

Configurar e solucionar problemas do SSO do WebApp no CMS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Diagrama de Rede](#)

[Instalação e Configuração Inicial do ADFS](#)

[Mapear usuários do CMS para o provedor de identidade \(IdP\)](#)

[Criar XML de Metadados do Webbridge para IdP](#)

[Importar metadados para Webbridge no Identity Provider \(IdP\)](#)

[Criar Regras de Declaração para o Serviço Webbridge no IdP](#)

[Criar arquivo ZIP de arquivo SSO para Webbridge:](#)

[Obter e configurar o idp_config.xml](#)

[Crie o config.jsonFile com Conteúdo](#)

[Defina sso_sign.key \(OPCIONAL\)](#)

[Defina sso_encrypt.key \(OPCIONAL\)](#)

[Criando o arquivo ZIP SSO](#)

[Carregue o\(s\) arquivo\(s\) Zip do SSO no Webbridge](#)

[Cartão de acesso comum \(CAC\)](#)

[Testando o login do SSO via WebApp](#)

[Troubleshooting](#)

[Troubleshooting Básico](#)

[Códigos de falha do Microsoft ADFS](#)

[Falha ao obter authenticationID](#)

[Nenhuma asserção foi aprovada/correspondida na validação](#)

[Falha ao Entrar no Aplicativo Web:](#)

[Cenário 1:](#)

[Cenário 2:](#)

[Cenário 3:](#)

[O nome de usuário não é reconhecido](#)

[Cenário 1:](#)

[Cenário 2:](#)

[Log do Webbridge mostrando o exemplo de log de trabalho em. Exemplo gerado com ?trace=true no URL de junção:](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e solucionar problemas da implementação do Cisco Meeting Server (CMS) Web App de Logon Único (SSO).

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- CMS Callbridge versão 3.1 ou posterior
- CMS Webbridge versão 3.1 ou posterior
- Servidor do Active Directory
- Identificar Provedor (IdP)

Componentes Utilizados

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

- CMS Callbridge versão 3.2
- CMS Webbridge versão 3.2
- Microsoft Active Directory Windows Server 2012 R2
- Windows Server 2012 R2 do Microsoft ADFS 3.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.


Background

O CMS 3.1 e versões posteriores introduziram a capacidade de os usuários entrarem usando um SSO sem a necessidade de digitar sua senha toda vez que o usuário fizer login, pois uma única sessão é criada com o provedor Identify.

Este recurso está usando a Security Assertion Markup Language (SAML) versão 2.0 como o Mecanismo SSO.

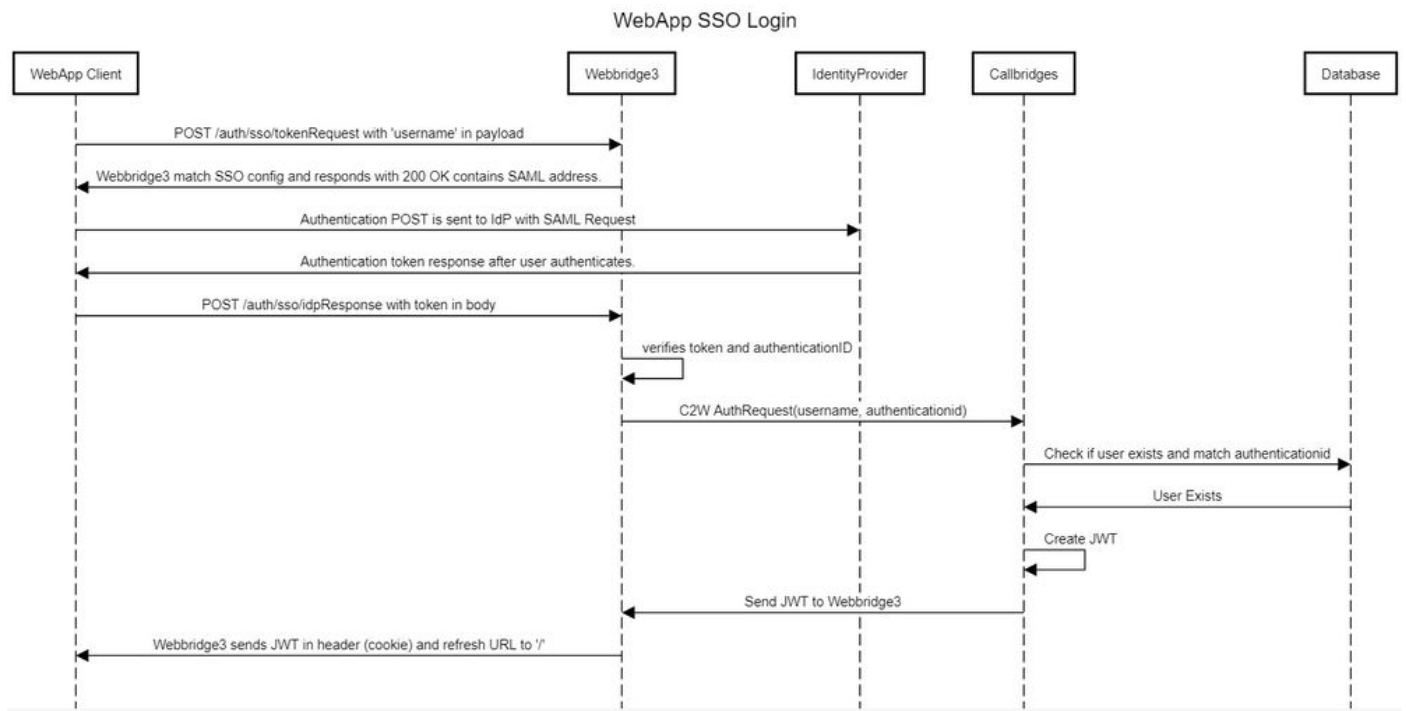


Nota: O CMS suporta apenas associações HTTP-POST no SAML 2.0 e rejeita qualquer Identify Provider sem associações HTTP-POST disponíveis.

 Observação: quando o SSO está ativado, a autenticação LDAP básica não é mais possível.

Configurar

Diagrama de Rede



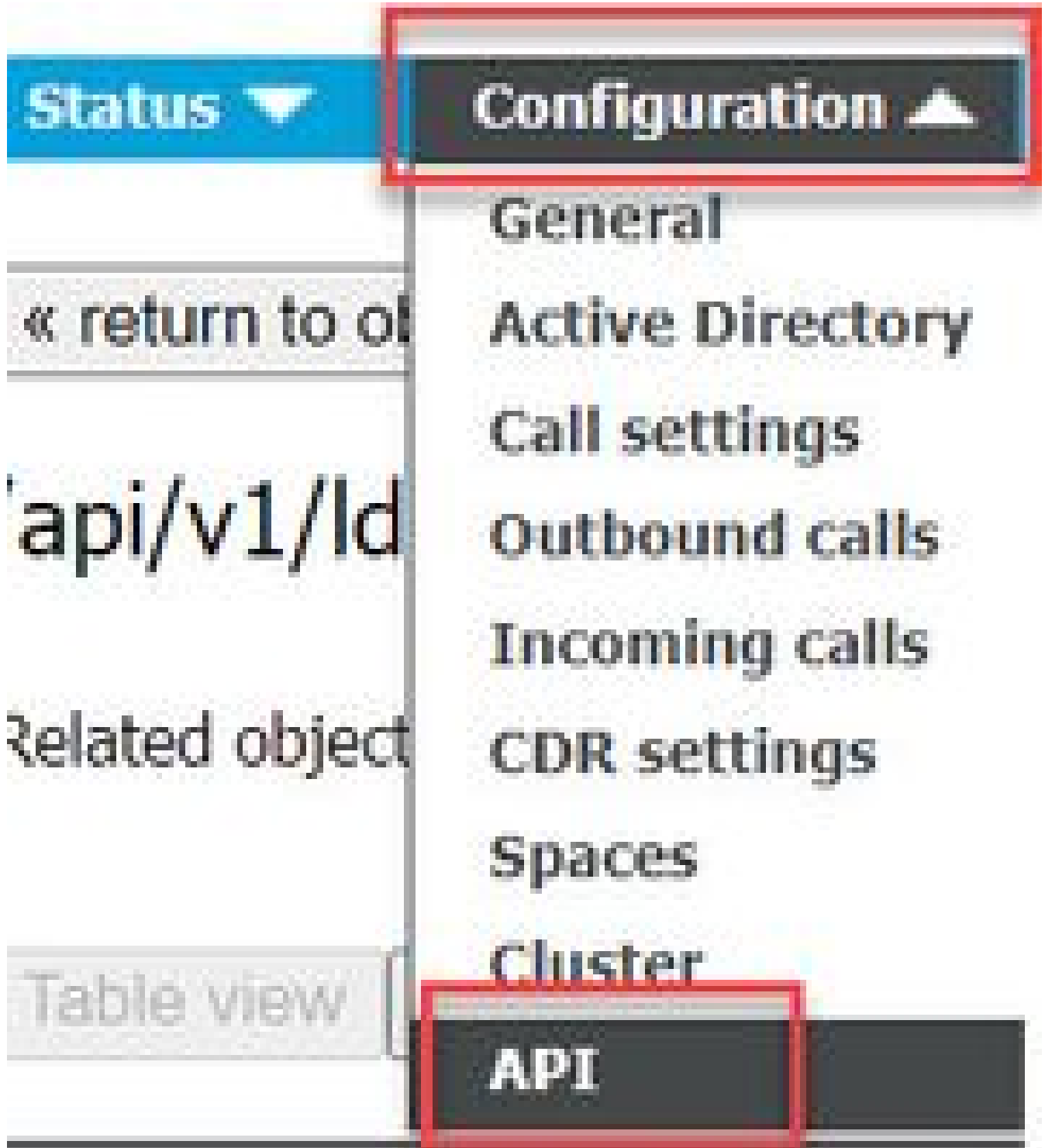
Instalação e Configuração Inicial do ADFS

Este cenário de implantação usa os Serviços de Federação do Microsoft Active Directory (ADFS) como o Provedor de Identidade (IdP) e, portanto, sugere-se ter um ADFS (ou IdP pretendido) instalado e em execução antes desta configuração.

Mapear usuários do CMS para o provedor de identidade (IdP)

Para que os usuários obtenham uma autenticação válida, eles devem ser mapeados na Interface de Programação de Aplicativos (API) para um campo correlacionado fornecido pelo IdP. A opção usada para isso é `authenticationIdMapping` no `IdapMapping` da API.

1. Navegue até Configuration > API na GUI do CMS Web Admin



2. Localize o Mapeamento LDAP existente (ou criando um novo) em `api/v1/ldapMappings/<GUID-of-Ldap-Mapping>`.

API objects

This page shows a list of the objects supported by the API. Where you see a ► control, you can expand that section to either see details of one specific section of configuration.

Filter (2 of 129 nodes)

/api/v1/ldapMappings ◀


◀ start < prev 1 - 2 (of 2) next >

object id	iidMapping
458ad270-860b-4bac-9497-b74278ed2086	\$sAMAccountName\$@brhuff.com

3. No objeto ldapMapping selecionado, atualize o authenticationIdMapping para o atributo LDAP que é passado do IdP. No exemplo, a opção \$sAMAccountName é usada como o atributo LDAP para mapeamento.

/api/v1/ldapMappings/458ad270-860b-4bac-9497-b74278ed2086

jidMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$@brhuff.com"/>	- present
nameMapping	<input type="checkbox"/>	<input type="text" value="\$cn\$"/>	- present
cdrTagMapping	<input type="checkbox"/>	<input type="text"/>	
coSpaceUriMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$ space"/>	- present
coSpaceSecondaryUriMapping	<input type="checkbox"/>	<input type="text"/>	
coSpaceNameMapping	<input type="checkbox"/>	<input type="text" value="\$cn\$'s Space"/>	- present
coSpaceCallIdMapping	<input type="checkbox"/>	<input type="text"/>	
authenticationIdMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$"/>	- present

 Observação: O authenticationIdMapping é usado pelo callbridge/banco de dados para validar a declaração enviada do IdP na SAMLResponse e fornecer ao usuário um JWT (JSON Web Token).

4. Execute uma sincronização LDAP no ldapSource associado ao ldapMapping recentemente modificado:

Por exemplo:

/api/v1/ldapSyncs

tenant	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
ldapSource	<input checked="" type="checkbox"/>	<input type="text" value="0b8de8cd-ccce-4ccb-89a8-08ba69e98ec7"/>	<input type="button" value="Choose"/>
removeWhenFinished	<input type="checkbox"/>	<unset> ▼	
<input type="button" value="Create"/>			

5. Após a conclusão da sincronização LDAP, navegue na API do CMS em Configuration > api/v1/users e selecione um usuário que foi importado e verifique se a authenticationId está preenchida corretamente.

Object configuration	
userId	jdoe@brhuff.com
name	John Doe
email	john.doe@brhuff.com
authenticationId	jdoe
userProfile	d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3

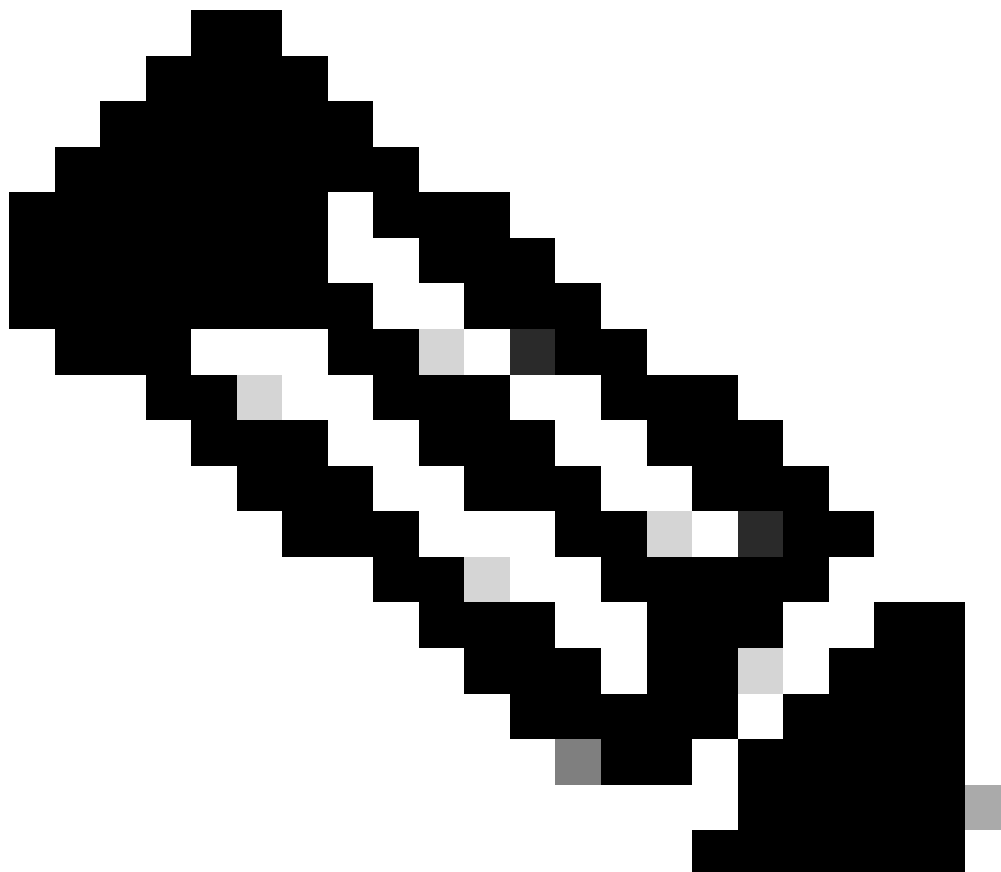
Criar XML de Metadados do Webbridge para IdP

O Microsoft ADFS permite que um arquivo XML de metadados seja importado como uma terceira parte confiável para identificar o provedor de serviços que está sendo usado. Há algumas maneiras de criar o arquivo XML de metadados para essa finalidade, no entanto, há alguns atributos que devem estar presentes no arquivo:

