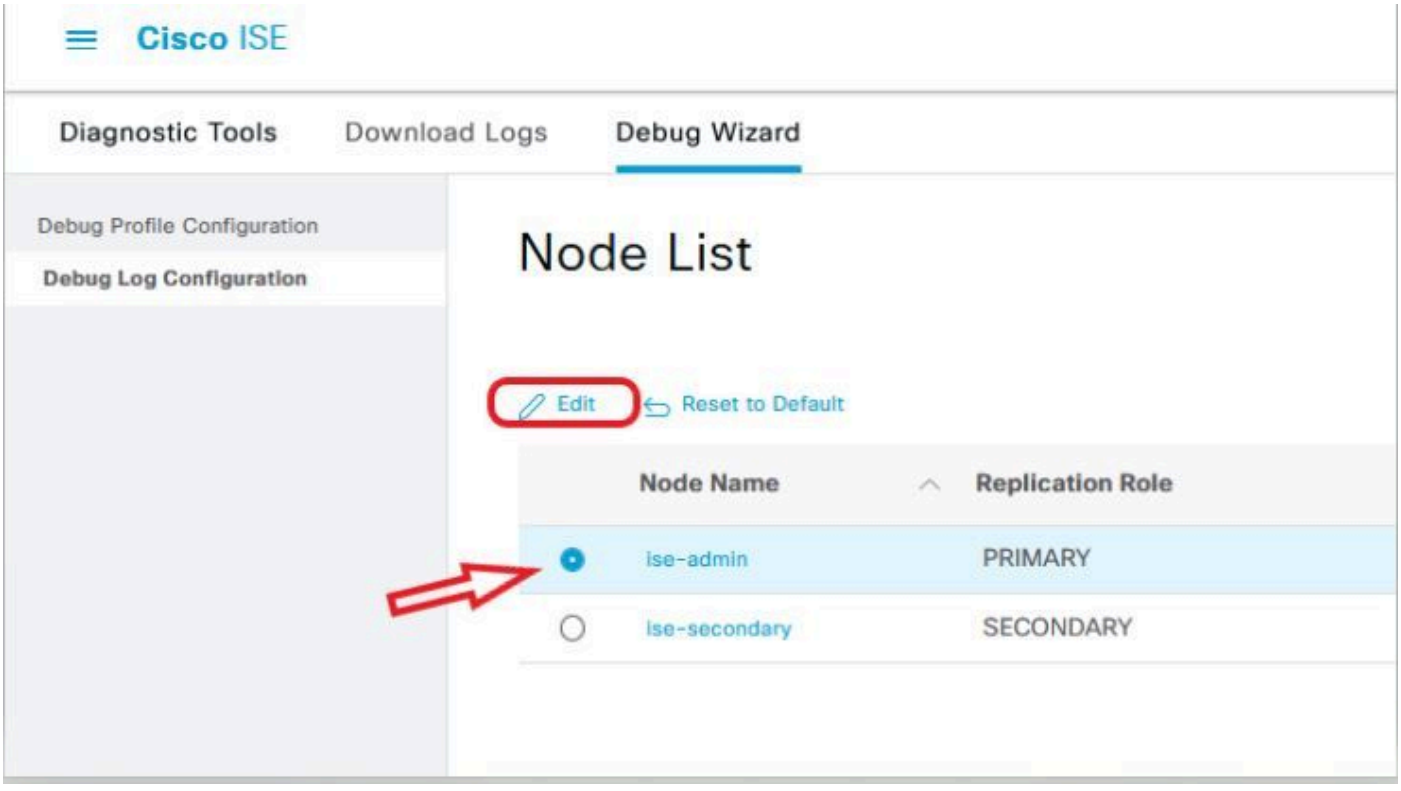
- ISE版本3.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

