

Configuración y solución de problemas del SSO de WebApp en CMS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Diagrama de la red](#)

[Instalación y configuración inicial de ADFS](#)

[Asignar usuarios de CMS a proveedor de identidad \(IdP\)](#)

[Crear XML de metadatos de Webbridge para IdP](#)

[Importar metadatos para Webbridge en Identity Provider \(IdP\)](#)

[Creación de reglas de reclamación para el servicio Webbridge en el IdP](#)

[Crear archivo ZIP de archivo SSO para Webbridge:](#)

[Obtenga y configure idp_config.xml](#)

[Cree el archivo config.jsonFile con contenido](#)

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

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

[Creación del archivo ZIP de SSO](#)

[Cargue los archivos zip de SSO en Webbridge](#)

[Tarjeta de acceso común \(CAC\)](#)

[Prueba de SSO Inicie sesión mediante WebApp](#)

[Resolución de problemas](#)

[Resolución de problemas básicos](#)

[Códigos de error de Microsoft ADFS](#)

[Error al obtener authenticationID](#)

[No se superó ni coincidió ninguna afirmación en la validación](#)

[Error de inicio de sesión en aplicación web:](#)

[Escenario 1:](#)

[Escenario 2:](#)

[Escenario 3:](#)

[El nombre de usuario no se reconoce](#)

[Escenario 1:](#)

[Escenario 2:](#)

[Ejemplo de registro de Webbridge que muestra el registro de trabajo. Ejemplo generado mediante ?trace=true en la URL de combinación:](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y solucionar problemas de la implementación de Cisco Meeting Server (CMS) Web App de Single Sign On (SSO).

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- CMS Callbridge versión 3.1 o posterior
- CMS Webbridge versión 3.1 o posterior
- Servidor de directorio activo
- Identificar proveedor (IdP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.


Background

CMS 3.1 y versiones posteriores han introducido la capacidad para que los usuarios inicien sesión mediante un SSO sin necesidad de introducir su contraseña cada vez que el usuario inicia sesión, ya que se crea una única sesión con el proveedor de identidad.

Esta función utiliza el lenguaje de marcado de aserción de seguridad (SAML) versión 2.0 como mecanismo de SSO.

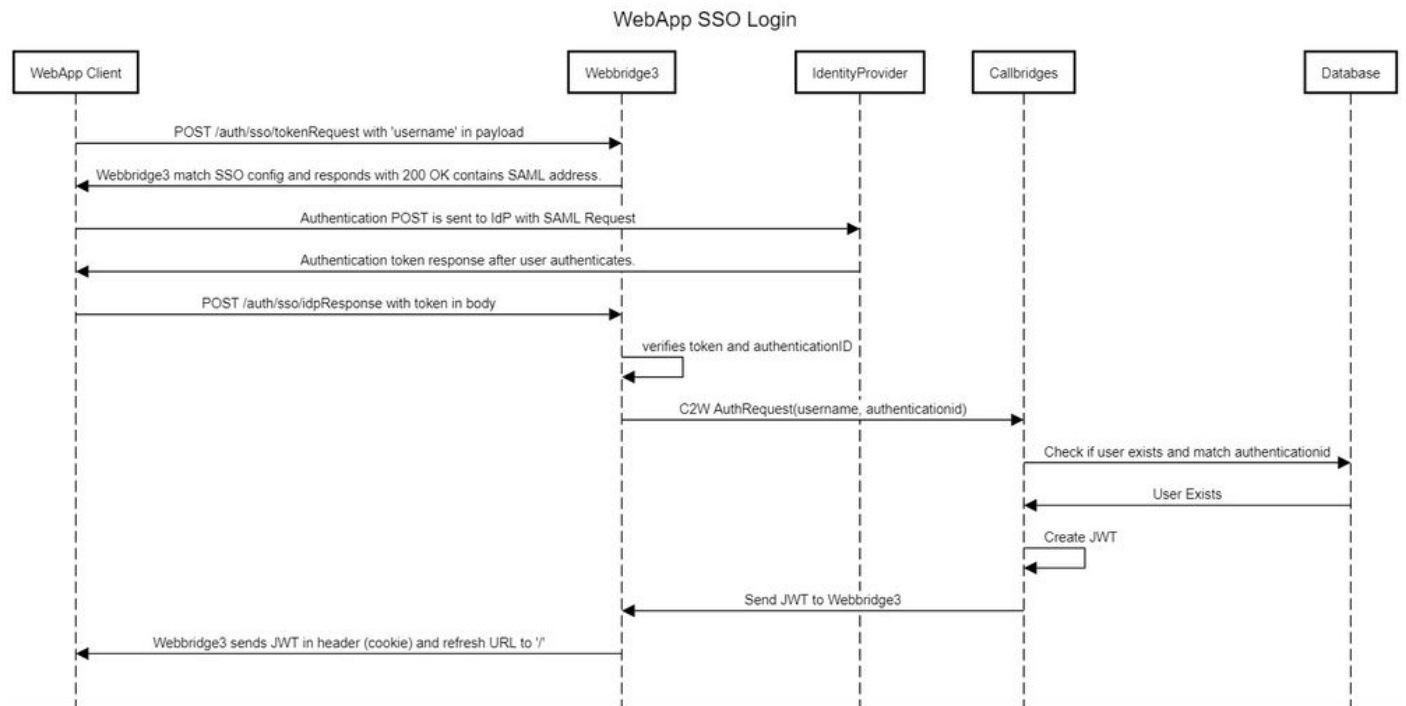
 Nota: CMS sólo admite enlaces HTTP-POST en SAML 2.0 y rechaza cualquier proveedor