Exemplo de metadados de Webbridge com valores obrigatórios:

```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true"
    AuthnRequestsSigned="false">
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:AssertionConsumerService index="0" Location="https://meet.brhuff.local:443/api/auth/sso/idpResponse"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

1. entityID - É o endereço do servidor Webbridge3 (FQDN/Nome do host) e a porta associada que pode ser alcançada pelos navegadores para usuários.



Observação: se houver várias Webbridges usando um único URL, esse deverá ser um endereço de balanceamento de carga.

2. Location - (Local) O local no qual o AssertionConsumerService HTTP-POST para o endereço Webbridge. Isso é o que informa ao IdP para onde redirecionar um usuário autenticado após a entrada. Ele deve ser definido como a URL idpResponse: <https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponse>. Por exemplo, <https://join.example.com:443/api/auth/sso/idpResponse>.
3. OPCIONAL - Chave Pública para Assinatura - é a chave pública (certificado) para assinatura, que deve ser usada pelo IdP para verificar AuthRequest da Webbridge. Isso DEVE corresponder à chave privada 'sso_sign.key' no pacote SSO carregado no Webbridge para que o IdP possa usar a chave pública (certificado) para verificar a assinatura. Você pode usar um certificado existente de sua implantação. Abra o certificado em um arquivo de texto e copie o conteúdo no arquivo de metadados do Webbridge. Use a chave correspondente para o certificado usado no arquivo sso_xxxx.zip como o arquivo sso_sign.key.

4. OPCIONAL - Chave pública para criptografia - esta é a chave pública (certificado) que o IdP usa para criptografar informações SAML enviadas de volta para Webbridge. Isso DEVE corresponder à chave privada 'sso_encrypt.key' no pacote SSO carregado no Webbridge, para que o Webbridge possa descriptografar o que é enviado de volta pelo IdP. Você pode usar um certificado existente de sua implantação. Abra o certificado em um arquivo de texto e copie o conteúdo no arquivo de metadados do Webbridge. Use a chave correspondente para o certificado usado no arquivo sso_xxxx.zip como o arquivo sso_encrypt.key.

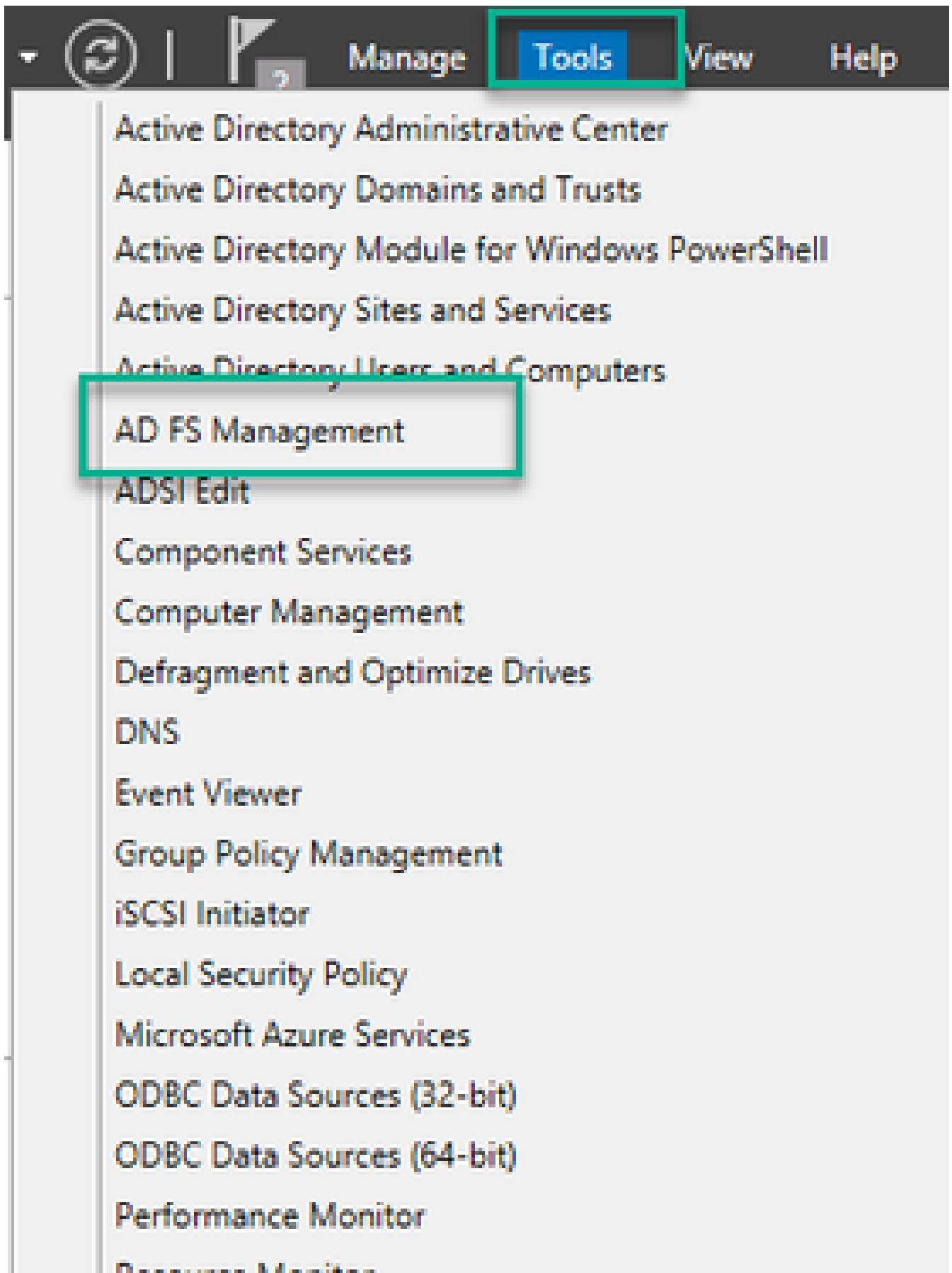
Exemplo de metadados de Webbridge a serem importados para o IdP com dados opcionais de chave pública (certificado):

```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
          <ds:X509Certificate>MIIFwTCCBKmqAwIBAgIT[REDACTED]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    - <md:KeyDescriptor use="encryption">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
          <ds:X509Certificate>MIIFwTCCBKmqAwIBAgIT[REDACTED]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
    <md:AssertionConsumerService index="0" Location="https://meet.brhuff.local:443/api/auth/sso/idpResponse" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

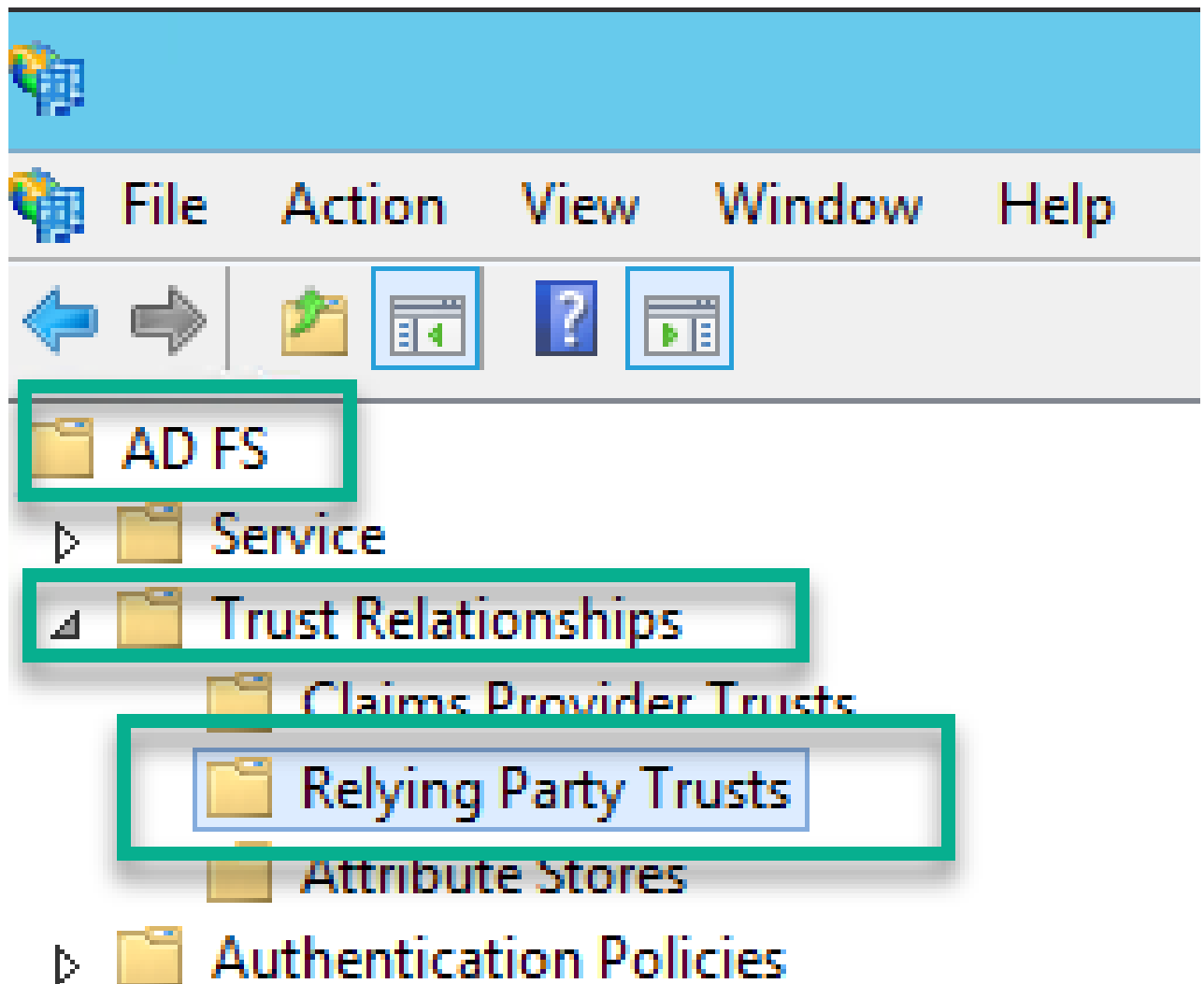
Importar metadados para Webbridge no Identity Provider (IdP)

Depois que o XML de metadados tiver sido criado com os atributos apropriados, o arquivo poderá ser importado para o servidor Microsoft ADFS para criar uma Terceira Parte Confiável Confiável.

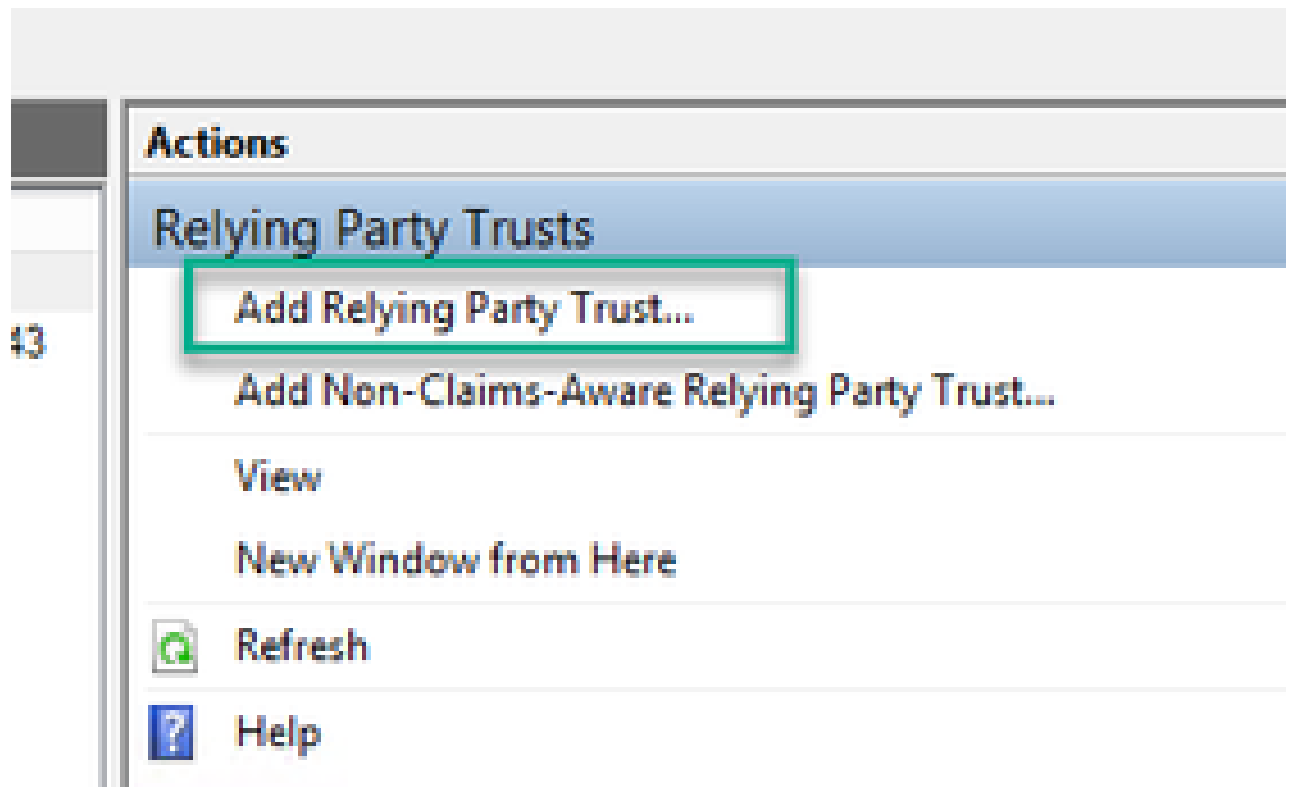
1. Área de Trabalho Remota no Windows Server que hospeda os serviços ADFS
2. Abra o Console de Gerenciamento do AD FS, que geralmente pode ser acessado por meio do Gerenciador do Servidor.



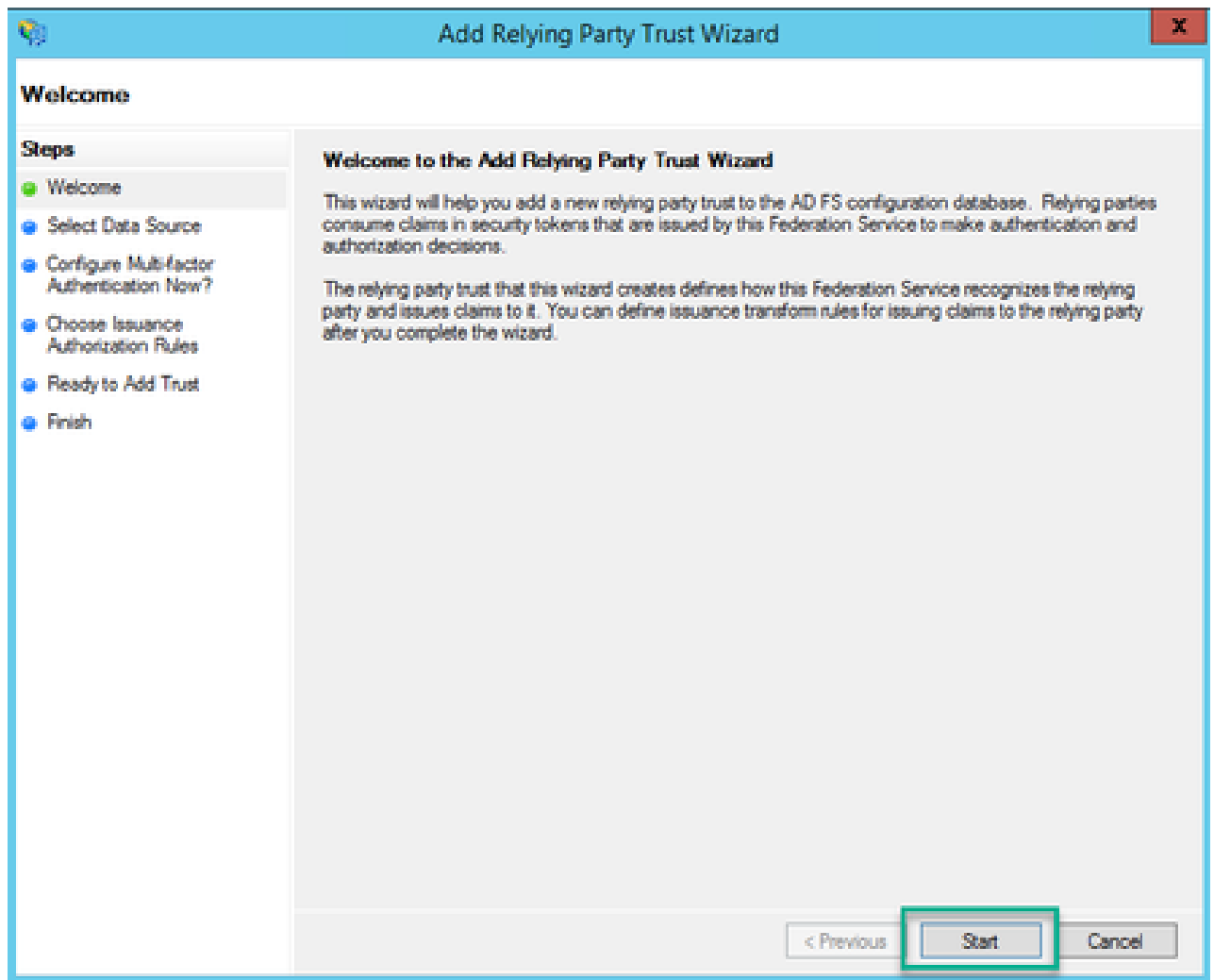
3. No console Gerenciamento do ADFS, navegue para ADFS > Relações de Confiança > Confiança da Terceira Parte Confiável no painel Esquerdo.