### 启用调试

要开始故障排除，必须首先启用调试，如下所述。

导航到操作>故障排除>调试向导>调试日志配置。选择Primary admin节点，然后单击Edit，如下图所示。



- 将下一个组件设置为DEBUG级别。

| 组件名称 | 日志级别 | 日志文件名 |
| --- | --- | --- |
| 门户 | 调试 | guest.log |
| opensaml | 调试 | ise-psc.log |
| saml | 调试 | ise-psc.log |

注意：完成故障排除后，请记住通过选择节点并点击Reset to Default来重置调试。

下载日志

重现问题后，您必须获取必要的日志文件。

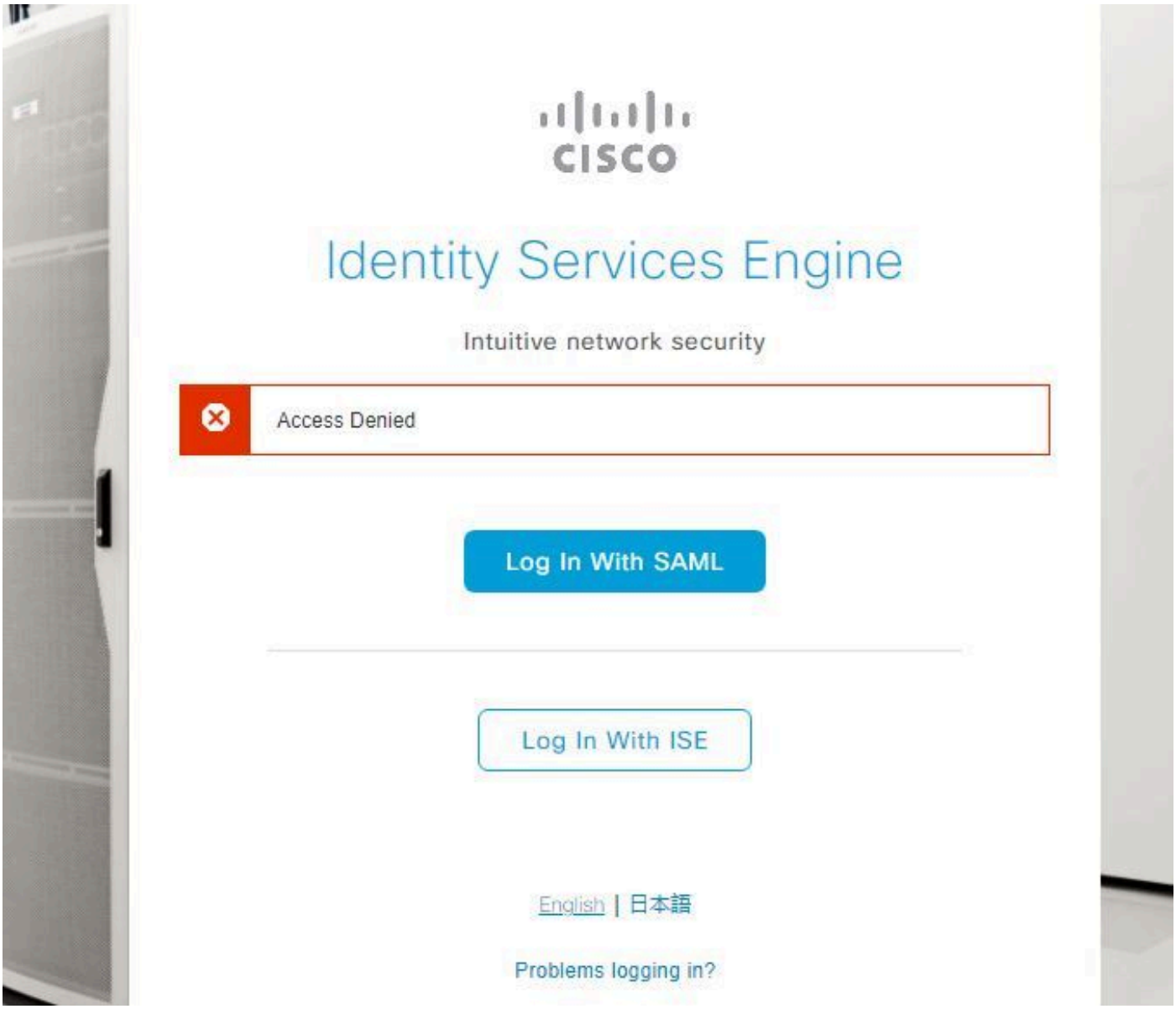
步骤1.导航到操作>故障排除>下载日志。在Appliance node list > Debug Logs下选择主管理节点。