 de identidad sin enlaces HTTP-POST disponibles.

 Nota: Cuando SSO está habilitado, la autenticación LDAP básica ya no es posible.

Configurar

Diagrama de la red



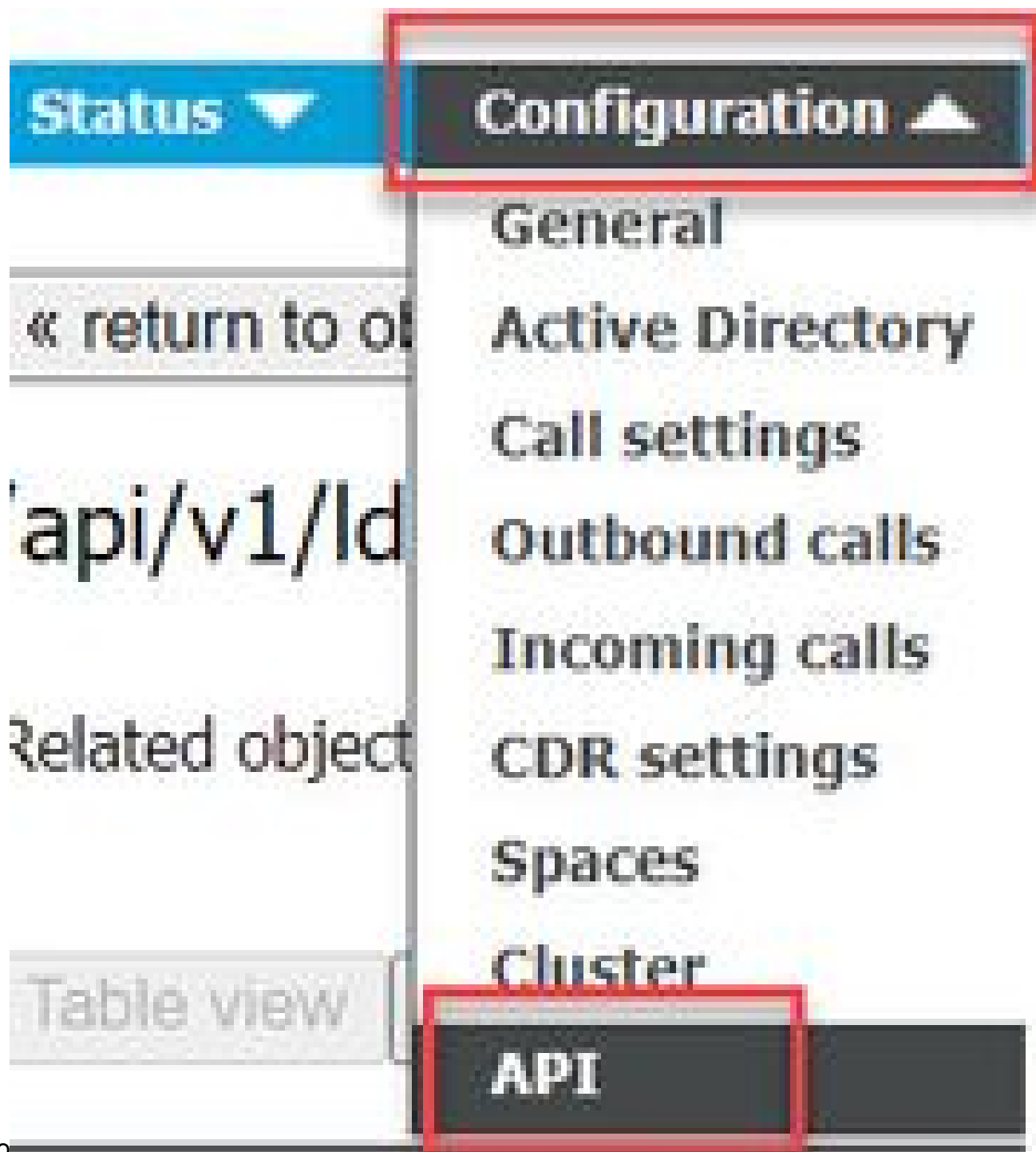
Instalación y configuración inicial de ADFS