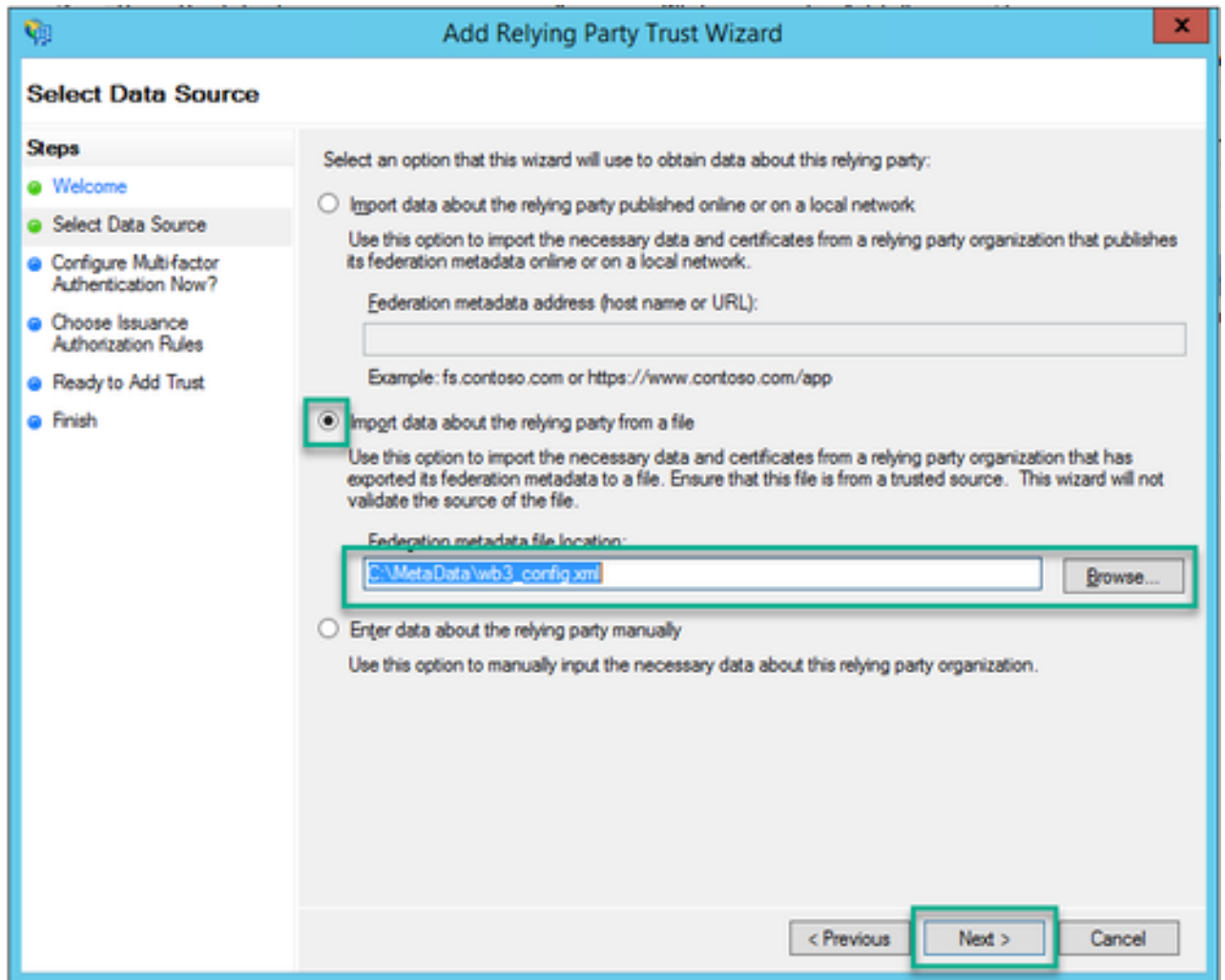
4. No painel Direito do Console de Gerenciamento do ADFS, selecione a opção Adicionar Terceira Parte Confiável...



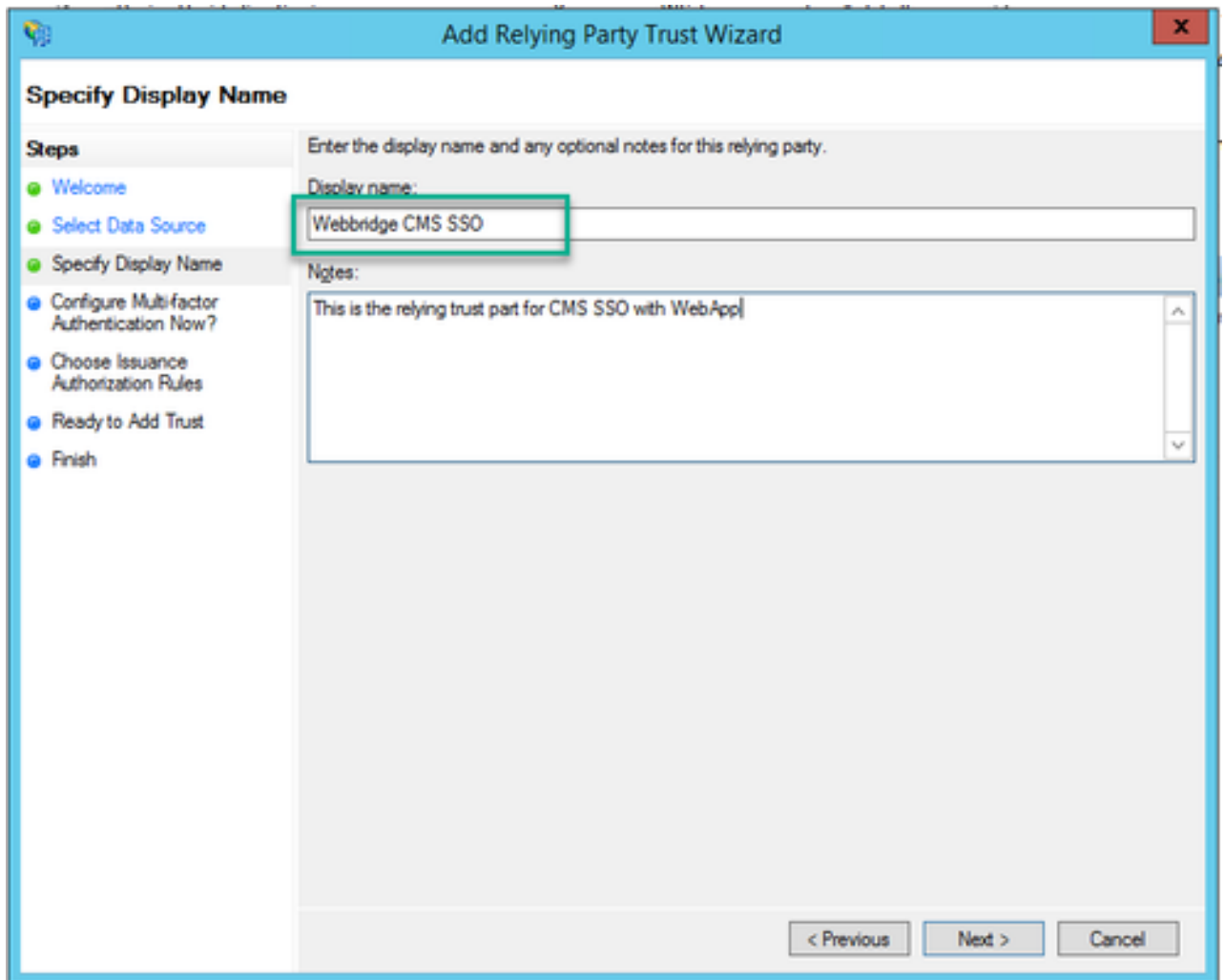
5. Depois de fazer essa seleção, o Assistente de Adição de Confiança da Terceira Parte Confiável será aberto. Selecione a opção Start.



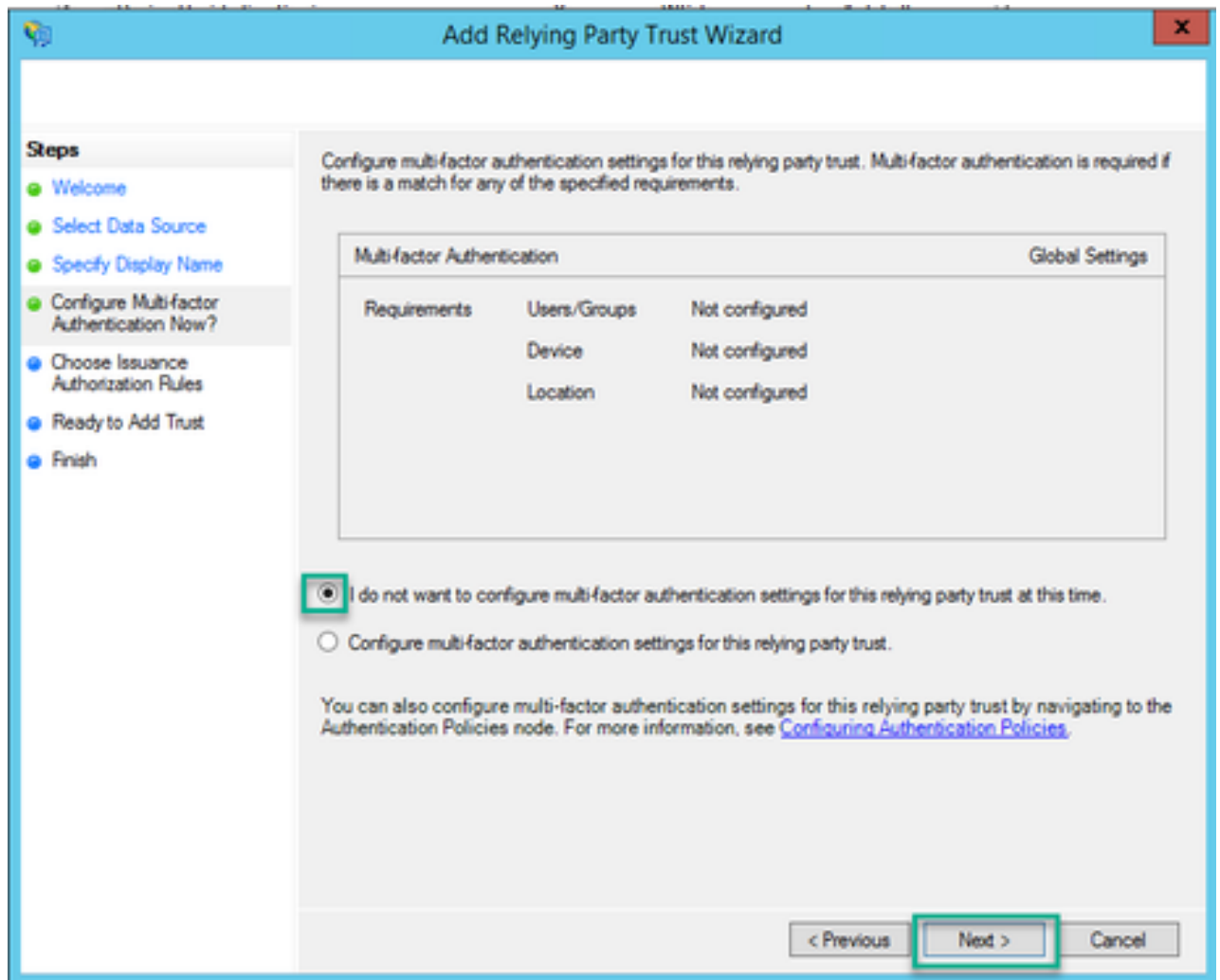
6. Na página Selecionar Origem de Dados, selecione o botão de opção Importar dados sobre a terceira parte confiável de um arquivo e selecione Procurar e navegue até o local do arquivo de Metadados do Webbridge.



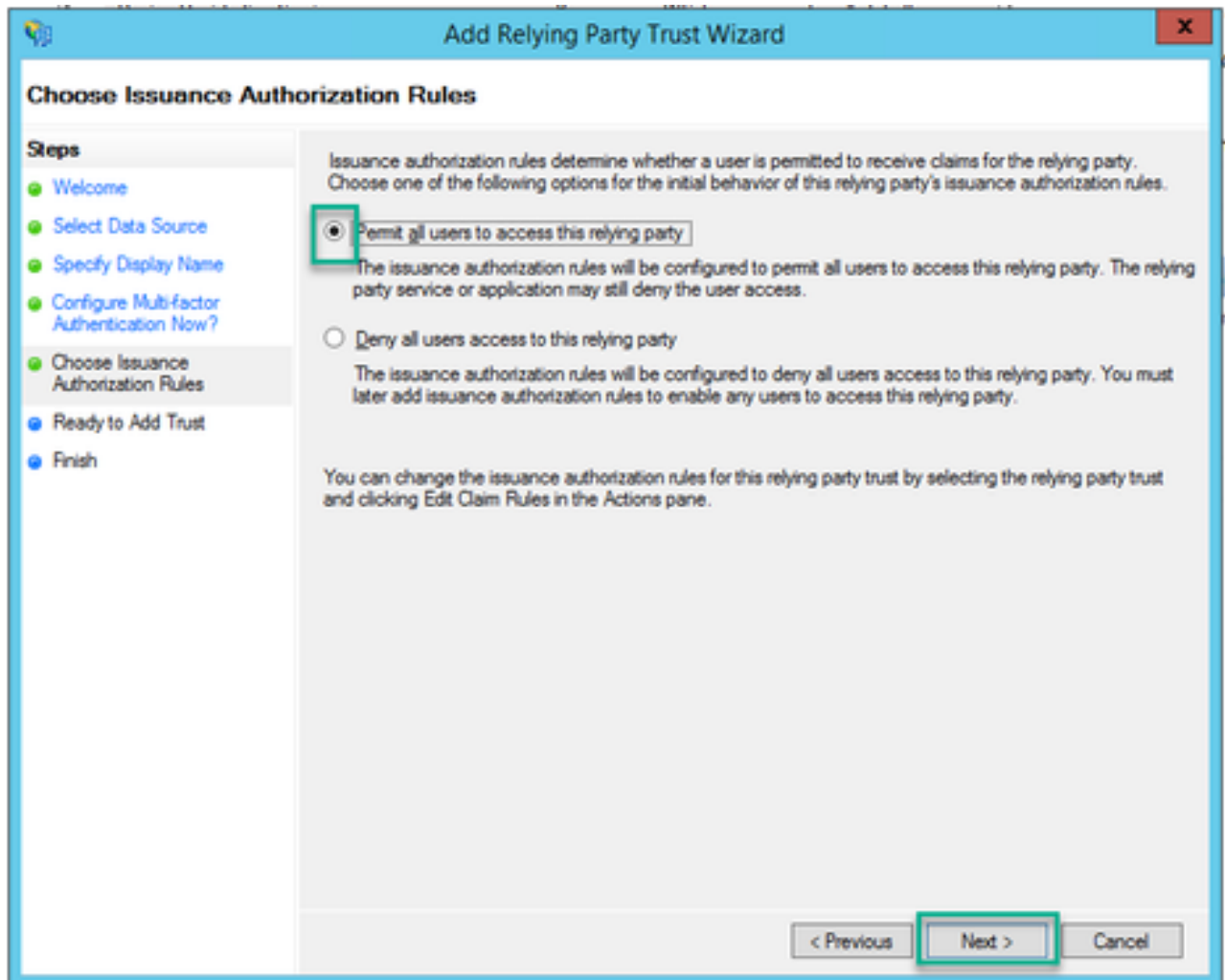
7. Na página Especificar Nome para Exibição, coloque um nome a ser exibido para a entidade no ADFS (o Nome para Exibição não serve para fins de comunicação do ADFS e é meramente informativo).



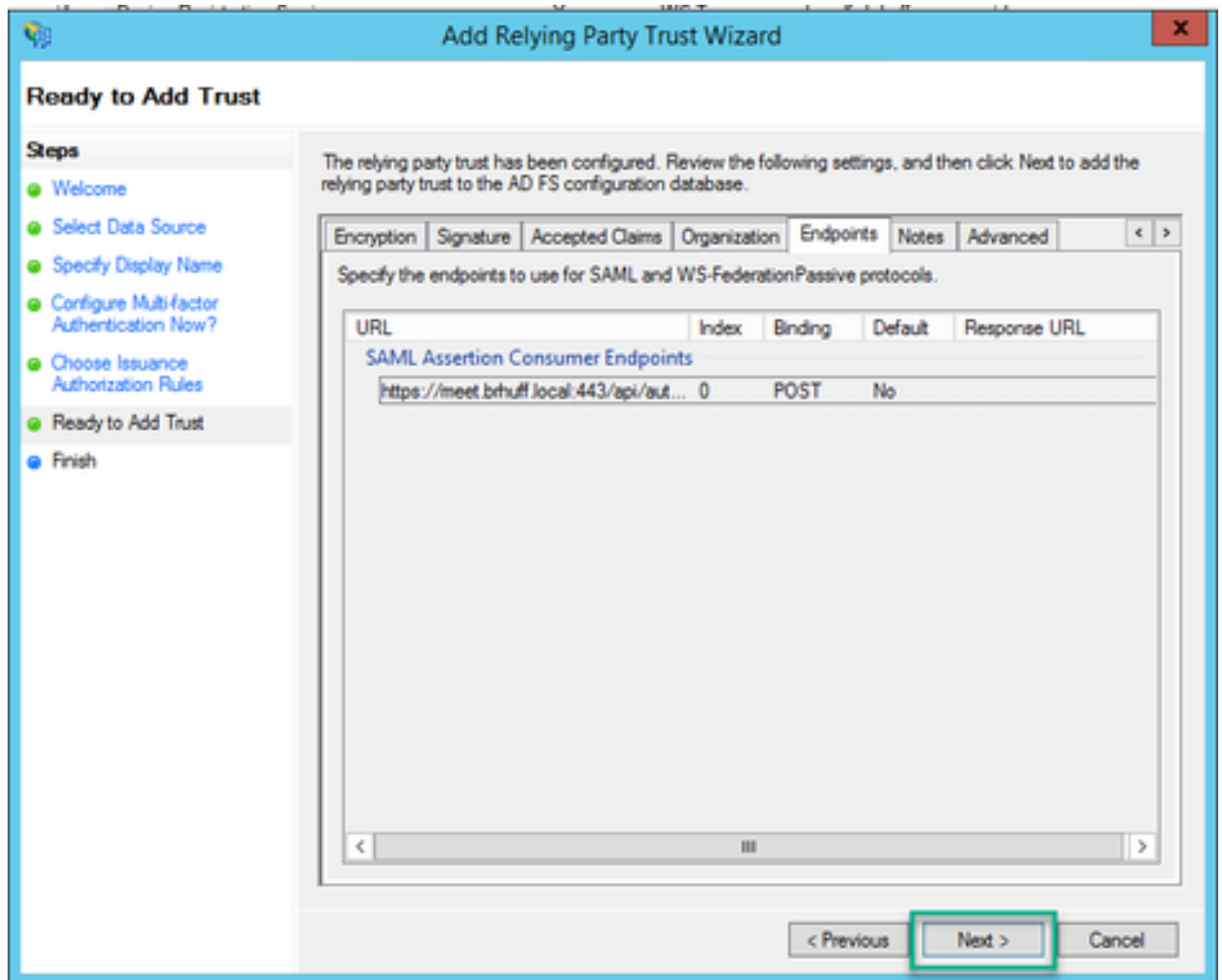
8. Na página Configurar Multi-fator Authentication Now?, deixe como padrão e selecione Próximo.



