

Solucionar problemas de login da GUI do ISE 3.1 com o SAML SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Ativar depurações](#)

[Fazer download dos logs](#)

[Problema 1a: Acesso negado](#)

[Causa/solução](#)

[Problema 1b: Vários grupos na resposta SAML \(acesso negado\)](#)

[Problema 2: 404 Recurso não encontrado](#)

[Causa/solução](#)

[Problema 3: Aviso de certificado](#)

[Causa/solução](#)

Introduction

Este documento descreve a maioria dos problemas que foram observados no ISE 3.1 com o login da GUI SAML. Através do uso do padrão SAML 2.0, o login do administrador baseado em SAML adiciona o recurso de login único (SSO) ao ISE. Você pode usar qualquer Identity Provider (IdP), como Azure, Okta, PingOne, DUO Gateway ou qualquer IdP que implemente SAML 2.0.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

1. Cisco ISE 3.1 ou posterior
2. Entender os fundamentos das configurações de SSO SAML

Consulte o [guia do administrador do ISE 3.1 para configuração SAML](#) e [Fluxo de Logon do Administrador do ISE via SAML com Azure AD](#) para obter mais detalhes sobre a configuração e o fluxo.

Note: Você deve estar familiarizado com o serviço do Provedor de identidade e verificar se ele está funcionando.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