步骤2.查找并展开访客和ise-psc父文件夹

步骤3.下载guest.log和ise-psc.log文件。

问题1a — “Access denied”

- 配置基于SAML的管理员登录后。
- 选择Log in With SAML。
- 重定向到IdP登录页面的工作情况如预期所示。
- 根据SAML/IdP响应，身份验证成功。
- IdP发送组属性，您可以看到在ISE中配置的相同组/对象ID。
- 然后，当ISE尝试分析其策略时，它会抛出导致“Access Denied”消息的异常，如屏幕截图所示。




登录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

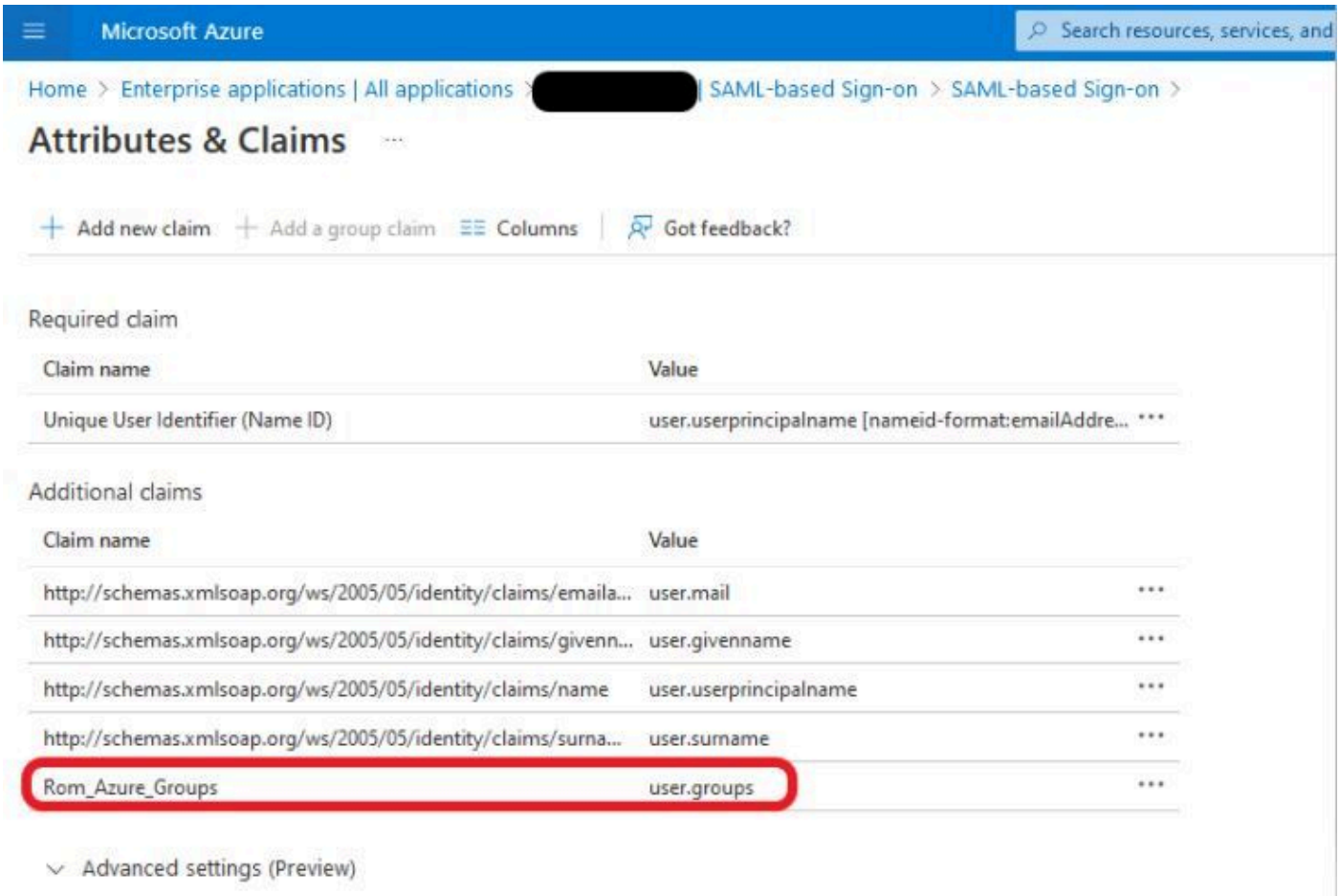
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login A
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login A
2021-09-27 17:16:18,402 ERROR  [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::-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