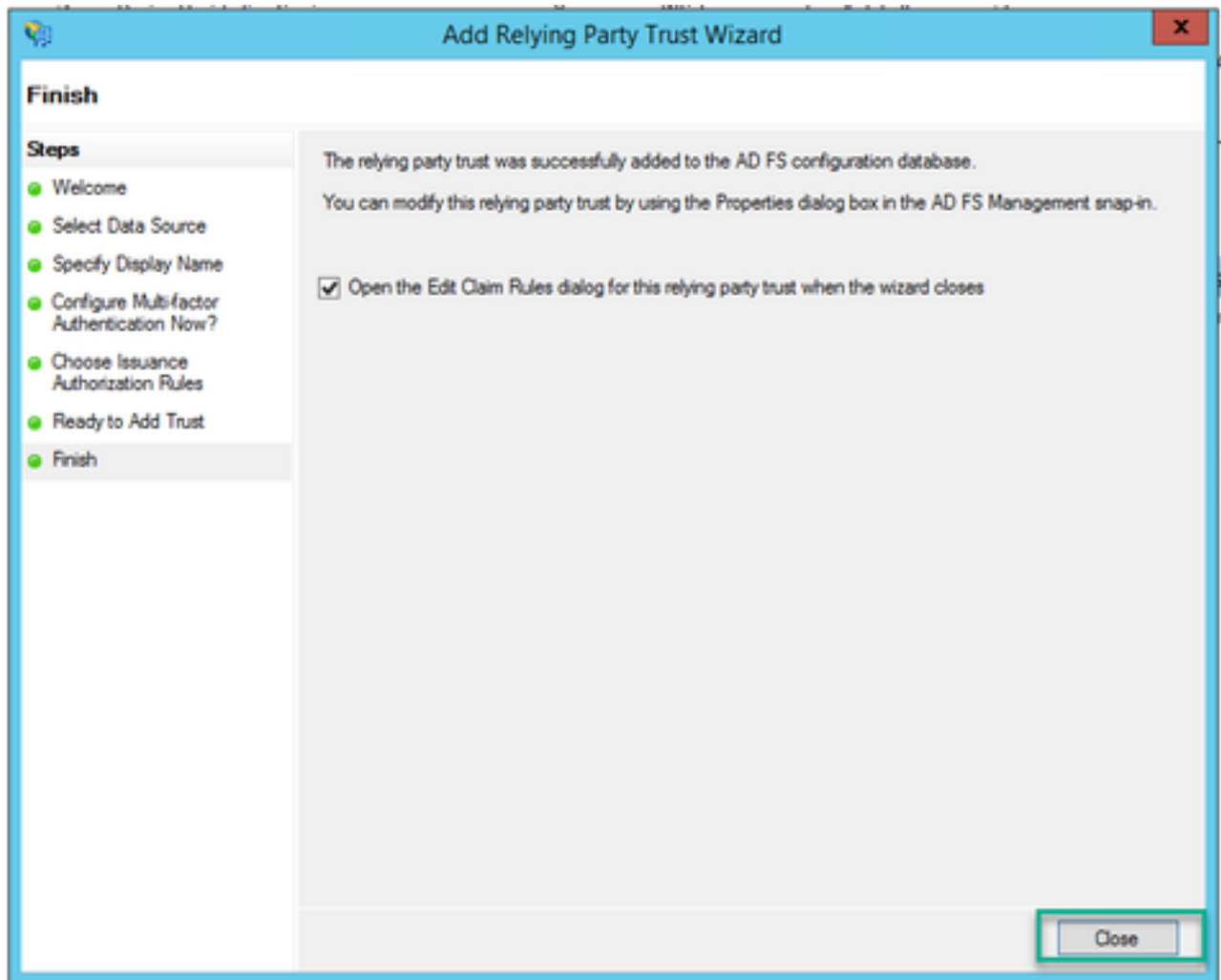
9. Na página Escolher Regras de Autorização de Emissão, deixe como selecionado Permitir que todos os usuários acessem esta terceira parte confiável.



10. Na página Pronto para Adicionar Confiança, os detalhes importados da Terceira Parte Confiável Confiável para Webbridge podem ser revisados por meio das guias. Verifique os Identificadores e Pontos Finais para obter os detalhes da URL para o Provedor de Serviços Webbridge.



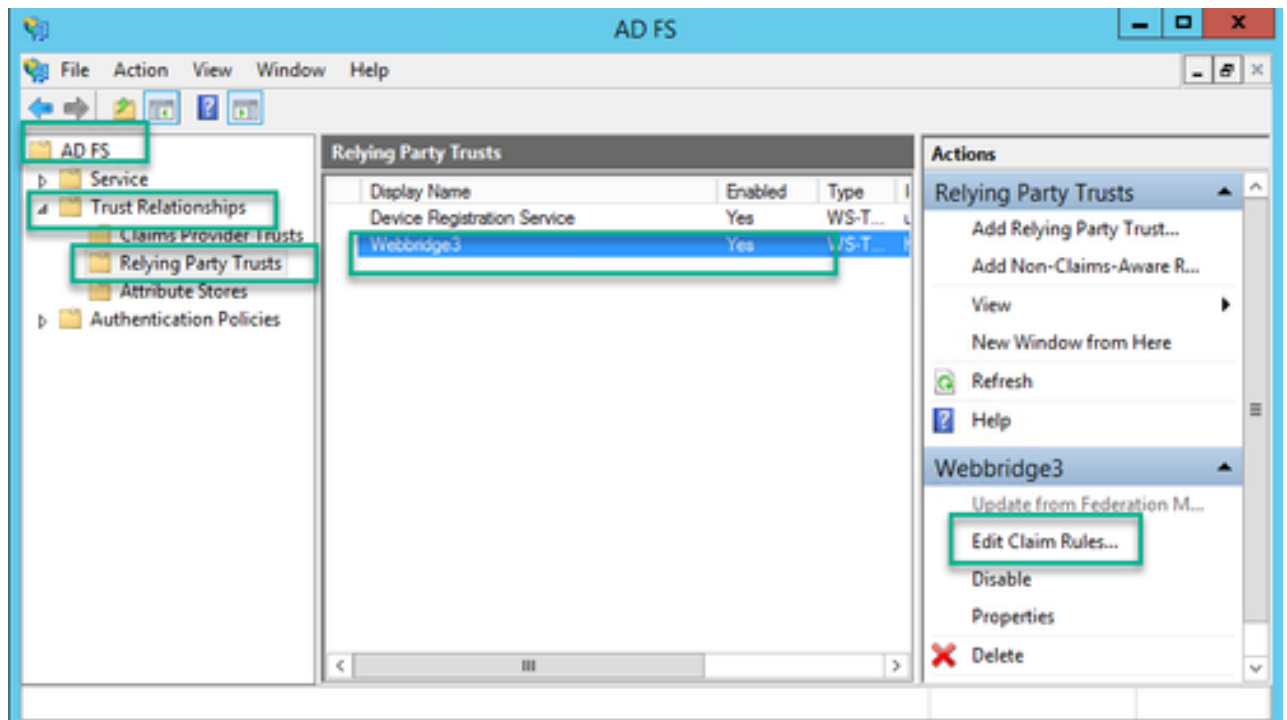
11. Na página Finalizar, selecione a opção Fechar para fechar o assistente e continuar a editar as regras de reivindicação.



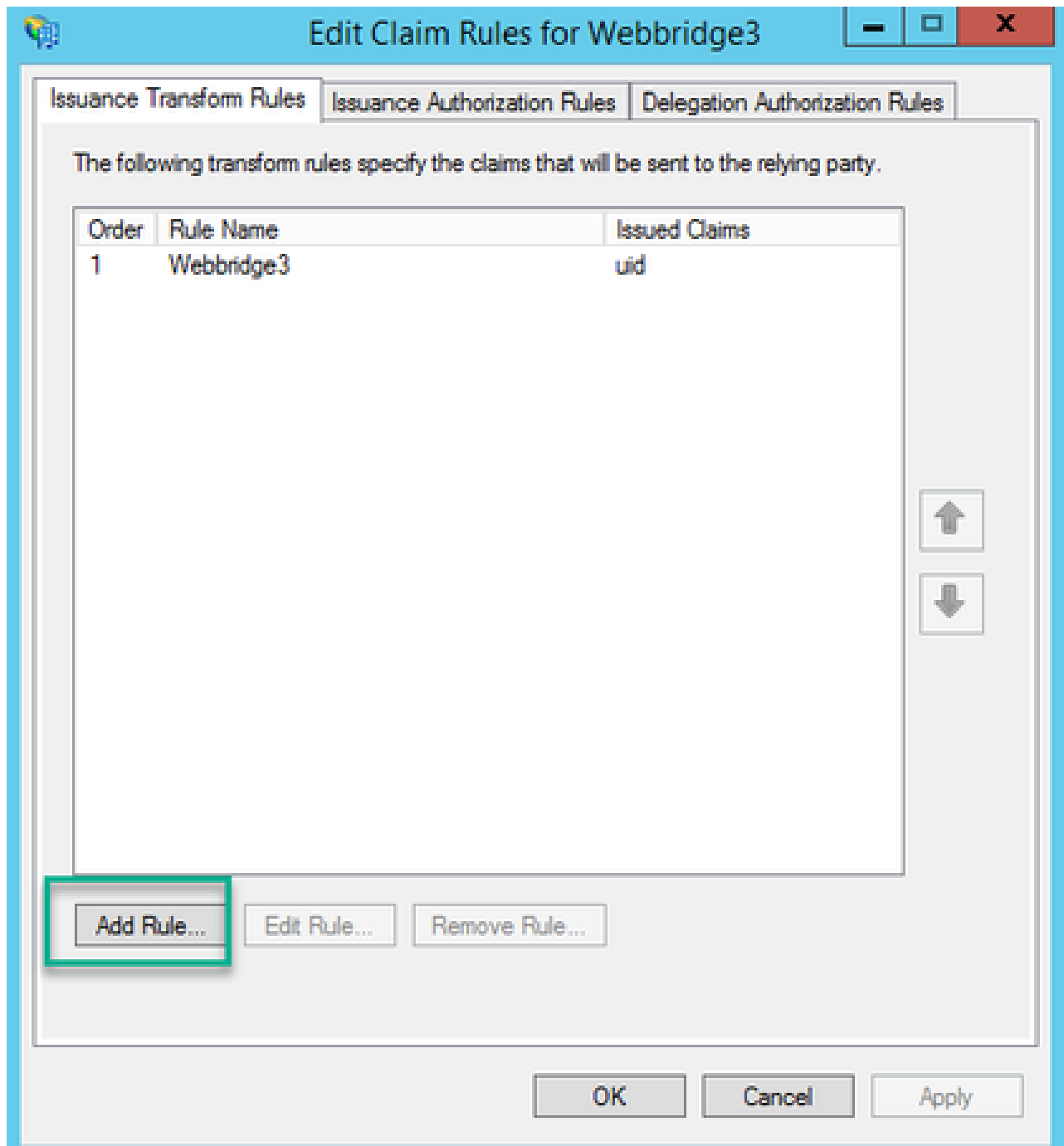
Criar Regras de Declaração para o Serviço Webbridge no IdP

Agora que a Confiança da Terceira Parte Confiável foi criada para a Webbridge, as regras de declaração podem ser criadas para corresponder Atributos LDAP específicos a tipos de declaração de saída a serem fornecidos à Webbridge na Resposta SAML.

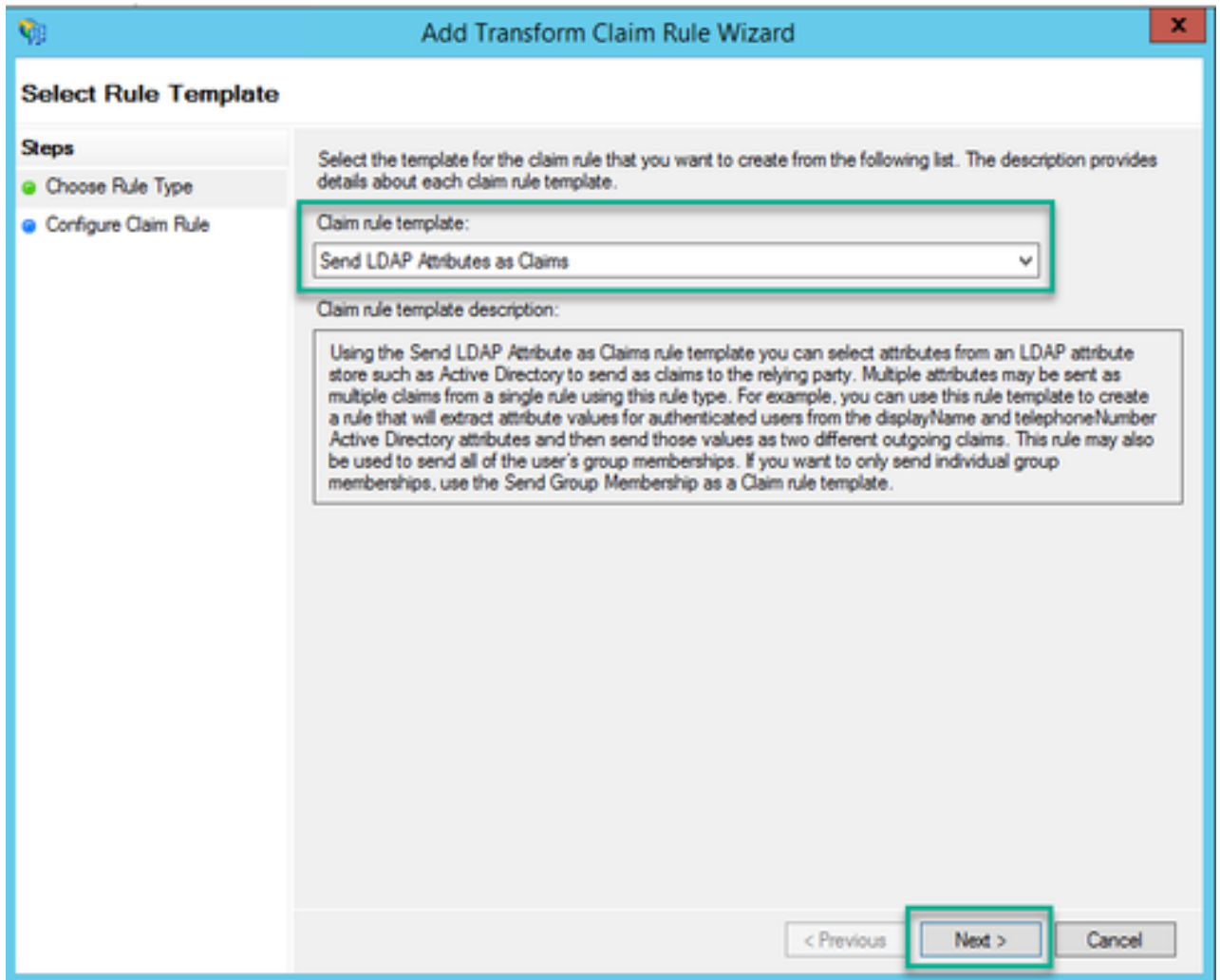
1. No console de Gerenciamento do ADFS, realce a Terceira Parte Confiável para a Webbridge e selecione Editar Regras de Reivindicação no painel direito.



2. Na página Editar Regras de Reivindicação para <DisplayName>, selecione Adicionar Regra....



3. Na página Assistente para Adicionar Regra de Reivindicação de Transformação, selecione Enviar Atributos LDAP como Reivindicações para a opção de modelo Regra de reivindicação e selecione Próximo.



4. Na página Configurar Regra de Declaração, configure a regra de declaração para o Objeto de Confiança da Terceira Parte Confiável com estes valores:

1. Nome da regra de declaração = deve ser um nome dado à regra no ADFS (somente para referência de regra)
2. Repositório de atributos = Ative Diretory
3. Atributo LDAP = Deve corresponder ao authenticationIdMapping na API do Callbridge. (Por exemplo, \$sAMAccountName\$.)
4. Tipo de Declaração de Saída = Deve corresponder ao authenticationIdMapping no Webbridge SSO config.json. (Por exemplo, uid.)

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Webbridge3

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
⊞		

View Rule Language...

OK

Cancel

Criar arquivo ZIP de arquivo SSO para Webbridge:

Essa configuração é o que a Webbridge menciona para validar a configuração SSO para domínios suportados, mapeamento de autenticação e assim por diante. Estas regras devem ser consideradas para esta parte da configuração:

- O arquivo ZIP DEVE começar com sso_ prefixado ao nome do arquivo (por exemplo, sso_cmstest.zip).
- Depois que esse arquivo é carregado, o Webbridge desabilita a autenticação básica e SOMENTE o SSO pode ser usado para o Webbridge no qual ele foi carregado.

- Se houver vários provedores de identidade usados, um arquivo ZIP separado deverá ser carregado com um esquema de nomeação diferente (AINDA prefixado com o sso_).
- Ao criar o arquivo zip, certifique-se de realçar e compactar o conteúdo do arquivo e não coloque os arquivos necessários em uma pasta e compacte-a.