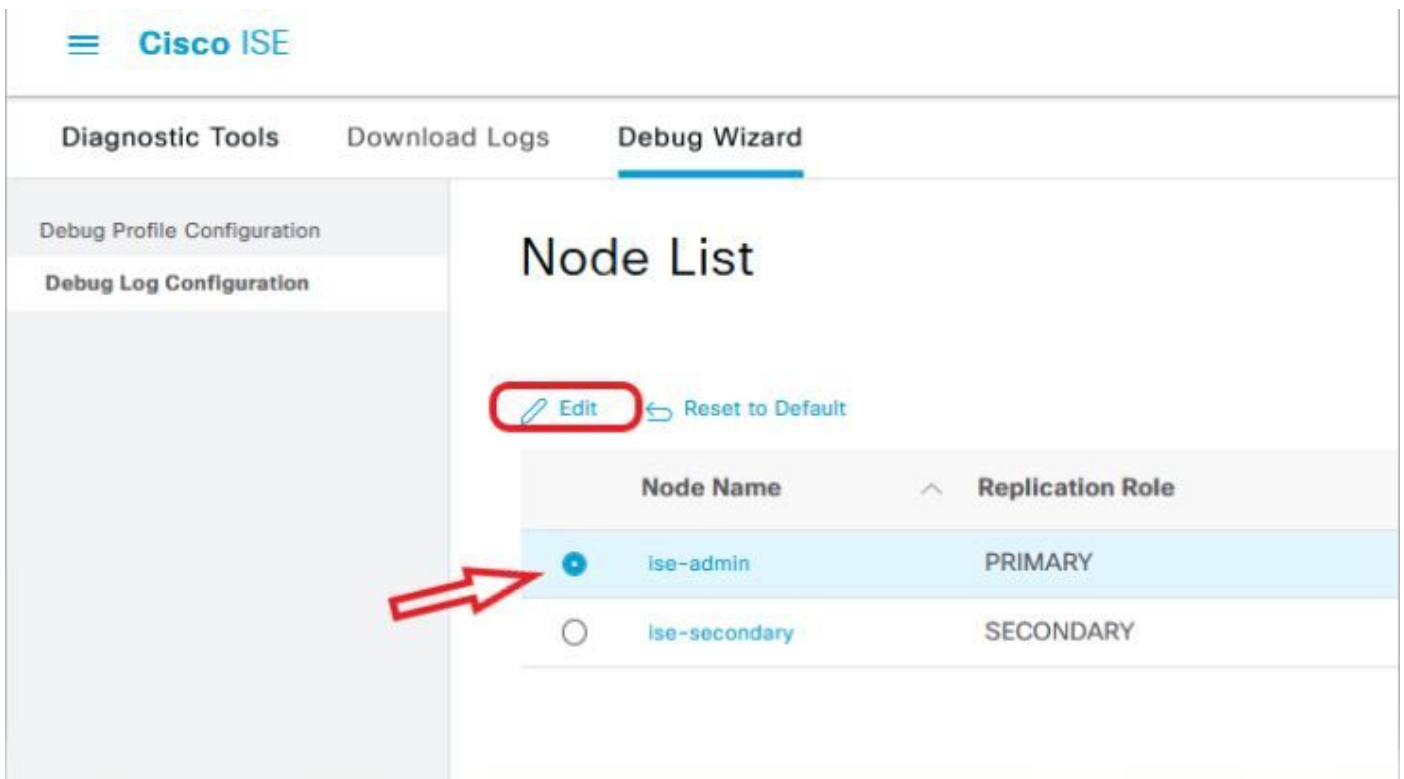
- ISE versão 3.1

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Ativar depurações

Para iniciar a solução de problemas, você deve primeiro habilitar as depurações conforme descrito abaixo.

Navegue até **Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração**. Selecione o nó Primary admin e clique em **Edit** conforme mostrado na imagem a seguir.



- Defina os próximos componentes para o nível **DEBUG**.

Nome do componente	Nível de log	Nome do arquivo de log
portal	DEBUG	guest.log
opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Note: Quando terminar de solucionar problemas, lembre-se de redefinir as depurações selecionando o nó e clique em "Redefinir para padrão".

Fazer download dos logs

Depois que o problema for reproduzido, você deverá obter os arquivos de log necessários.

Etapa 1. Navegue até **Operations > Troubleshoot > Download logs**. Selecione o nó principal admin em 'Appliance node list' > **Debug Logs**

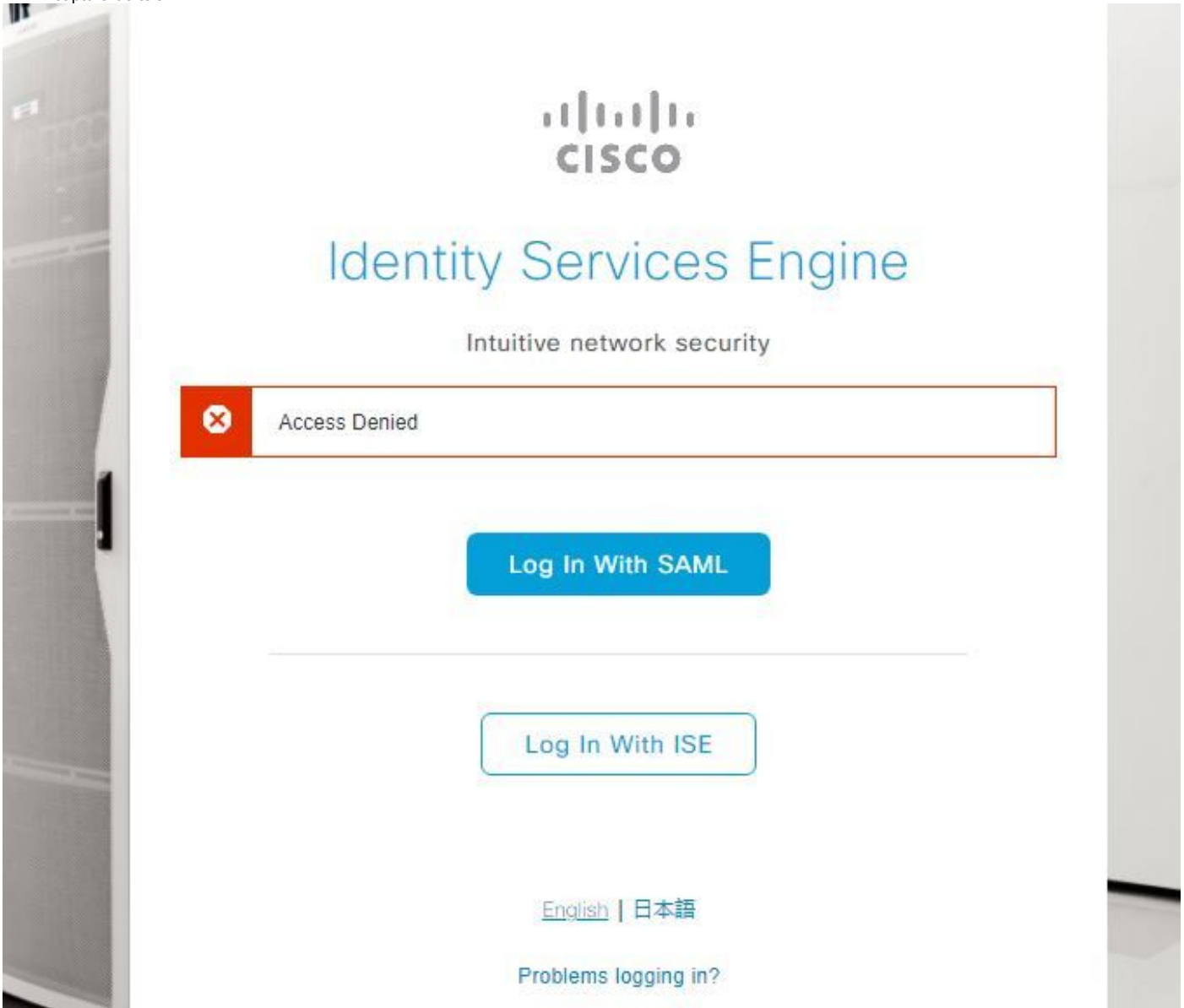
Etapa 2. Localizar e expandir as pastas pai **guest** e **ise-psc**