Este escenario de implementación utiliza Microsoft Active Directory Federation Services (ADFS) como proveedor de identidad (IdP) y, por tanto, se recomienda tener un ADFS (o IdP previsto) instalado y en ejecución antes de esta configuración.

Asignar usuarios de CMS a proveedor de identidad (IdP)

Para que los usuarios obtengan una autenticación válida, deben ser asignados en la Interfaz de programación de aplicaciones (API) para un campo de correlación proporcionado por IdP. La opción utilizada para esto es la `authenticationIdMapping` en `IdapMapping` de la API.

1. Navegue hasta Configuración > API en la GUI de administración web de CMS



2. Localice la asignación LDAP existente (o creando una nueva) en `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. En el objeto ldapMapping seleccionado, actualice el authenticationIdMapping al atributo LDAP que se pasa desde el IdP. En el ejemplo, la opción \$sAMAccountName se utiliza como atributo LDAP para la asignación.

/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

 Nota: El authenticationIdMapping es utilizado por callbridge/base de datos para validar la reclamación enviada desde el IdP en SAMLResponse y proporcionar al usuario un token web JSON (JWT).

4. Realice una sincronización LDAP en el ldapSource asociado con el ldapMapping modificado recientemente:

Por ejemplo:

/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. Una vez completada la sincronización LDAP, navegue en la API de CMS en Configuración > api/v1/users y seleccione un usuario que se importó y verifique que authenticationId se haya llenado correctamente.