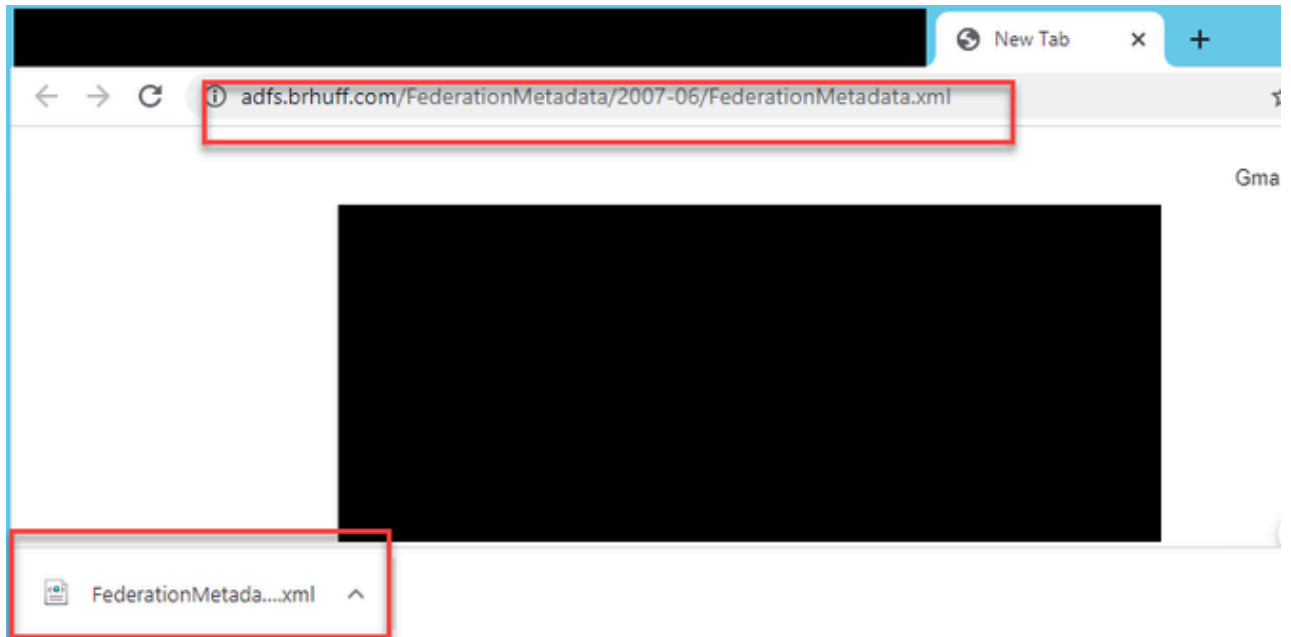
O conteúdo do arquivo zip é composto de 2 a 4 arquivos, dependendo se a criptografia está sendo usada ou não.

Nome de arquivo	Descrição	Necessário?
idp_config.xml	Este é o arquivo de Metadados que pode ser coletado pelo idP. No ADFS, ela pode ser localizada em <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml .	SIM
config.json	Esse é o arquivo JSON no qual o Webbridge usa o para validar os domínios suportados, o mapeamento de autenticação para o SSO.	SIM
sso_sign.key	Esta é a chave privada da chave pública de assinatura configurada no Provedor de Identificação. Necessário apenas para proteger os dados assinados	NO
sso_encrypt.key	Esta é a chave privada para a chave de criptografia pública configurada no Provedor de Identificação. Necessário apenas para proteger os dados criptografados	NO

Obter e configurar o idp_config.xml

1. No servidor ADFS (ou em um local que tenha acesso ao ADFS), abra um navegador da Web.

2. No Navegador da Web, insira o URL: <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml> (Você também poderá usar localhost em vez do FQDN se estiver localmente no servidor ADFS). Isso faz download do arquivo FederationMetadata.xml.



3. Copie o arquivo baixado para um local onde o arquivo zip esteja sendo criado e renomeie para idp_config.xml.

Name

config.json

FederationMetadata.xml

Open

Edit

Share with Skype

Move to OneDrive

7-Zip

CRC SHA

Edit with Notepad++

Share

Open with

Cisco AMP For Endpoints

Restore previous versions

Send to

Cut

Copy

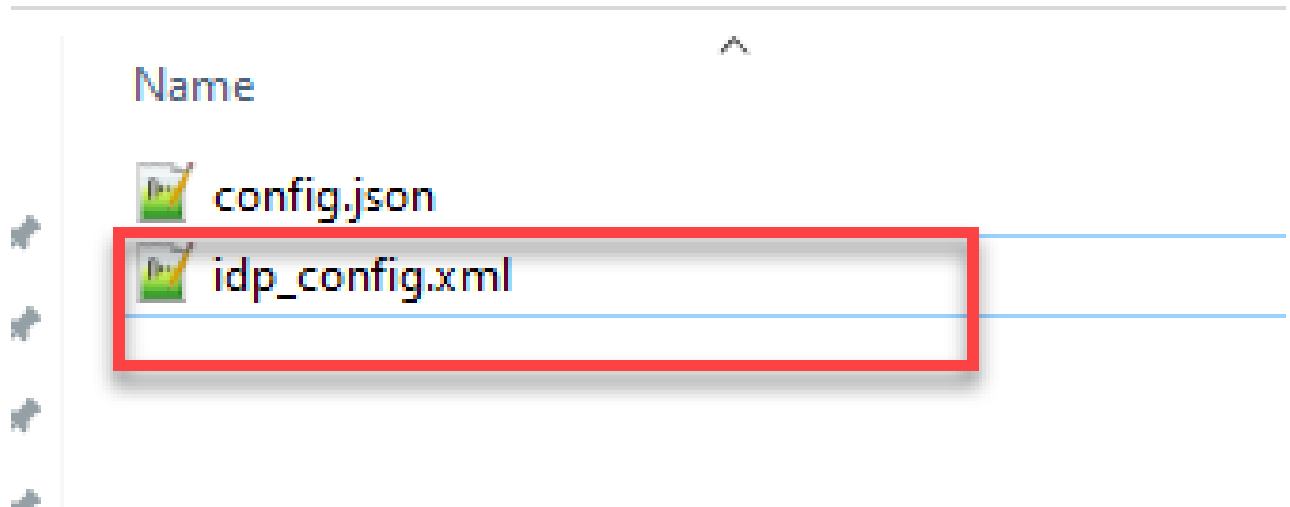
Create shortcut

Delete

Rename

Properties

Local Disk (D:) > brentssoconfig > SSOconfig



Crie o arquivo config.json com conteúdo

O config.json contém esses 3 atributos e eles devem estar entre colchetes, { }:

1. supportedDomains - Esta é uma lista de domínios nos quais a autenticação SSO é verificada em relação ao IdP. Vários domínios podem ser separados por vírgulas.
2. authenticationIdMapping - Este é o parâmetro repassado como parte da regra de declaração de saída do ADFS/IdP. Ele deve corresponder ao valor do nome do tipo de declaração de saída no IdP. Regra de reivindicação.
3. ssoServiceProviderAddress - Este é o URL do FQDN para o qual o Identify Provider envia as respostas SAML. Deve ser o FQDN Webbridge.

Configured as 'uid' to match outgoing claim on ADFS

```
1 {
2   "authenticationIdMapping": "uid",
3   "ssoServiceProviderAddress": "https://meet.brhuff.local:443",
4   "supportedDomains": ["brhuff.com"]
5 }
```

the URL of Webbridge for IdP to send response to

supported domain of 'brhuff.com' for SSO authentication

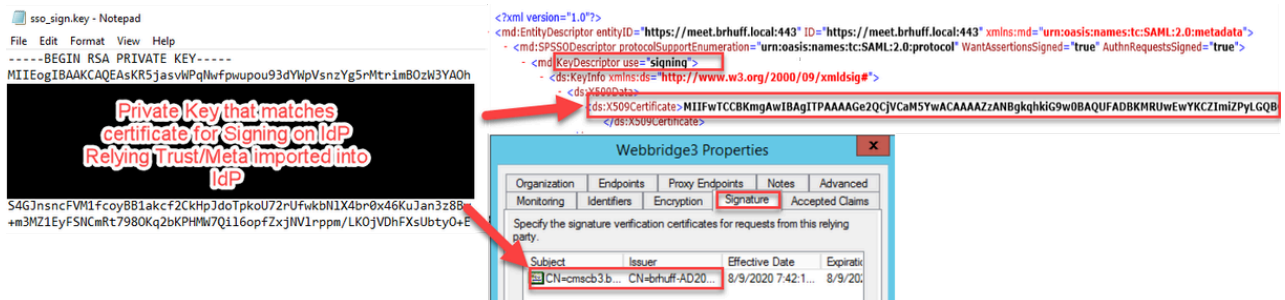
Make sure the LDAP attribute used in ADFS for the Claim rule matches the authenticationIdMapping in the CMS API

Defina sso_sign.key (OPCIONAL)

Esse arquivo deve conter a chave privada do certificado usado para autenticação nos metadados do Webbridge que foram importados para o IdP. O certificado usado para assinatura pode ser definido durante a importação dos metadados Webbridge no ADFS preenchendo o X509Certificate com as informações do certificado na seção <KeyDescriptor use=signing>. Ele também pode ser exibido (e importado) no ADFS na Terceira Parte Confiável Confiável Webbridge em Propriedades > Assinatura.

No próximo exemplo, você pode ver o certificado callbridge (CN=cmscb3.brhuff.local), que foi adicionado aos metadados do Webbridge antes de ser importado para o ADFS. A chave privada inserida em sso_sign.key é a que corresponde ao certificado cmscb3.brhuff.local.

Esta é uma configuração opcional e necessária somente se a intenção for criptografar as Respostas SAML.

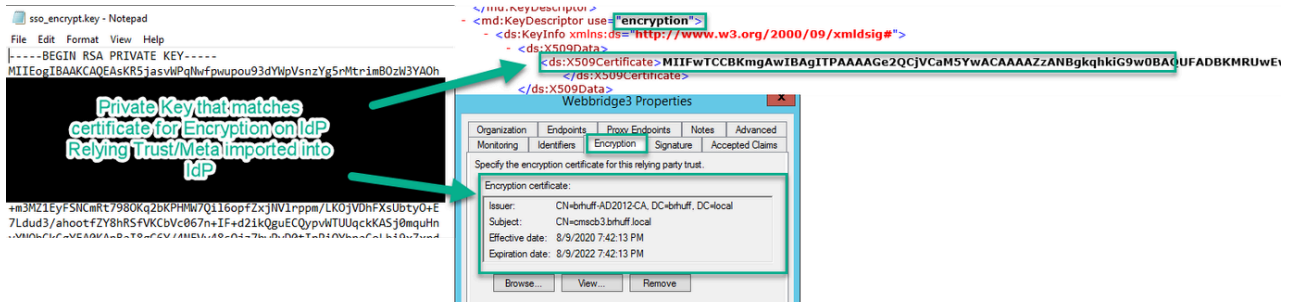


Defina sso_encrypt.key (OPCIONAL)

Esse arquivo deve conter a chave privada do certificado usado para criptografia nos metadados de webbridge que foram importados para o IdP. O certificado usado para criptografia pode ser definido durante a importação dos metadados Webbridge no ADFS preenchendo o X509Certificate com as informações do certificado na seção <KeyDescriptor use=encryption>. Ele também pode ser exibido (e importado) no ADFS na terceira parte confiável Webbridge em Propriedades > Criptografia.

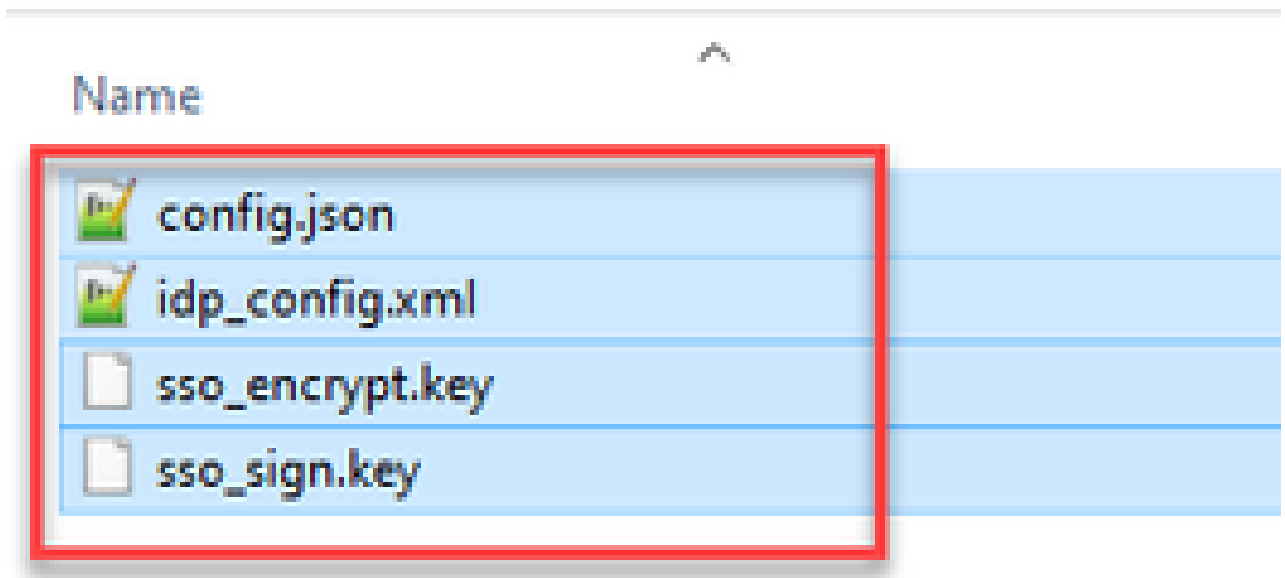
No próximo exemplo, você pode ver o certificado callbridge (CN=cmscb3.brhuff.local), que foi adicionado aos metadados do Webbridge antes de ser importado para o ADFS. A chave privada inserida em 'sso_encrypt.key' é a que corresponde ao certificado cmscb3.brhuff.local.

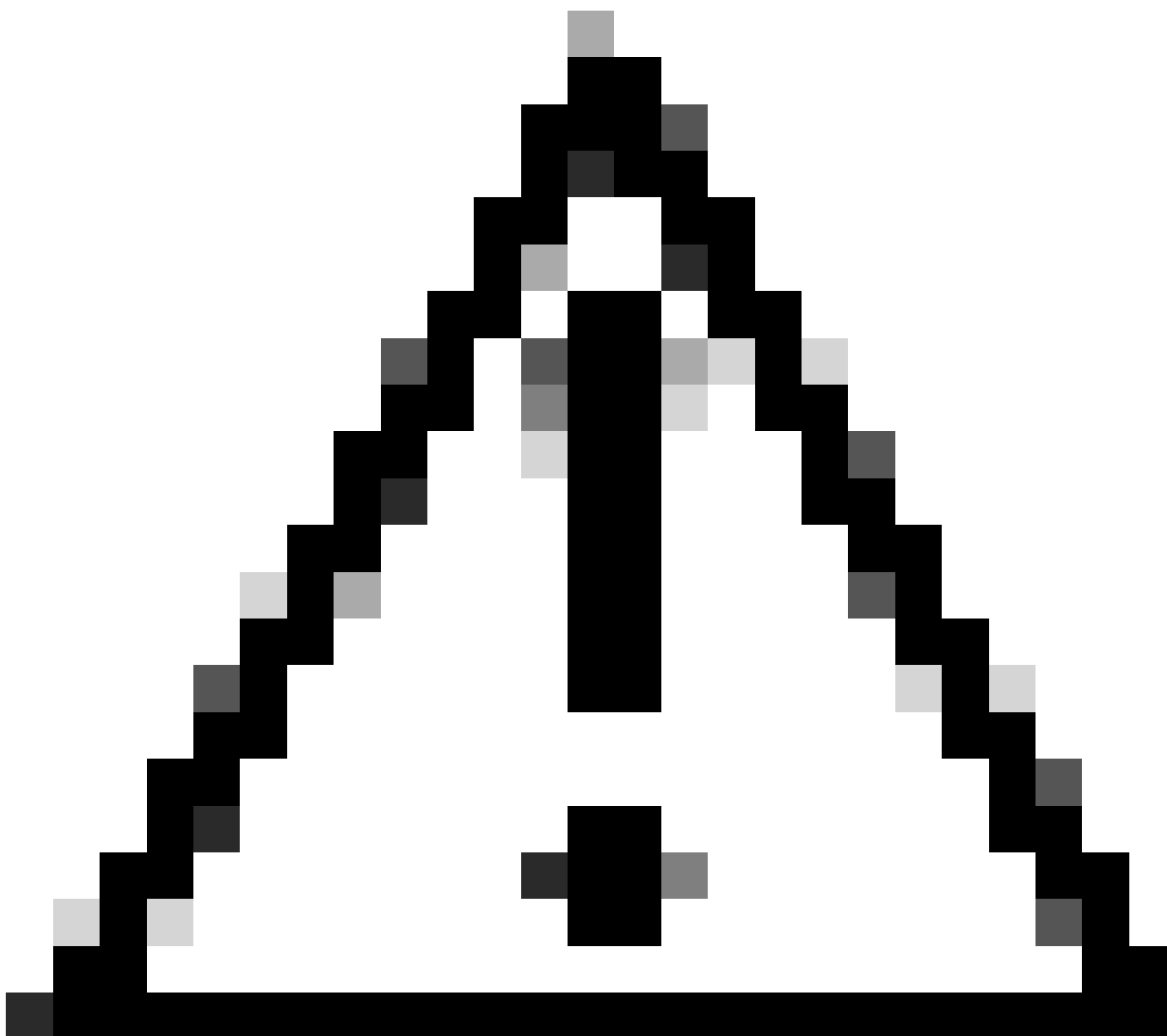
Esta é uma configuração opcional e só será necessária se você pretende criptografar as Respostas SAML.