## 原因

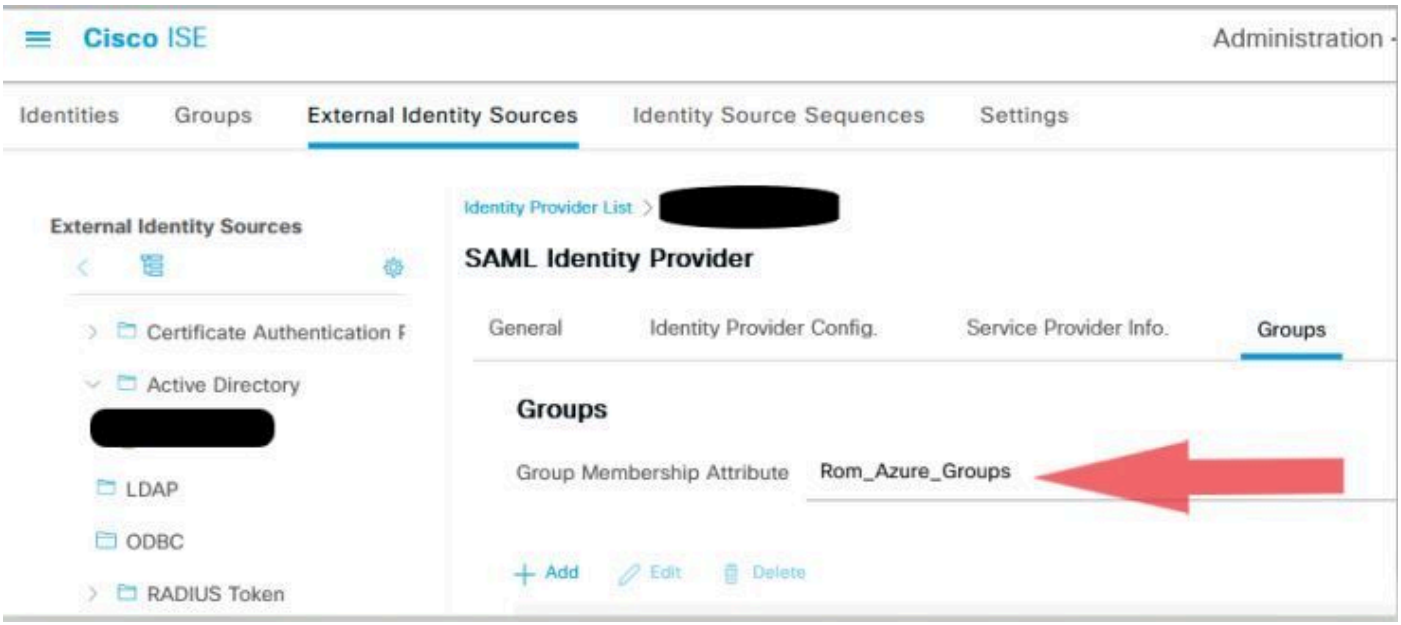
确保IdP配置中的组声明名称与ISE中配置的名称相同。

## 解决方案

下一个屏幕截图取自Azure端：




ISE端的屏幕截图：




问题1b - SAML响应中的多个组（“访问被拒绝”）

如果之前的修复程序不能解决问题，请确保用户不是多个组的成员。如果出现这种情况，您必须遇到Cisco Bug ID CSCwa17470，其中ISE仅与SAML响应列表中的第一个值（组名称/ID）匹配。此Bug已在3.1 P3中解决。