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

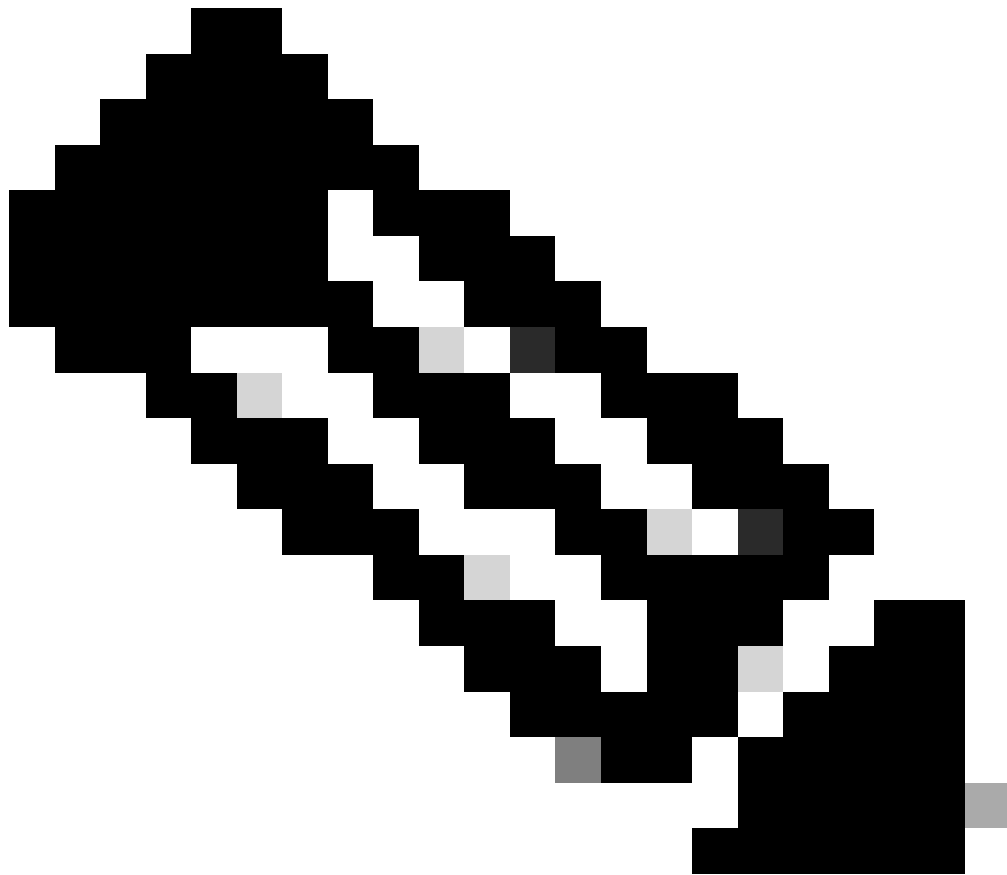
Crear XML de metadatos de Webbridge para IdP

Microsoft ADFS permite importar un archivo XML de metadatos como tercero de confianza para identificar el proveedor de servicios que se está utilizando. Existen algunas formas de crear el archivo XML de metadatos para este fin, sin embargo, hay algunos atributos que deben estar presentes en el archivo:

Ejemplo de metadatos de Webbridge con valores requeridos:

```
<?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: Se trata de la dirección del servidor Webbridge3 (FQDN/nombre de host) y el puerto asociado al que pueden acceder los exploradores para los usuarios.



Nota: Si hay varios Webbridges utilizando una sola URL, esta debe ser una dirección de balanceo de carga.

2. Location: Ubicación en la que HTTP-POST AssertionConsumerService corresponde a la dirección de Webbridge. Esto es lo que indica al IdP dónde redirigir a un usuario autenticado después de iniciar sesión. Debe establecerse en la URL idpResponse: <https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponse>. Por ejemplo, <https://join.example.com:443/api/auth/sso/idpResponse>.
3. OPTIONAL - Public Key for Signing - ésta es la clave pública (certificado) para la firma, que es utilizada por el IdP para verificar la AuthRequest de Webbridge. Esto DEBE coincidir con la clave privada 'sso_sign.key' en el paquete SSO cargado en Webbridge para que el IdP pueda utilizar la clave pública (certificado) para verificar la firma. Puede utilizar un certificado existente de la implementación. Abra el certificado en un archivo de texto y copie el contenido en el archivo de metadatos de Webbridge. Utilice la clave coincidente del certificado utilizado en el archivo sso_xxxx.zip como el archivo sso_sign.key.

4. OPCIONAL - Public Key for Encryption - ésta es la clave pública (certificado) que el IdP utiliza para cifrar la información SAML enviada de vuelta a Webbridge. Esto DEBE coincidir con la clave privada 'sso_encrypt.key' en el paquete SSO cargado