Criando o arquivo ZIP SSO

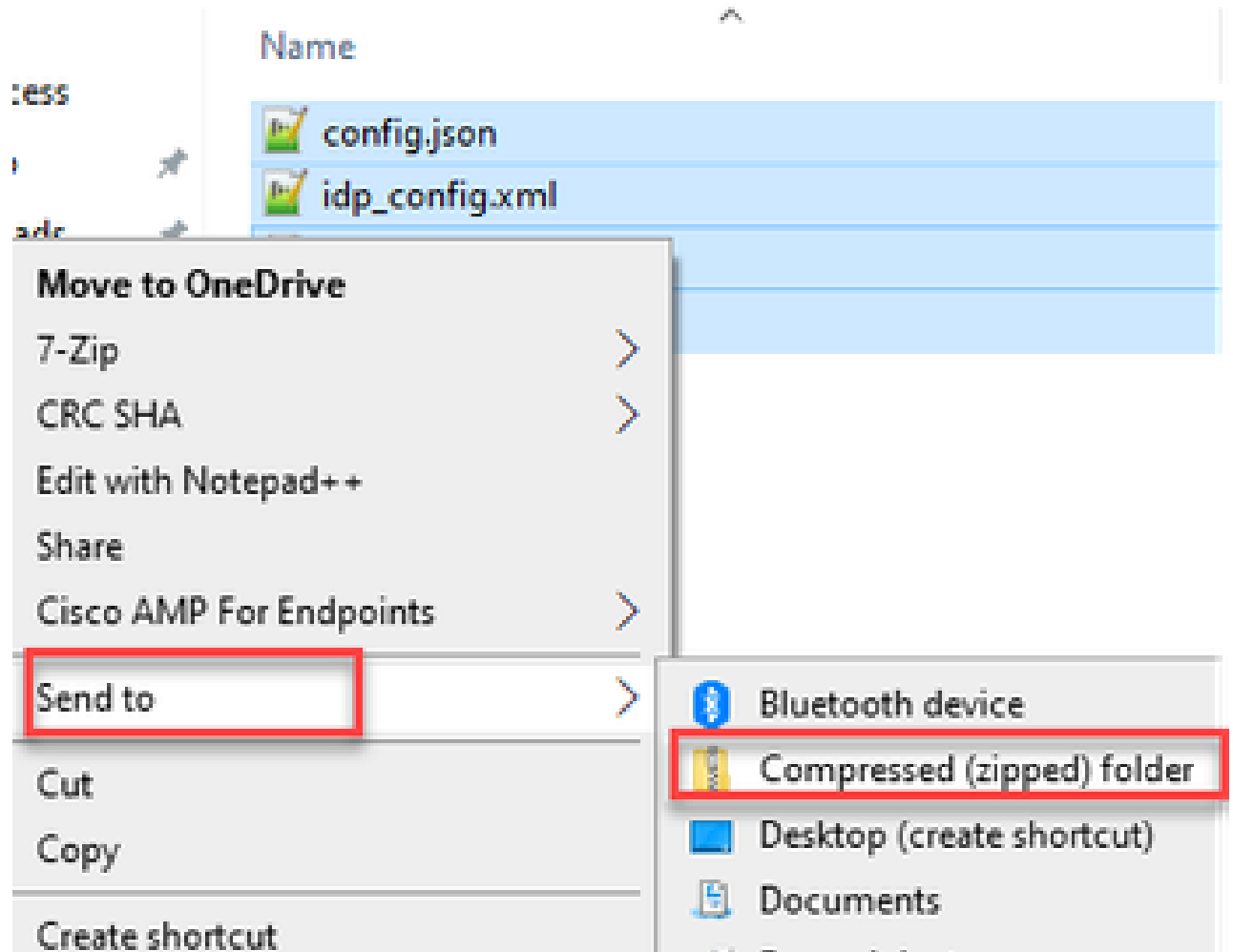
1. Destaque todos os arquivos destinados a serem usados para o arquivo de configuração SSO.



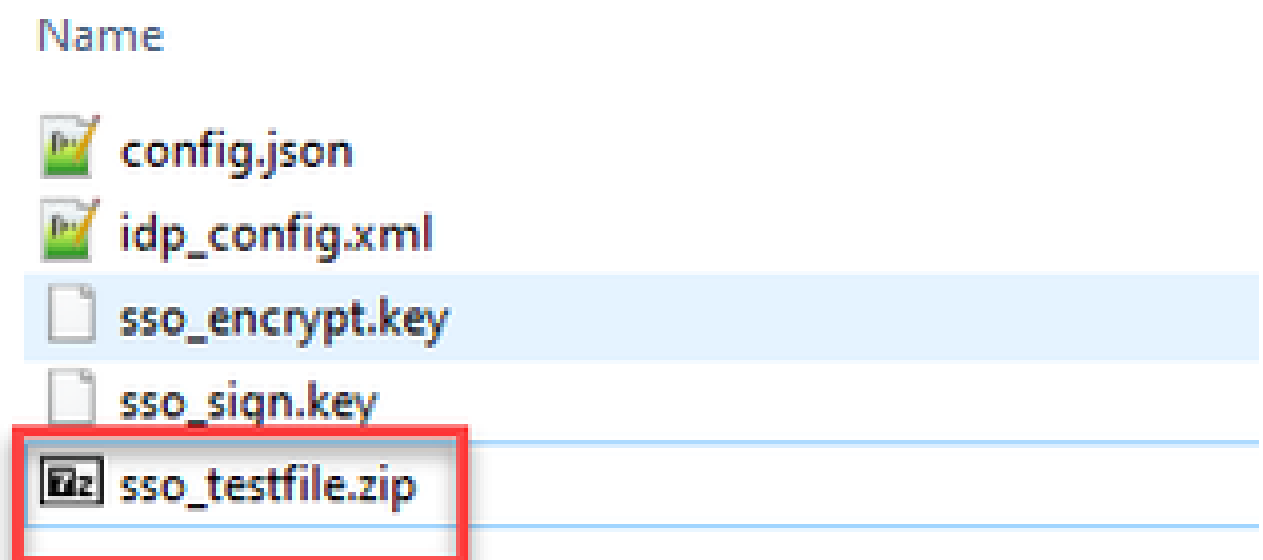


Cuidado: Não compacte a pasta que contém os arquivos porque isso faz com que o SSO não funcione.

2. Clique com o botão direito do mouse nos arquivos de destaque e selecione Enviar para > pasta compactada (zipada).



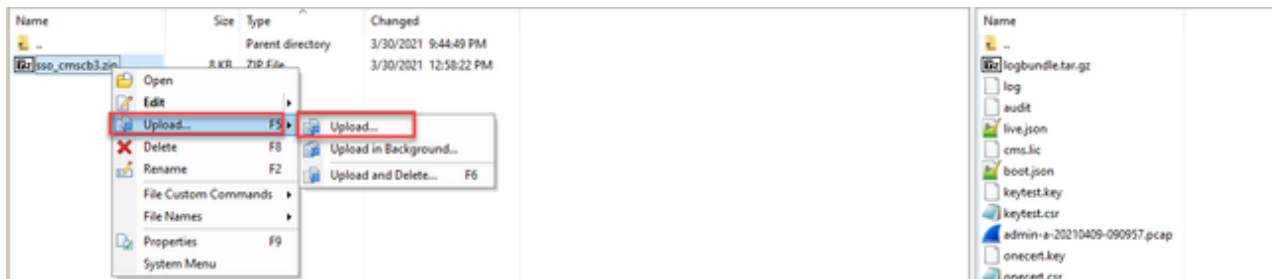
3. Após os arquivos terem sido zipados, renomeie-os com o nome desejado com o prefixo sso_:



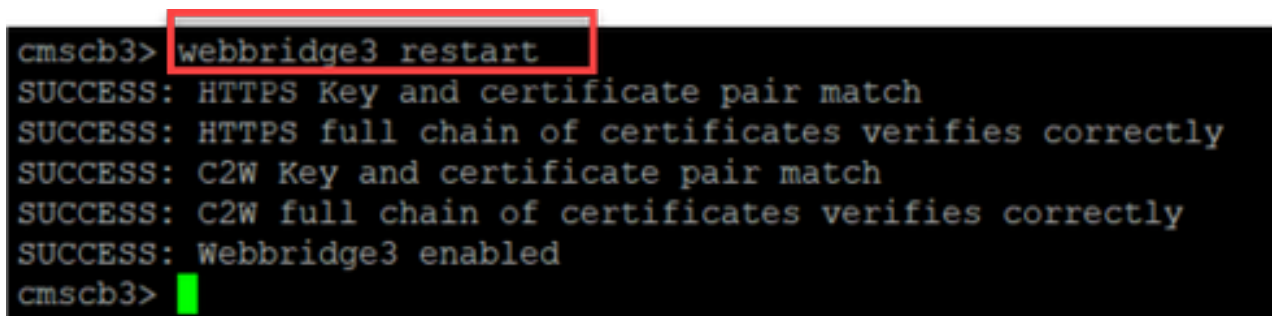
Carregue o(s) arquivo(s) Zip do SSO no Webbridge

Abra um cliente SFTP/SCP, neste exemplo, o WinSCP está sendo usado, e conecte-se ao servidor que hospeda Webbridge3.

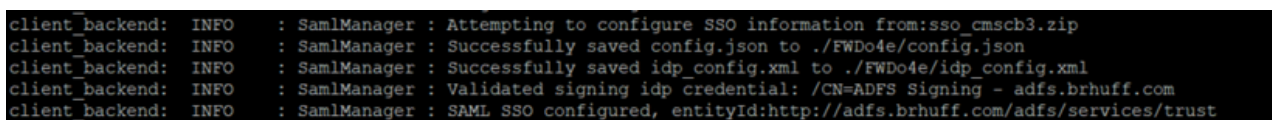
1. No painel esquerdo, navegue até o local onde o arquivo Zip SSO reside e clique com o botão direito do mouse para selecionar upload ou arraste e solte o arquivo.



2. Depois que o arquivo tiver sido completamente carregado no servidor Webbridge3, abra uma sessão SSH e execute o comando `webbridge3 restart`.



3. No syslog, essas mensagens indicam que a ativação de SSO foi bem-sucedida:



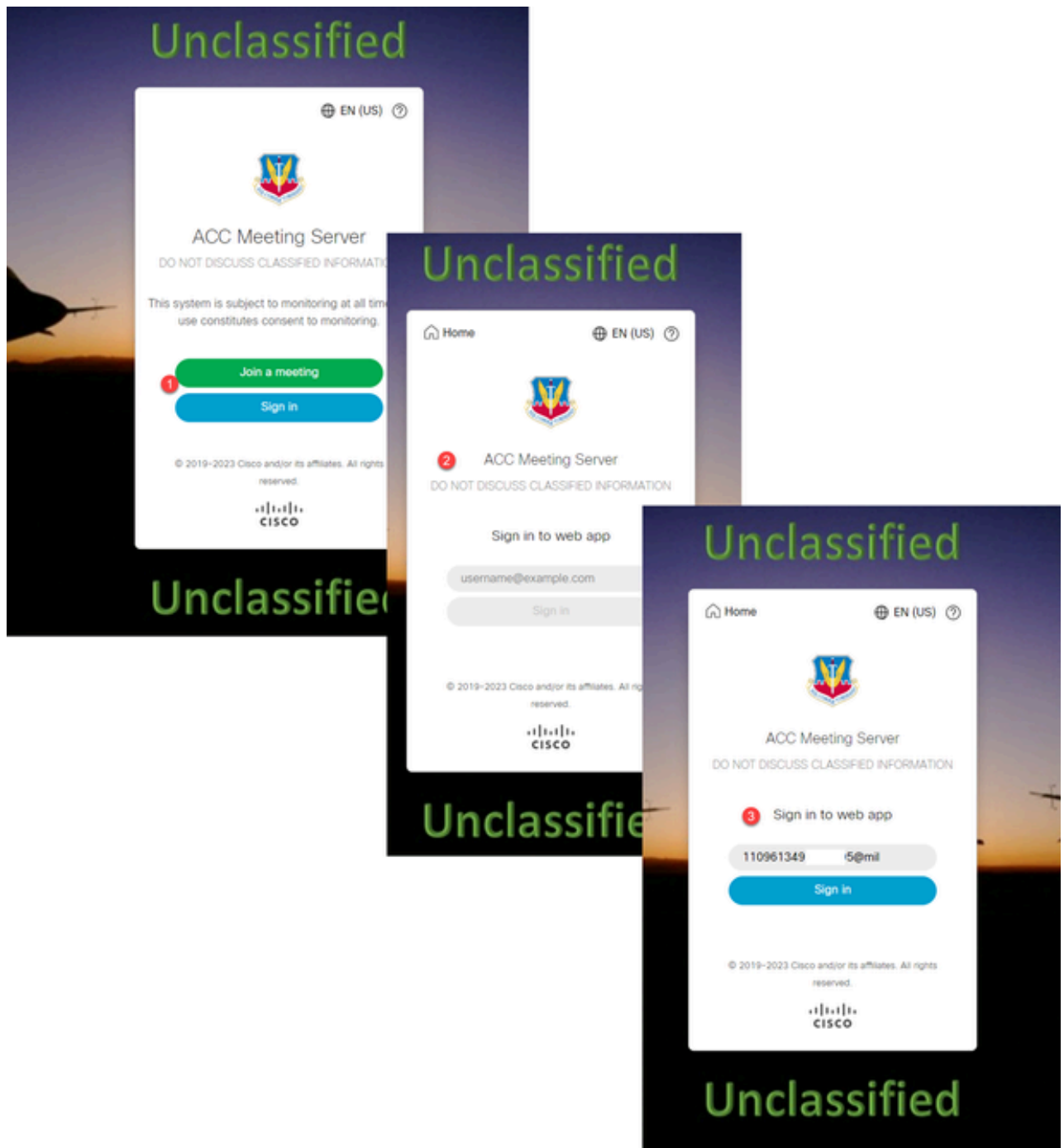
Cartão de acesso comum (CAC)

Um Cartão de Acesso Comum (CAC) é um cartão inteligente que serve como a identificação padrão para militares de serviço ativo, funcionários civis do DoD e pessoal contratado elegível.

Este é o processo de entrada completo para usuários que usam cartões CAC:

1. Ligue o PC e encaixe na placa CAC
2. Faça login (às vezes, selecione o certificado) e digite Pin
3. Abrir navegador
4. Navegue até a URL de ingresso e veja as opções Ingressar em uma reunião ou Entrar
5. Entrar: insira o nome de usuário configurado como `jidMapping` e o Ative Diretory esperará de um login CAC

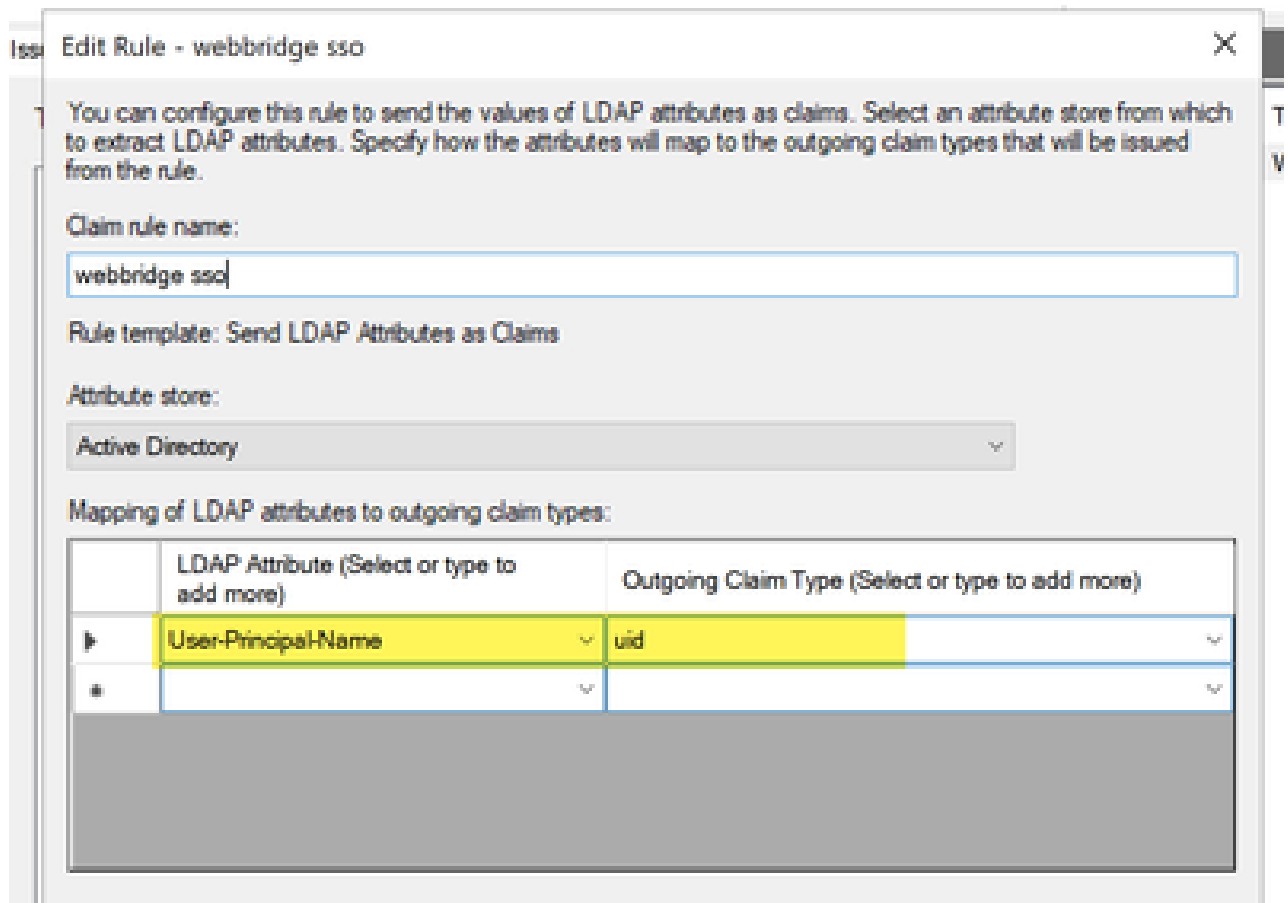
6. Entrar pressionando
7. A página do ADFS aparece brevemente e é preenchida automaticamente
8. O usuário será conectado neste ponto



Configure `jidMapping` (esse é o nome de entrada dos usuários) no `Ldapmapping` da mesma forma que o ADFS usa para a placa CAC. `$userPrincipalName$` por exemplo (diferencia maiúsculas de minúsculas)

Defina também o mesmo atributo LDAP para `authenticationIdMapping` para corresponder ao atributo usado na regra Claim no ADFS.