Etapa 3. Download **guest.log** e **ise-psc.log** arquivos.

Problema 1a: Acesso negado

- Depois de configurar seu login de administrador baseado em SAML,
- Selecione Fazer login com SAML.

- O redirecionamento para a página de logon do IdP funciona como esperado
- Autenticação bem-sucedida por resposta SAML/IdP
- O IdP envia o atributo de grupo e você pode ver o mesmo ID de grupo/objeto configurado no ISE.
- Em seguida, enquanto o ISE tenta analisar suas políticas, ele lança uma exceção que causa uma mensagem de "Acesso negado", como mostrado na captura de tela.



Efetua login 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
```

Causa/solução

Verifique se o nome da declaração de grupo nas configurações de IdP é o mesmo que o configurado no ISE.

A próxima captura de tela foi tirada do lado do Azure.

The screenshot shows the Microsoft Azure portal interface for configuring SAML-based Sign-on. The page title is "Attributes & Claims". Below the title, there are options to "Add new claim", "Add a group claim", "Columns", and "Got feedback?". The main content is divided into two sections: "Required claim" and "Additional claims".

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddre... ***

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila...	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn...	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surna...	user.surname ***
Rom_Azure_Groups	user.groups ***

Advanced settings (Preview)

Captura de tela do lado ISE.

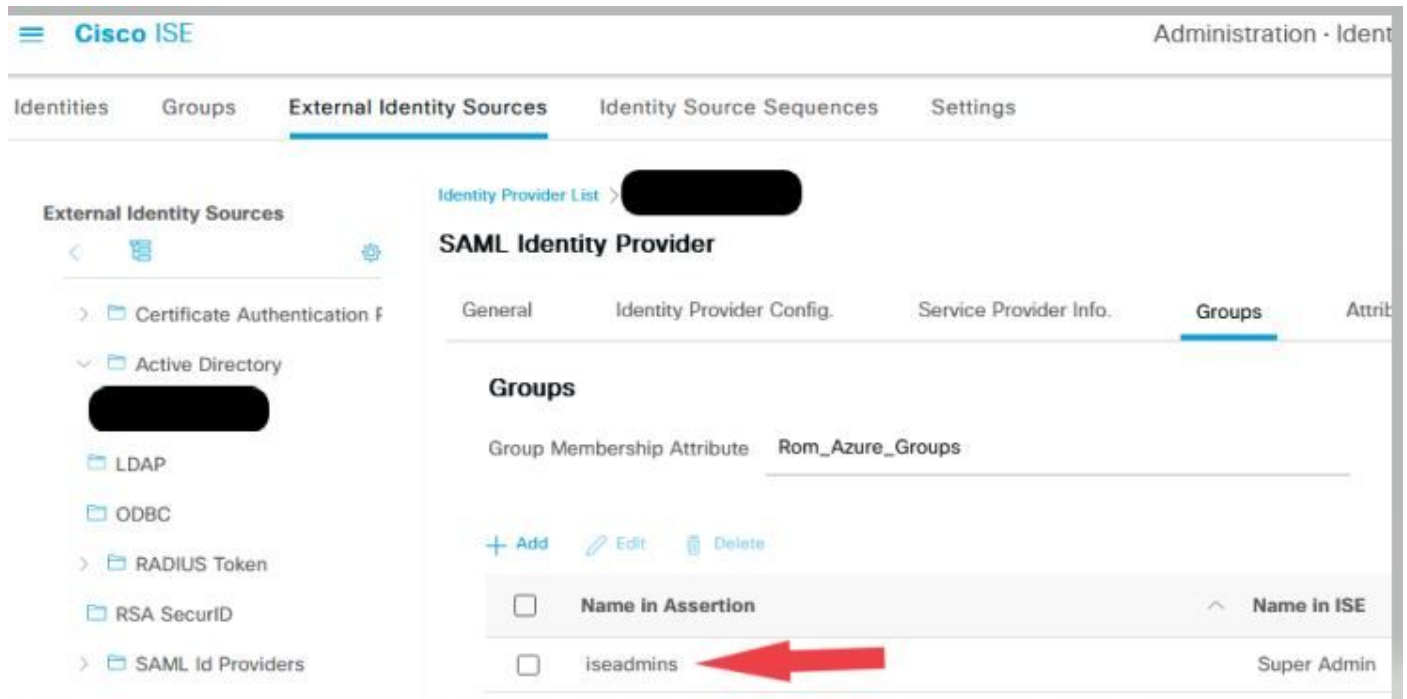
The screenshot shows the Cisco ISE Administration console. The navigation menu includes "Identities", "Groups", "External Identity Sources", "Identity Source Sequences", and "Settings". The "External Identity Sources" section is expanded, showing "Certificate Authentication F", "Active Directory", "LDAP", "ODBC", and "RADIUS Token". The "SAML Identity Provider" configuration page is displayed, with tabs for "General", "Identity Provider Config.", "Service Provider Info.", and "Groups". The "Groups" tab is selected, showing a table with "Group Membership Attribute" and "Rom_Azure_Groups". A red arrow points to the "Rom_Azure_Groups" value.