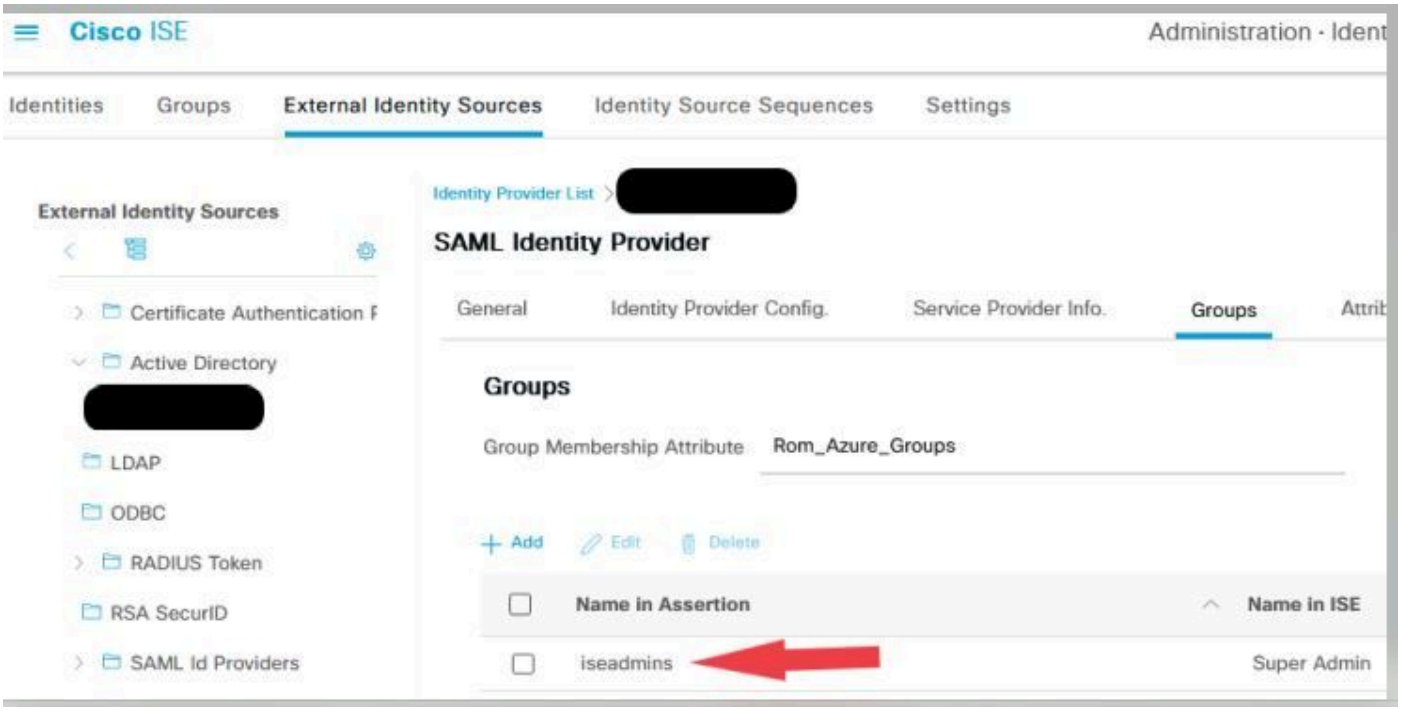
```
iseadmins
```

```
Sysadmins
```

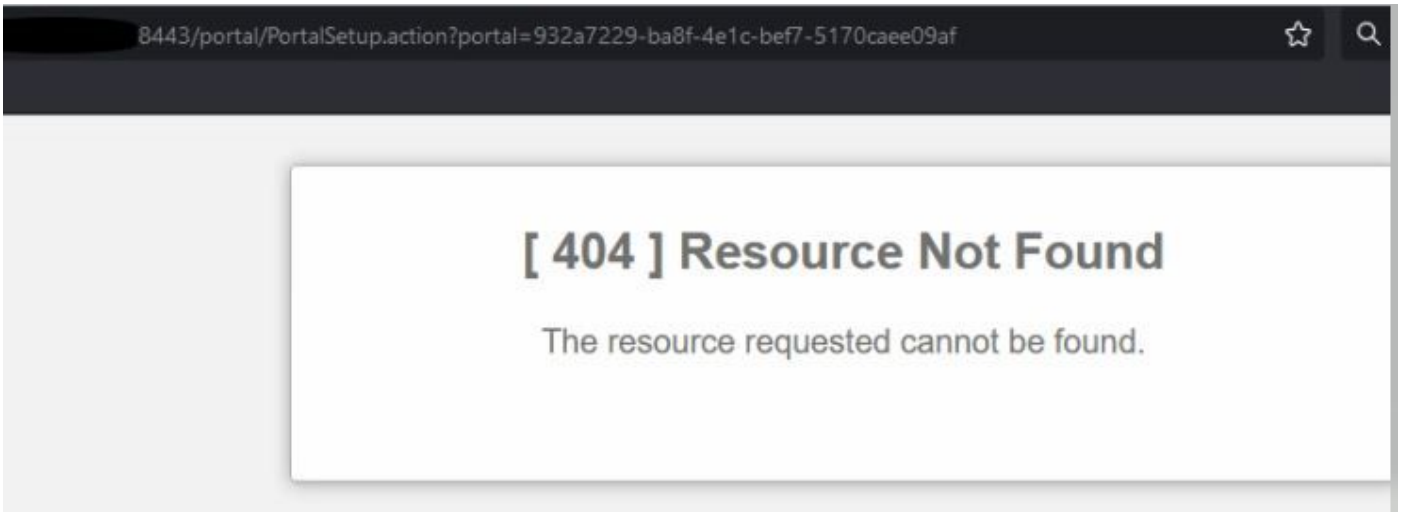
```
domain admins
```

```
change-esc
```

根据之前给定的IdP响应，必须配置iseadmins组的ISE映射才能成功登录。




问题2 — “404资源未找到”