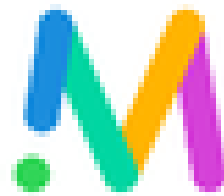
Aqui, a regra de reivindicação mostra que ela enviará `$userPrincipalName$` de volta ao CMS como UID.



Testando o login do SSO via WebApp

Agora que o SSO foi configurado, você pode testar o servidor:

1. Navegue até a URL do Webbridge para o Web App e selecione o botão Entrar.



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

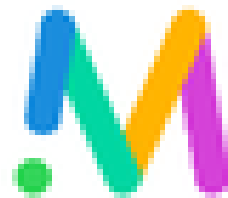
Join a meeting

Sign in

© 2020 Cisco and/or its affiliates. All rights reserved.



2. O usuário recebe a opção de inserir seu nome de usuário (não há opção de senha nesta página).



Cisco Meeting Server

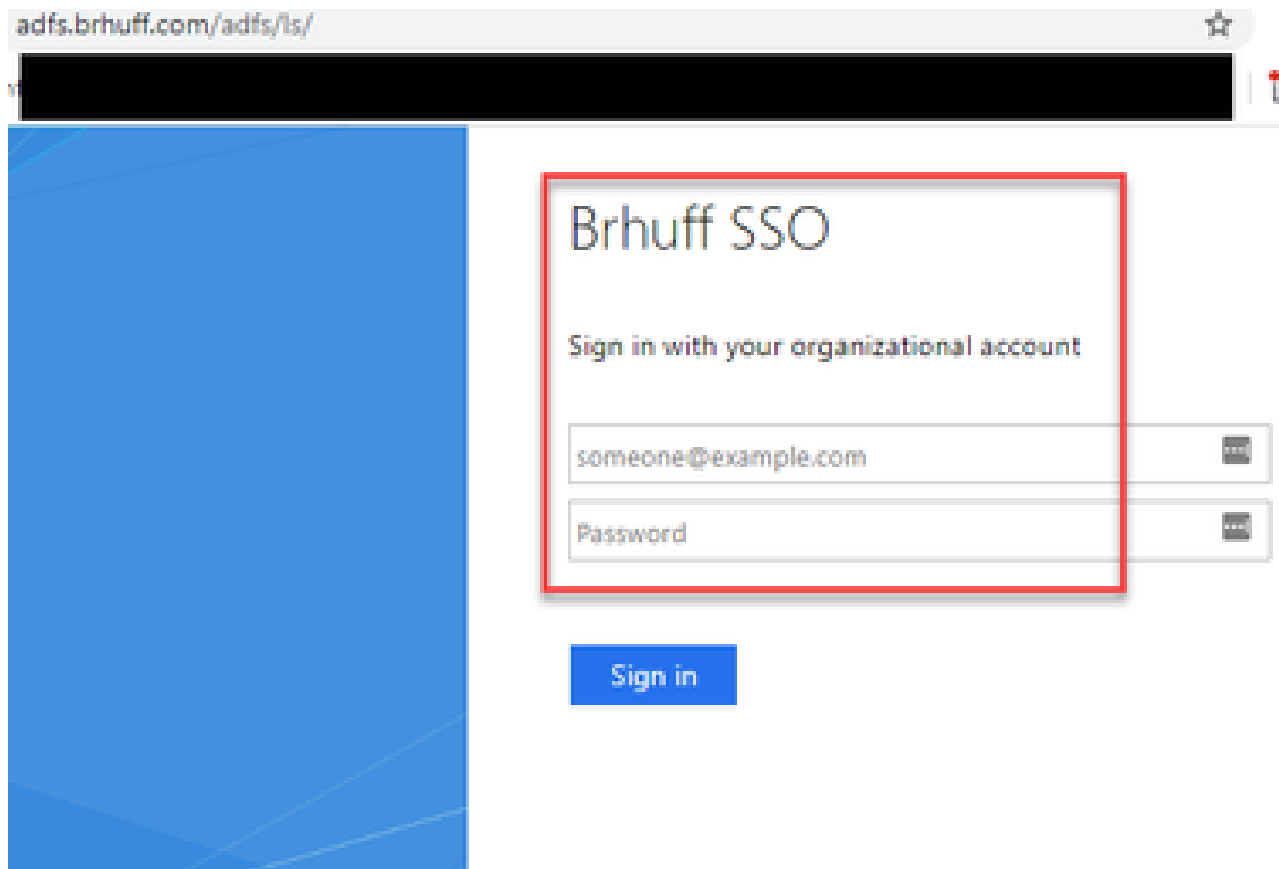
web app

Sign in to web app

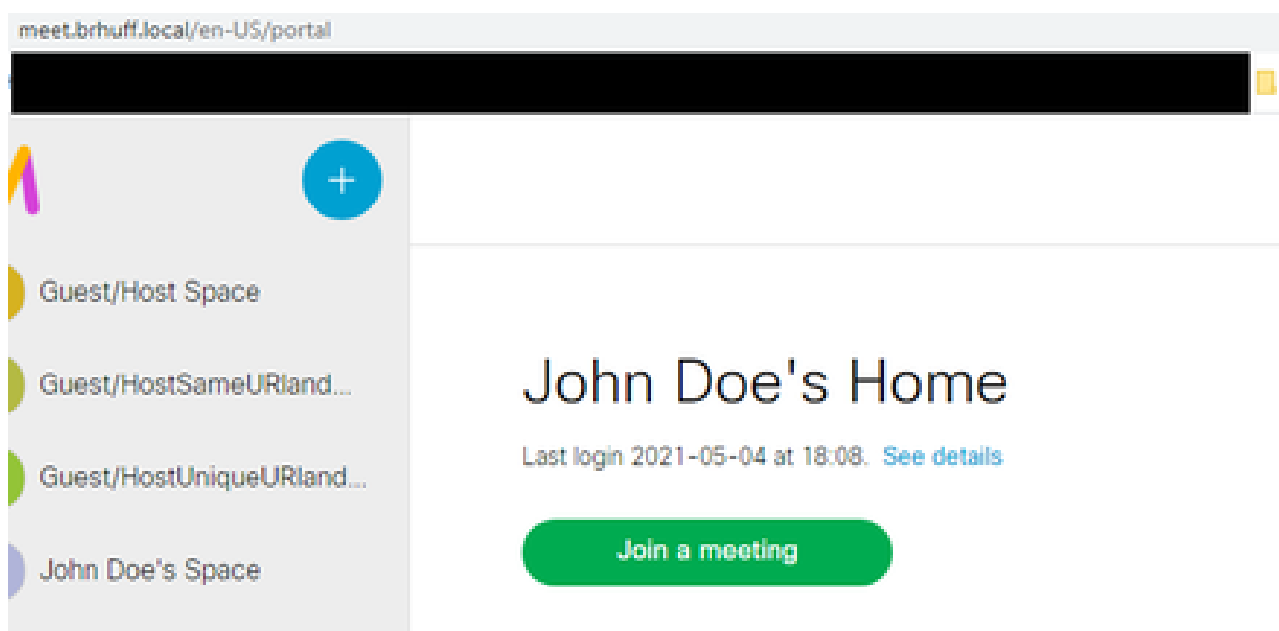
© 2020 Cisco and/or its affiliates. All rights reserved.



3. Em seguida, o usuário é redirecionado para a página ADFS (depois de inserir os detalhes do usuário), na qual ele deve inserir suas credenciais para se autenticar no IdP.



4. O usuário, depois de inserir e validar credenciais com o IdP, é redirecionado com o token para acessar a home page do Web App:



Troubleshooting

Troubleshooting Básico

Para Troubleshooting básico de qualquer problema de SSO:

1. Verifique se os Metadados construídos para a Webbridge3 usada para importar como Confiança Confiável em IdP estão configurados corretamente e se a URL configurada corresponde exatamente como ssoServiceProviderAddress no config.json.
2. Certifique-se de que os metadados fornecidos pelo IdP e compactados no arquivo de configuração do SSO Webbridge3 sejam os mais recentes do IdP, como se houvesse alguma alteração no nome do host do servidor, nos certificados e assim por diante, eles precisam ser reexportados e compactados no arquivo de configuração.
3. Se estiver usando a assinatura e a criptografia de chaves privadas para criptografar dados, certifique-se de que as chaves correspondentes corretas fazem parte do arquivo sso_xxxx.zip que você carregou no webbridge. Se possível, tente testar sem as chaves privadas opcionais para ver se o SSO funciona sem essa opção criptografada.
4. Certifique-se de que config.json esteja configurado com os detalhes corretos para domínios SSO, URL Webbridge3 E mapeamento de autenticação esperado para corresponder da SAMLResponse.

Também seria ideal tentar solucionar o problema sob a perspectiva do registro:

1. Ao navegar para o URL do Webbridge, coloque ?trace=true no final do URL para habilitar um registro detalhado no syslog do CMS. (por exemplo: <https://join.example.com/en-US/home?trace=true>).
2. Execute o syslog follow no servidor Webbridge3 para capturar em tempo real durante o teste ou execute o teste com a opção de rastreamento anexada ao URL e colete o logbundle.tar.gz dos servidores Webbridge3 e CMS Callbridge. Se webbridge e callbridge estiverem no mesmo servidor, será necessário apenas o arquivo logbundle.tar.gz único.

Códigos de falha do Microsoft ADFS

Às vezes, há uma falha no processo SSO que pode resultar em uma falha na configuração do IdP ou em sua comunicação com o IdP. Se estiver usando o ADFS, seria ideal revisar o próximo link para confirmar a falha e tomar medidas corretivas:

[Códigos de Status da Microsoft](#)

Um exemplo disso é:

```
client_backend: ERRO : SamlManager : solicitação de Autenticação SAML _e135ca12-4b87-4443-abe1-30d396590d58 falhou com o motivo:  
urn:oasis:names:tc:SAML:2.0:status:Responder
```

Esse erro indica que, de acordo com a documentação anterior, a falha ocorreu devido ao IdP ou ao ADFS e, portanto, exigiu que o Administrador do ADFS a resolvesse.

Falha ao obter authenticationID

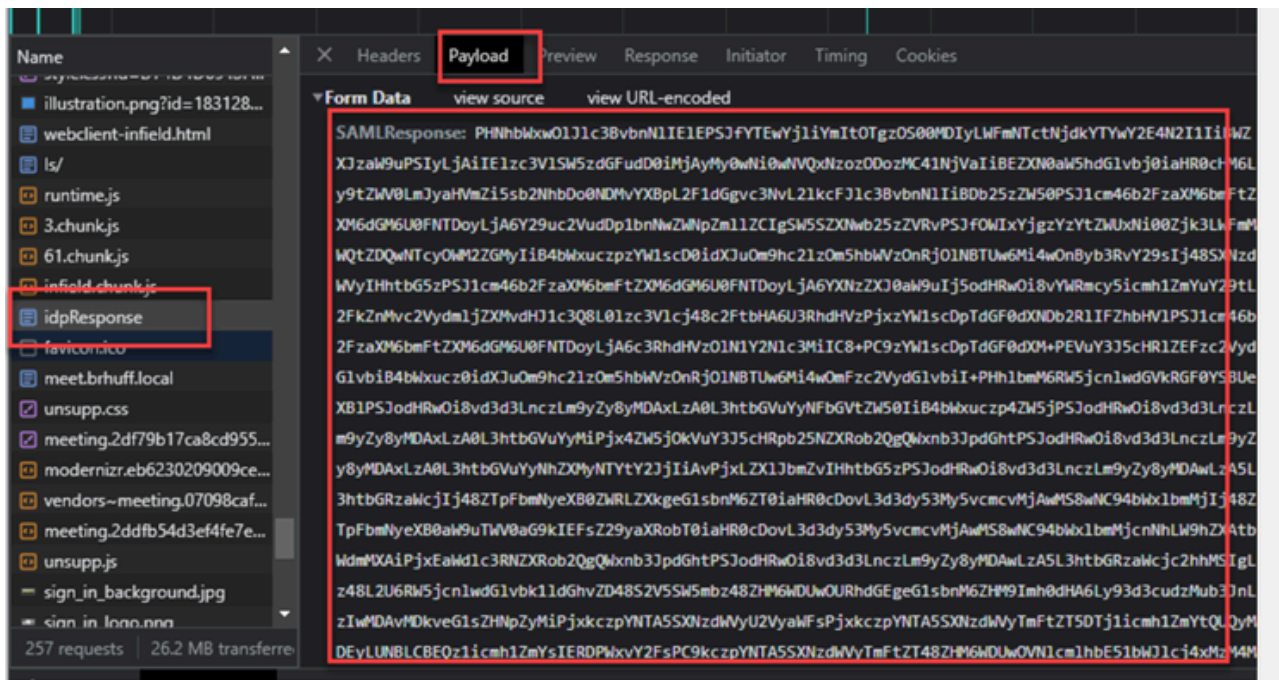
Pode haver casos em que, durante a troca de SAMLResponse de volta do IdP, a Webbridge possa exibir essa mensagem de erro nos logs com uma falha no login via SSO:

```
client_backend: INFO : SamlManager : [57dff9e3-862e-4002-b4fa-683e4aa6922c] Falha ao obter uma authenticationId
```

Isso indica que, ao revisar os dados SAMLResponse passados de volta do IdP durante a troca de autenticação, o Webbridge3 não encontrou um atributo correspondente válido na resposta em comparação com seu config.json para o authenticationId.

Se a comunicação não for criptografada com o uso do sinal e das chaves privadas de criptografia, a Resposta SAML pode ser extraída do Registro de Rede das Ferramentas de Desenvolvedor através de um navegador da Web e decodificada usando base64. Se a resposta for criptografada, você poderá solicitar a resposta SAML descriptografada no lado do IdP.

Na saída de registro de rede das ferramentas do desenvolvedor, também chamada de dados HAR, procure idpResponse na coluna name e selecione Payload para ver a resposta SAML. Como mencionado anteriormente, isso pode ser decodificado usando o decodificador base64.



Ao receber os dados de SAMLResponse, verifique a seção de <AttributeStatement> para localizar os nomes de atributo enviados e, dentro dessa seção, você pode encontrar os tipos de declaração configurados e enviados do IdP. Por exemplo:

```
<InstruçãoAtributo>  
<Attribute Name="<URL for commonname">  
<AttributeValue>testuser1</AttributeValue>  
</Atributo>  
<Attribute Name="<URL para NameID">  
<AttributeValue>testuser1</AttributeValue>  
</Atributo>  
<Attribute Name="uid">  
<AttributeValue>testuser1</AttributeValue>  
</Atributo>  
</AttributeStatement>
```

Revisando os nomes anteriores, você pode verificar o <AttributeName> na seção Instrução de Atributo e comparar cada valor com o que está definido na seção authenticationIdmapping do SSO config.json.

No exemplo anterior, você pode ver que a configuração para authenticationIdMapping NÃO corresponde exatamente ao que é passado e, portanto, resulta na falha de localizar um authenticationId correspondente:

authenticationIdMapping: <http://example.com/claims/NameID>

Para resolver esse problema, há dois métodos possíveis para tentar:

1. A regra de declaração de saída IdP pode ser atualizada para ter uma declaração correspondente que corresponda exatamente ao que está configurado em

authenticationIdMapping do config.json na Webbridge3. (Regra de declaração adicionada no IdP para <http://example.com/claims/NameID>)

OU

2. O config.json pode ser atualizado no Webbridge3 para ter o 'authenticationIdMapping' correspondendo exatamente ao que está configurado como uma das regras de declaração de saída configuradas no IdP. (Ou seja, 'authenticationIdMapping' a ser atualizado para corresponder a um dos nomes de atributo, que pode ser "uid", "<URL>/NameID" ou "<URL>/CommonName". Contanto que corresponda (exatamente) ao valor esperado configurado na API do Callbridge quando passado)

Nenhuma asserção foi aprovada/correspondida na validação

Às vezes, durante a troca da SAMLResponse do IdP, o Webbridge exibe este erro indicando que há uma falha na correspondência da asserção e ignora quaisquer asserções que não correspondem à configuração do servidor:

```
client_backend: ERRO: SamlManager: nenhuma declaração passou na validação
client_backend: INFO : SamlManager : Ignorando asserção sem nós na audiência permitida
```

O que este erro indica é que, ao revisar a SAMLResponse do IdP, o Webbridge falhou em localizar quaisquer asserções correspondentes e, assim, ignorou falhas não correspondentes e, por fim, resultou em um login de SSO com falha.

Para localizar esse problema, é ideal rever a SAMLResponse do IdP. Se a comunicação não for criptografada com o uso do sinal e das chaves privadas de criptografia, a Resposta SAML pode ser extraída do Registro de Rede das Ferramentas de Desenvolvedor através de um navegador da Web e decodificada usando base64. Se a resposta for criptografada, você poderá solicitar a resposta SAML descriptografada no lado do IdP.

Ao revisar os dados de SAMLResponse, observando a seção <AudienceRestriction> da resposta, você pode encontrar todos os públicos aos quais esta resposta está restrita:

```
<Condições NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>
<RestriçãoDoPúblico>
<Audience>https://cisco.example.com</Audience>
</RestriçãoDoPúblico>
</Condições>
```

Usando o valor na seção <Audience> (<https://cisco.example.com>) você pode compará-lo com o [ssoServiceProviderAddress](#) no config.json da configuração Webbridge e validar se é uma correspondência exata. Para este exemplo, você pode ver que o motivo da falha é que o público-alvo NÃO corresponde ao endereço do provedor de serviços na configuração, pois ele tem o anexo :443:

ssoServiceProviderAddress: <https://cisco.example.com:443>

Isso requer uma correspondência exata entre eles para não resultar em uma falha como essa. Para este exemplo, a correção seria um destes dois métodos:

1. O :443 pode ser removido do endereço na seção ssoServiceProviderAddress do config.json, para que corresponda ao campo Audience fornecido na SAMLResponse do IdP.