Group Membership Attribute	Value
	Rom_Azure_Groups

Problema 1b: Vários grupos na resposta SAML (acesso negado)

Se a correção anterior não resolver o problema, verifique se o usuário não é membro de mais de um grupo. Se esse for o caso, você deve ter encontrado o bug da Cisco ID [CSCwa17470](#) onde ISE corresponde apenas ao primeiro valor (nome/ID do grupo) na lista da resposta SAML. Este bug foi resolvido no 3.1 P3

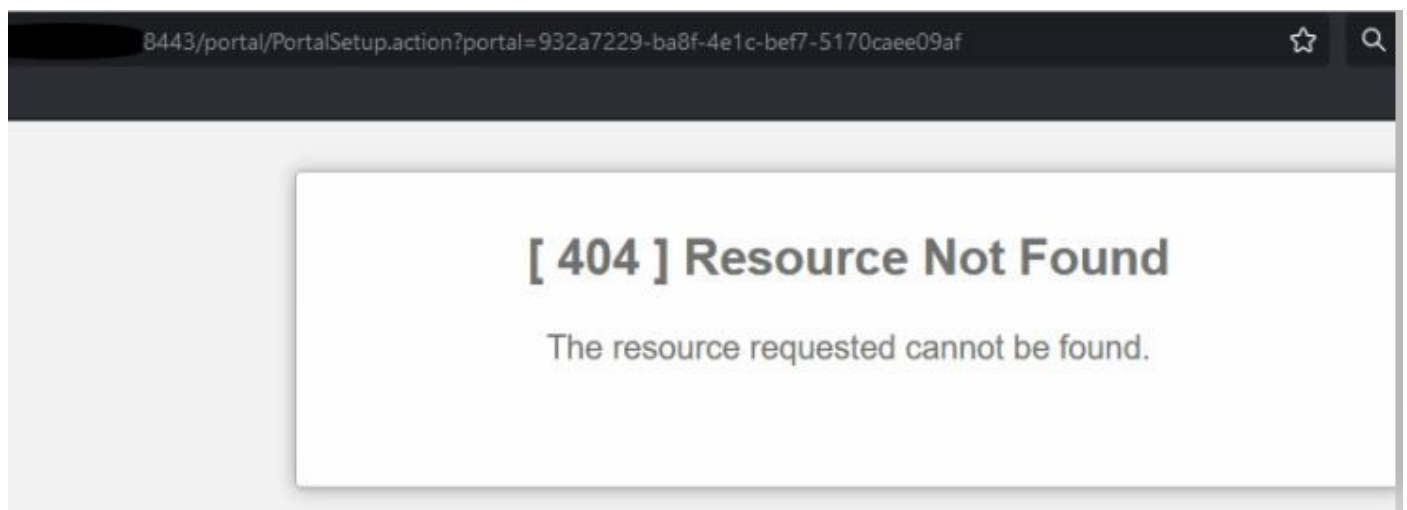
De acordo com a resposta de IdP fornecida anteriormente, o mapeamento do ISE para o grupo **iseadmins** deve ser configurado para que o logon seja bem-sucedido.



The screenshot shows the Cisco ISE Administration console. The left sidebar lists 'External Identity Sources' with categories like Certificate Authentication, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, and SAML Id Providers. The main area is titled 'SAML Identity Provider' and has tabs for 'General', 'Identity Provider Config.', 'Service Provider Info.', 'Groups', and 'Attrib'. The 'Groups' tab is active, showing a 'Group Membership Attribute' set to 'Rom_Azure_Groups'. Below this, there are '+ Add', 'Edit', and 'Delete' buttons. A table lists groups with columns for 'Name in Assertion' and 'Name in ISE'. The 'iseadmins' group is highlighted with a red arrow, and its 'Name in ISE' is 'Super Admin'.

<input type="checkbox"/>	Name in Assertion	Name in ISE
<input type="checkbox"/>	iseadmins	Super Admin

Problema 2: 404 Recurso não encontrado



The screenshot shows a web browser displaying a 404 error. The address bar contains the URL: `8443/portal/PortalSetup.action?portal=932a7229-ba8f-4e1c-bef7-5170caee09af`. The main content area shows a large white box with the text: **[404] Resource Not Found** and *The resource requested cannot be found.*

Você vê um erro em **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.
```