您在guest.log中看到错误：

<#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
```

原因

仅在创建第一个ID存储后发现此问题。

解决方案

要解决此问题，请按相同顺序尝试下一步：

步骤1.在ISE中创建新的SAML IdP（暂时不要删除当前的SAML IdP。）

步骤2.转到管理员访问权限页面，并为此新IdP分配管理员访问权限。

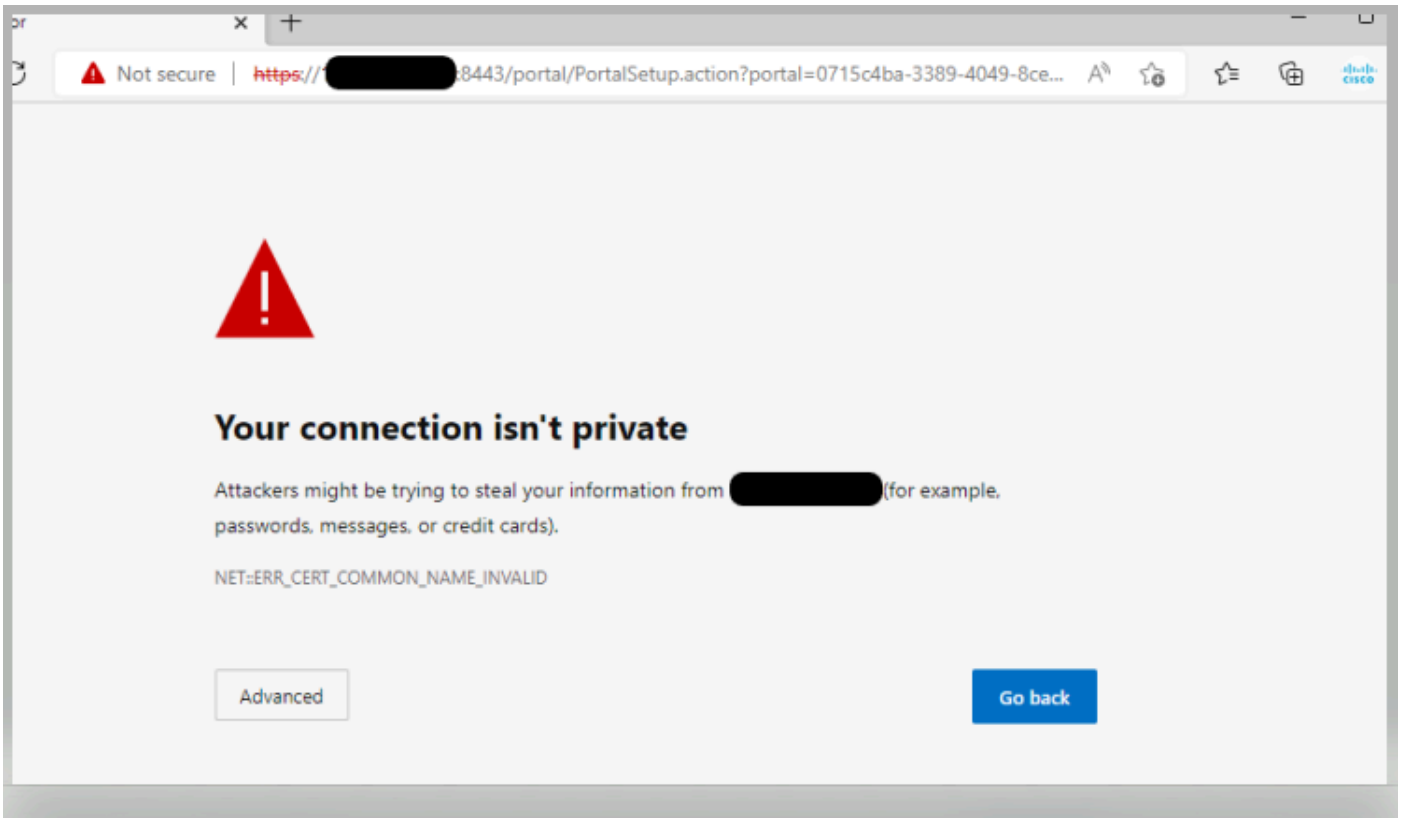
步骤3.删除External Identity Providers页中的旧IdP。

步骤4.将当前IdP元数据导入到步骤1中创建的新IdP中，并执行所有必要的组映射。

步骤5.现在尝试SAML登录并确保其正常工作。

问题3 — 证书警告

在多节点部署中，当您点击使用SAML登录时，可以在浏览器中看到不可信证书警告：




原因

在某些情况下，pPAN会将您重定向到活动PSN IP，而不是FQDN。如果SAN字段中没有IP地址，这会在某些PKI部署中引发证书警告。

解决方案

解决方法是在证书的SAN字段中添加IP。

Cisco Bug ID CSCvz89415。此问题已在3.1p1中解决。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。