OU

2. Os metadados OU a terceira parte confiável para Webbridge3 no IdP podem ser atualizados para que :443 sejam anexados à URL. (Se os metadados forem atualizados, eles deverão ser importados novamente como uma Terceira Parte Confiável Confiável no ADFS. No entanto, se você modificar a Terceira Parte Confiável Confiável diretamente do assistente de IdP, ela não precisará ser importada novamente.)

Falha ao Entrar no Aplicativo Web:



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

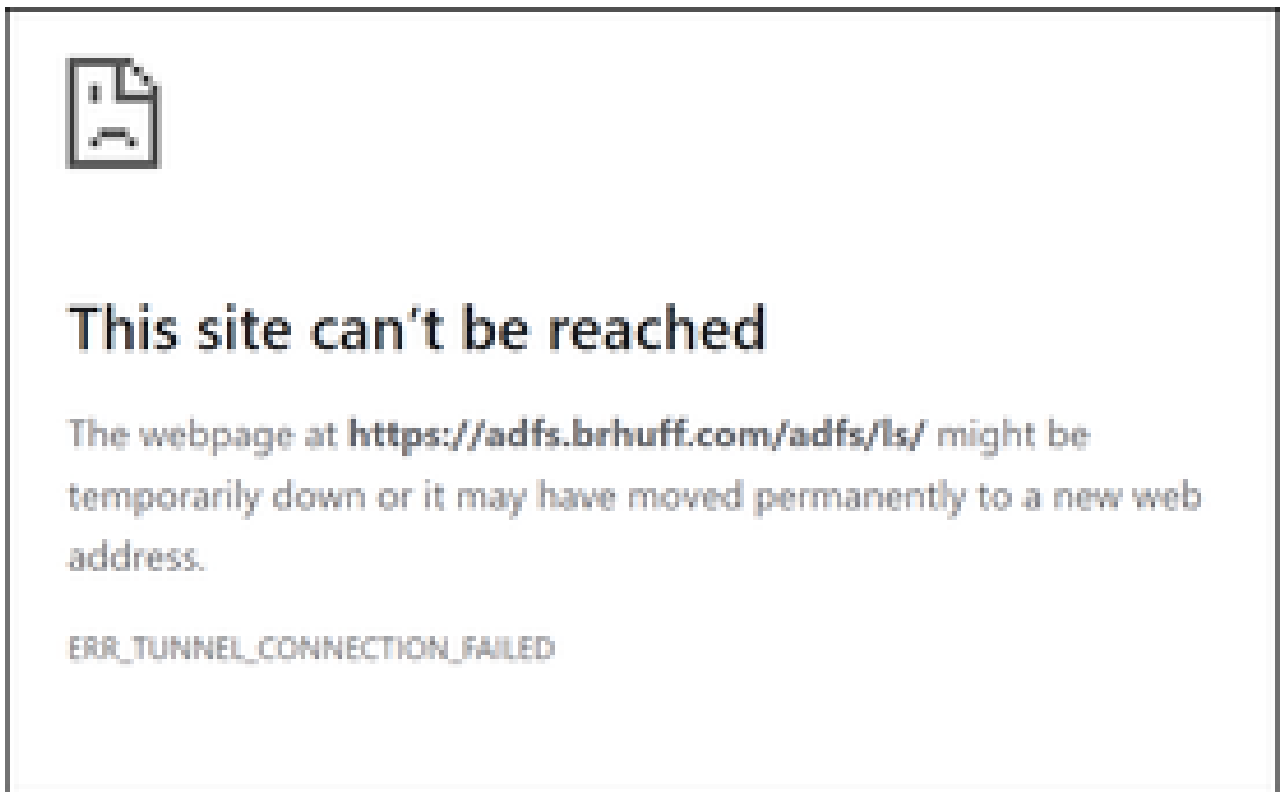
Sign in

 Sign in failed

© 2019-2023 Cisco and/or its affiliates. All rights reserved.



), o webbridge verifica se o domínio usado corresponde a um no arquivo config.json e, em seguida, envia as informações de SAML ao cliente, informando a ele onde se conectar para autenticação. O cliente tentará se conectar ao IdP que está no token SAML. No exemplo abaixo, o navegador mostra esta página porque não pode acessar o servidor ADFS.



Erro no navegador do cliente

Rastreamentos de Webbridge do CMS (enquanto ?trace=true é usado)

Mar 19 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SSO sso_2024.zip correspondido na solicitação de token SAML

Mar 19 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Tentando localizar SSO na Solicitação de Token SAML

Mar 19 10:47:07.930 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Token SAML gerado com êxito

Cenário 2:

O usuário tentou entrar usando um domínio que não está no arquivo zip SSO na página de entrada da webbridge. O cliente envia em uma tokenRequest com uma carga do nome de usuário que o usuário inseriu. O Webbridge interrompe a tentativa de login imediatamente.

Rastreamentos de Webbridge do CMS (enquanto ?trace=true é usado)

18 de março 14:54:52.698 user.err cmscb3-1 client_backend: ERRO: SamlManager:

tentativa de logon SSO inválida

Mar 18 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Falha ao localizar um SSO na Solicitação de Token SAML

Mar 18 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Tentando localizar SSO na Solicitação de Token SAML

Cenário 3:

O usuário inseriu o nome de usuário correto e aparece na página de entrada SSO. O usuário também digita o nome de usuário e a senha corretos aqui, mas ainda obtém Falha ao iniciar sessão

Rastreamentos de Webbridge do CMS (enquanto ?trace=true é usado)

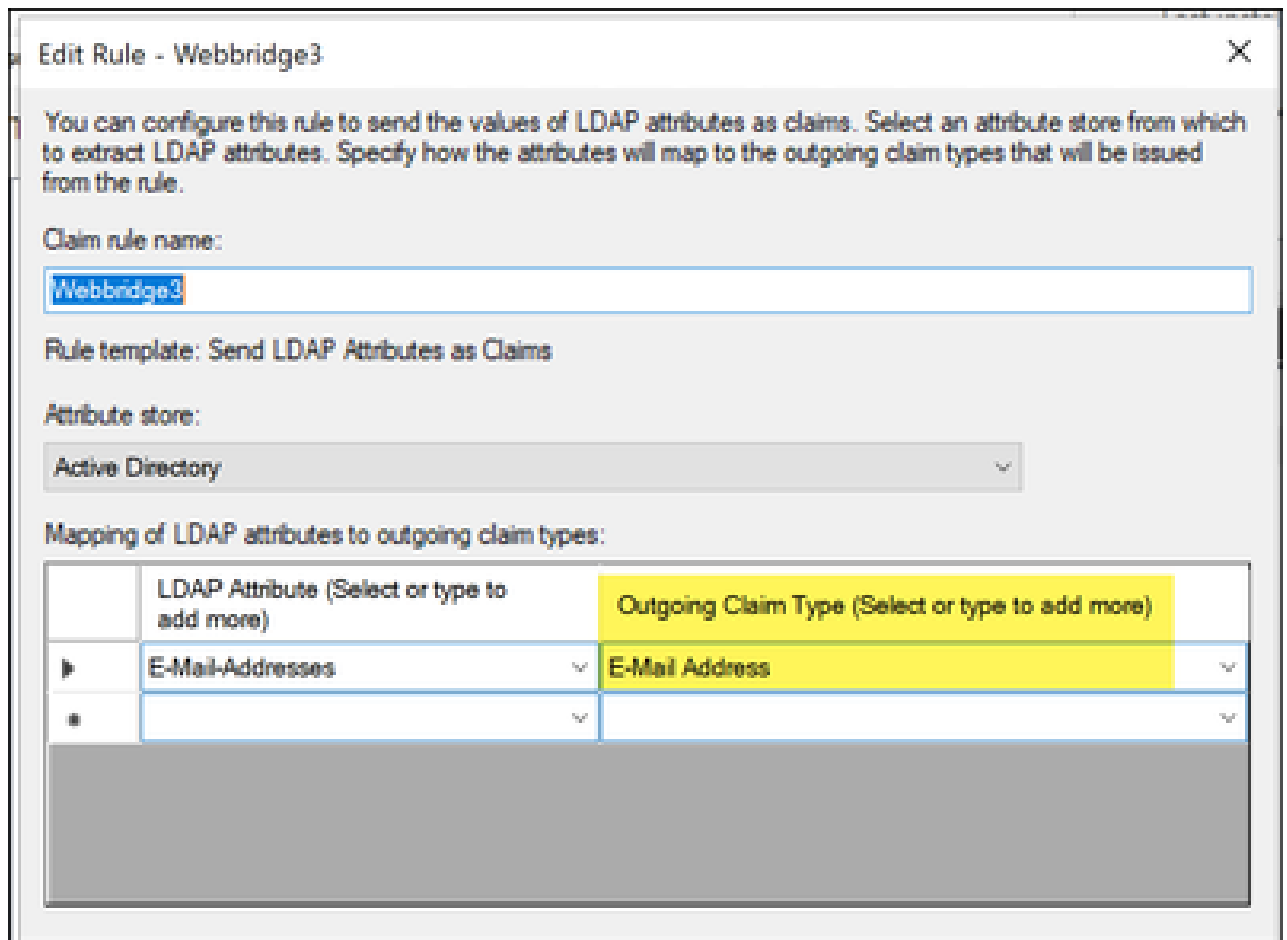
Mar 19 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] SSO sso_2024.zip na solicitação de token SAML

Mar 19 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Tentando localizar SSO em Resposta IDP SAML

Mar 19 16:39:17.720 user.err cmscb3-1 client_backend: ERRO : SamlManager : Nenhum elemento mapeado authenticationId encontrado em Asserções SAML assinadas

Mar 19 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Falha ao obter um authenticationID

A causa para o cenário 3 foi a regra de declaração no IdP estar usando um tipo de declaração que não correspondia ao authenticationIdMapping no arquivo config.json usado no arquivo zip SSO que foi carregado para webbridge. O Webbridge está examinando a resposta SAML e espera que o nome do atributo corresponda ao que está configurado no config.json.



Regra de Declaração no ADFS

```
1 {  
2   "authenticationIdMapping" : "uid",  
3   "ssoServiceProviderAddress" : "https://meet.brhuff.local:443",  
4   "supportedDomains" : ["brhuff.com"]  
5 }
```

exemplo config.json

O nome de usuário não é reconhecido

Cenário 1:

O usuário entrou com o nome de usuário errado (o domínio corresponde ao que está no arquivo zip SSO que foi carregado para webbridge3, mas o usuário não existe)



Blahman Industries

Blahman WebApp

Sign in to web app

steve@brhuff.com

Sign in

 Username is not recognized

© 2019-2023 Cisco and/or its affiliates. All rights reserved.



no mapeamento LDAP do CMS não corresponde ao atributo LDAP configurado usado para a regra de declaração no ADFS. A linha abaixo que diz "AuthenticationID:darmckin@brhuff.com" está dizendo que o ADFS tem uma regra de declaração configurada com o atributo que obtém darmckin@brhuff.com do Ative Directory, mas a AuthenticationID no CMS API > Users mostra que espera o darmckin. No CMS ldapMappings, o AuthenticationID é configurado como \$sAMAccountName\$, mas a regra de declaração no ADFS é configurada para enviar o E-Mail-Addresses, portanto, isso não corresponde.

Como corrigir isso:

Execute um dos seguintes procedimentos:

1. Altere o AuthenticationID no mapeamento ldp do CMS para corresponder ao que é usado na regra Claim no ADFS e execute uma nova sincronização
2. Alterar o Atributo LDAP usado na regra de Declaração ADFS para corresponder ao que está configurado no mapeamento ldapdo CMS

Related objects: </api/v1/ldapMappings>

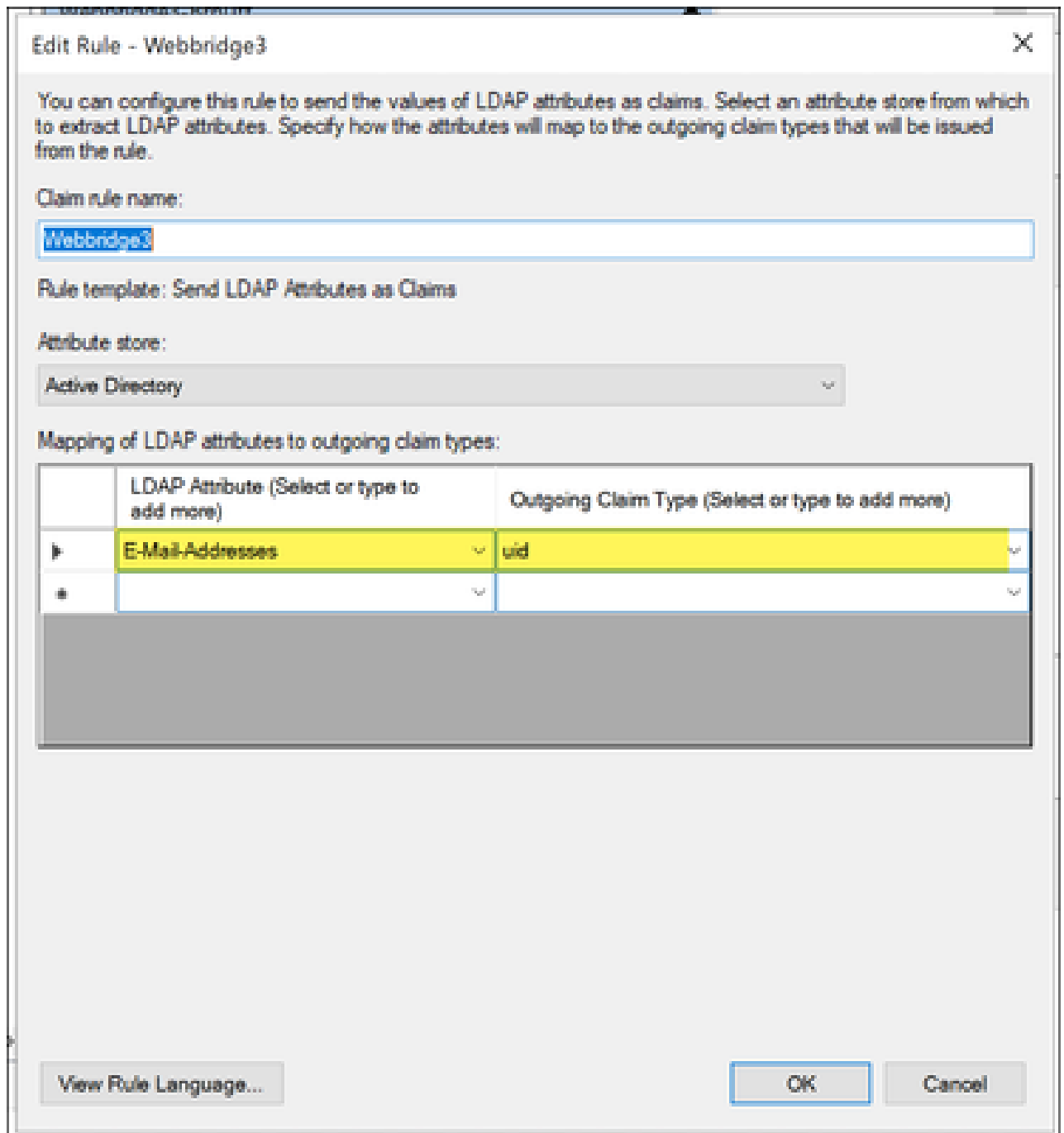
Table view XML view

Object configuration	
jidMapping	\$sAMAccountName\$@brhuff.com
nameMapping	\$cn\$
cdrTagMapping	
coSpaceNameMapping	\$cn\$'s Space
coSpaceUriMapping	\$sAMAccountName\$.space
coSpaceSecondaryUriMapping	\$extensionAttribute12\$
coSpaceCallIdMapping	
authenticationIdMapping	\$sAMAccountName\$

API LDAPMapping

Object configuration	
userId	darmckin@brhuff.com
name	Darren McKinnon
email	darmckin@brhuff.com
authenticationId	darmckin
userProfile	d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3

Exemplo de Usuário de API



Regra de Declaração do ADFS

Log do Webbridge mostrando o exemplo de log de trabalho em. Exemplo gerado com ?trace=true no URL de junção:

```
Mar 18 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] SSO sso_2024.zip na solicitação de token SAML
```

```
Mar 18 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Tentando localizar SSO em Resposta IDP SAML
```

```
Mar 18 14:24:01.101 user.info cmscb3-1 client_backend: INFO : SamlManager :
```

[7979f13c-d490-4f8b-899c-0c82853369ba] AuthenticationID:darmckin@brhuff.com obtida com êxito

Mar 18 14:24:01.102 user.info cmscb3-1 host:servidor: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequestReceived para a id de conexão=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0 272-42a1-b125-136fdf5612a5 (usuário=darmckin@brhuff.com)

18 de março 14:24:01.130 user.info cmscb3-1 host:servidor: INFO: solicitação de login bem-sucedida de darmckin@brhuff.com

Mar 18 14:24:01.130 user.info cmscb3-1 host:servidor: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] emissor do ID JWT e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

Mar 18 14:24:01.132 user.info cmscb3-1 host:servidor: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] enviando resposta auth (jwt length=1064, connection=64004556-faea-479f-aabe-691e17783aa5)

Mar 18 14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Rastreamento:7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25.247 - [18/Mar/2024:18:24:01 +00 00] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "<https://ads.brhuff.com/>" http_user_agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, como Gecko) Chrome/122.0.0.0 Safari/537.36" para upstream 192.0.0.2.2:9000: upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

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.