Causa/solução

Esse problema é observado depois que o cria somente o primeiro armazenamento de ID.

Para resolver isso, tente o seguinte na mesma ordem:

Etapa 1. Crie um novo IdP SAML no ISE (Não remova o atual ainda.).

Etapa 2. Vá para a página de acesso de administrador e atribua o seu acesso de administrador a este novo IdP.

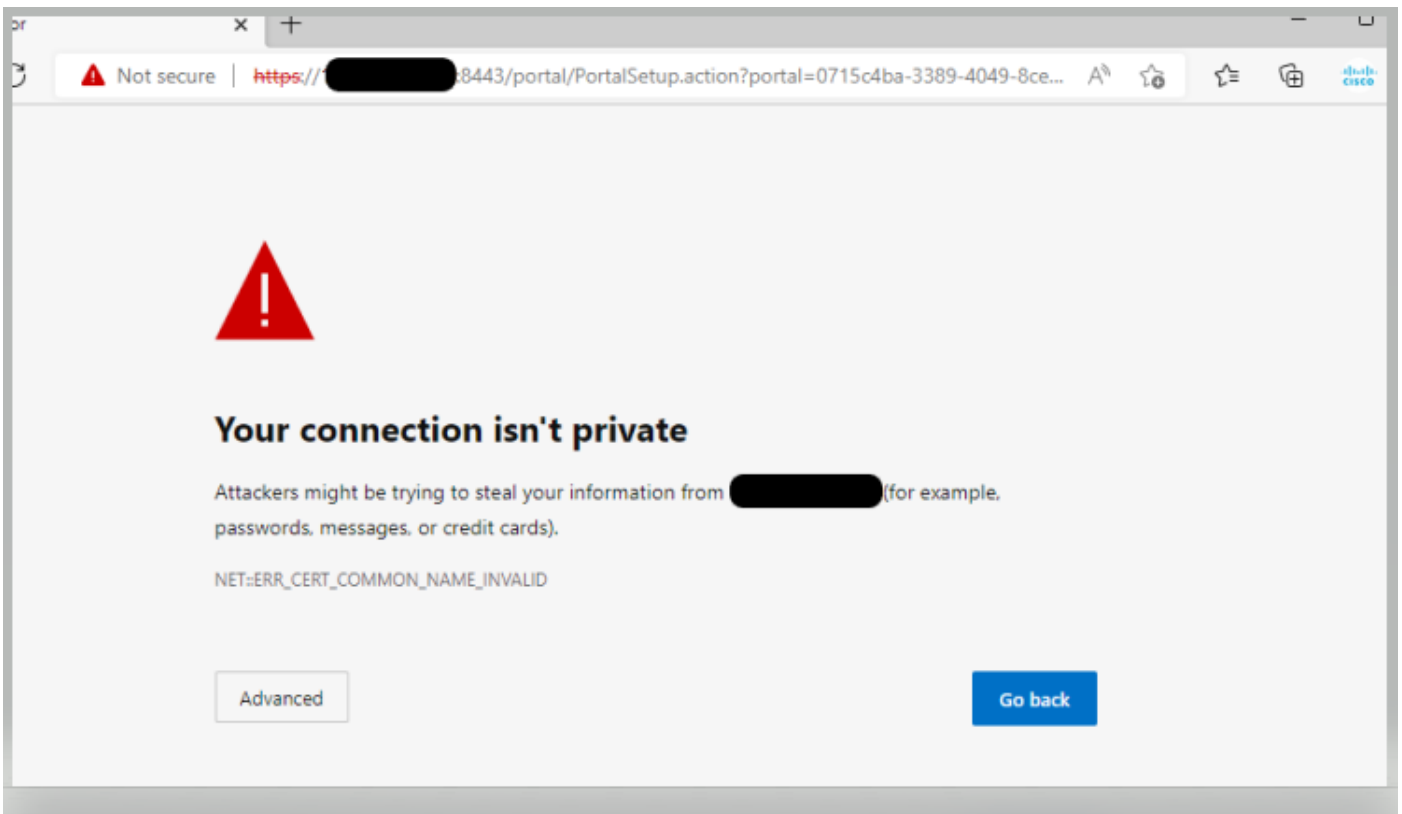
Etapa 3. Excluir o IdP antigo na página Provedores de identidade externos.

Etapa 4. Importe os metadados de IdP atuais para o novo IdP criado na etapa 1 e execute todos os mapeamentos de grupo necessários.

Etapa 5. Agora tente o login SAML; funcionará.

Problema 3: Aviso de certificado

Em uma implantação de vários nós, quando você clica em "Fazer login com SAML", você pode ver um aviso de certificado não confiável no navegador



Causa/solução

Em alguns casos, o pPAN o redireciona para o IP PSNs ativo, não para o FQDN. Isso causa um aviso de certificado em alguma implantação de PKI, se não houver endereço IP no campo SAN.

A solução é adicionar o IP no campo SAN do certificado.

ID de bug da Cisco [CSCvz89415](#). Resolvido no 3.1p1

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.