en Webbridge, de modo que Webbridge pueda descifrar lo que se devuelve mediante IdP. Puede utilizar un certificado existente de la implementación. Abra el certificado en un archivo de texto y copie el contenido en el archivo de metadatos de Webbridge. Utilice la clave coincidente del certificado utilizado en el archivo sso_xxxx.zip como archivo sso_encrypt.key.

Ejemplo de metadatos de Webbridge que se van a importar en IdP con datos de clave pública (certificado) opcionales:

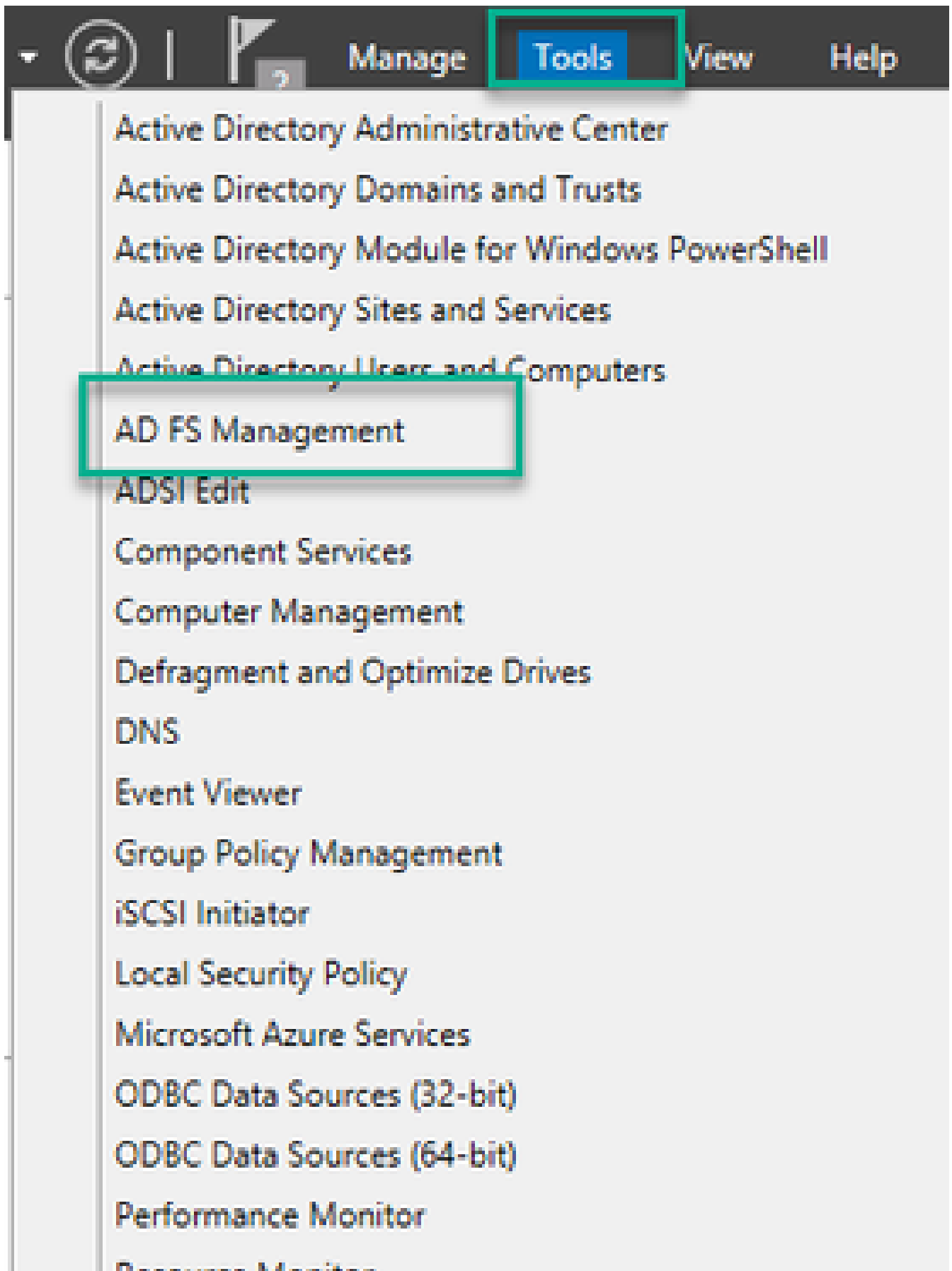
```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
- <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
- <md:KeyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:X509Data>
- <ds:X509Certificate>MIIFwTCCBmqAwIBAgIT[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>MIIFwTCCBmqAwIBAgIT[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>
```

conservado

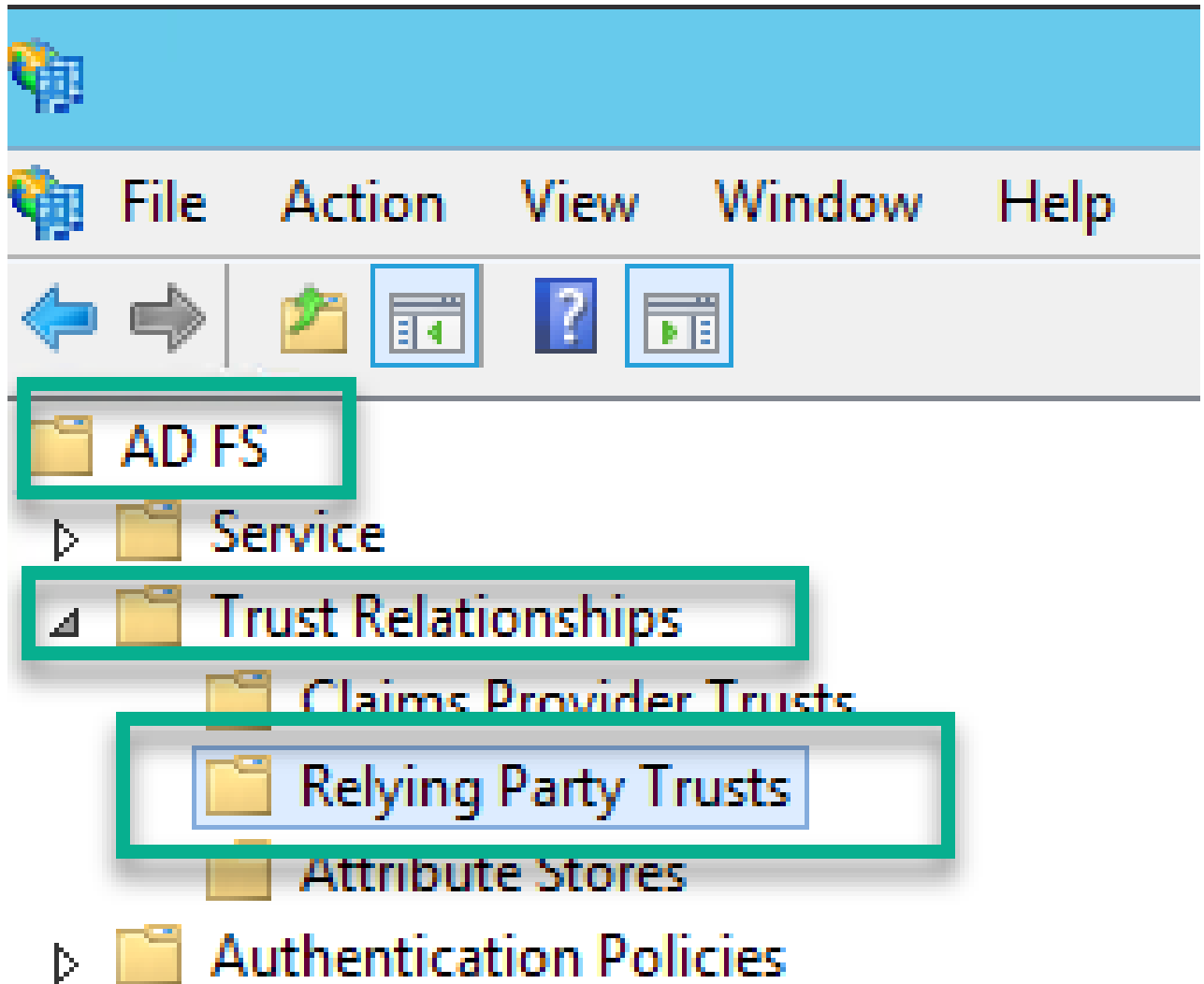
Importar metadatos para Webbridge en Identity Provider (IdP)

Una vez creado el archivo XML de metadatos con los atributos adecuados, el archivo se puede importar al servidor de Microsoft ADFS para crear un tercero de confianza de confianza.

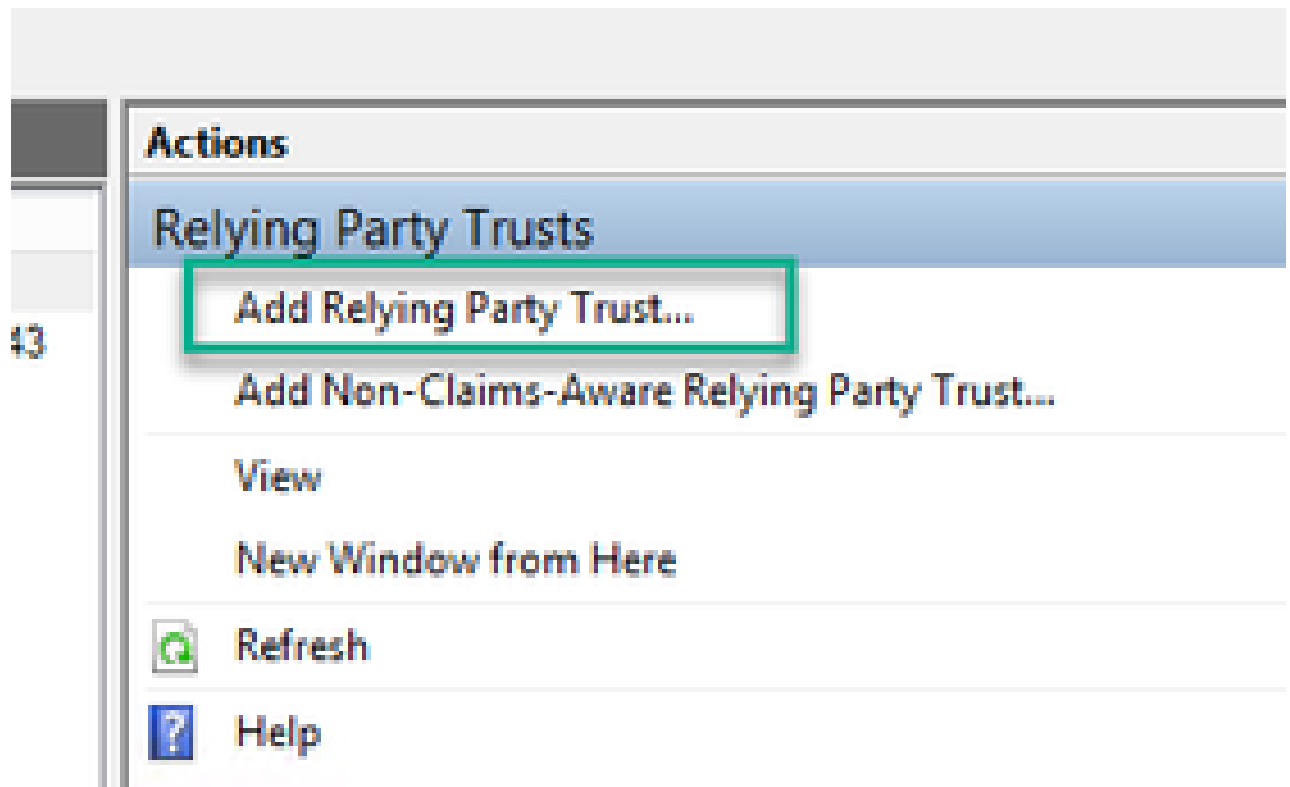
1. Escritorio remoto en el servidor de Windows que aloja los servicios ADFS
2. Abra la Consola de administración de AD FS, a la que normalmente se puede tener acceso a través del Administrador del servidor.



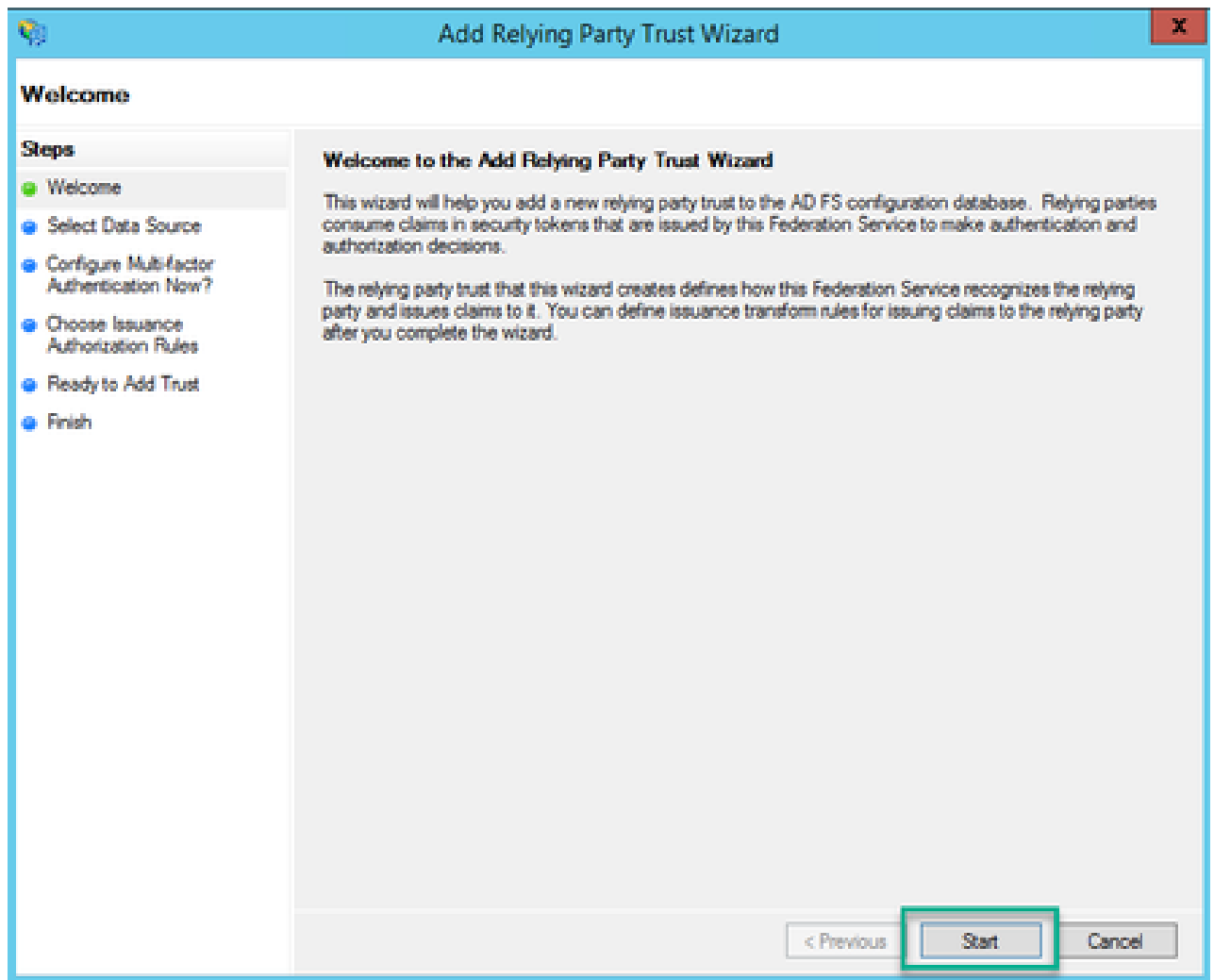
3. Una vez en la consola de administración de ADFS, navegue hasta ADFS > Relaciones de confianza > Confianza de usuario de confianza en el panel izquierdo.



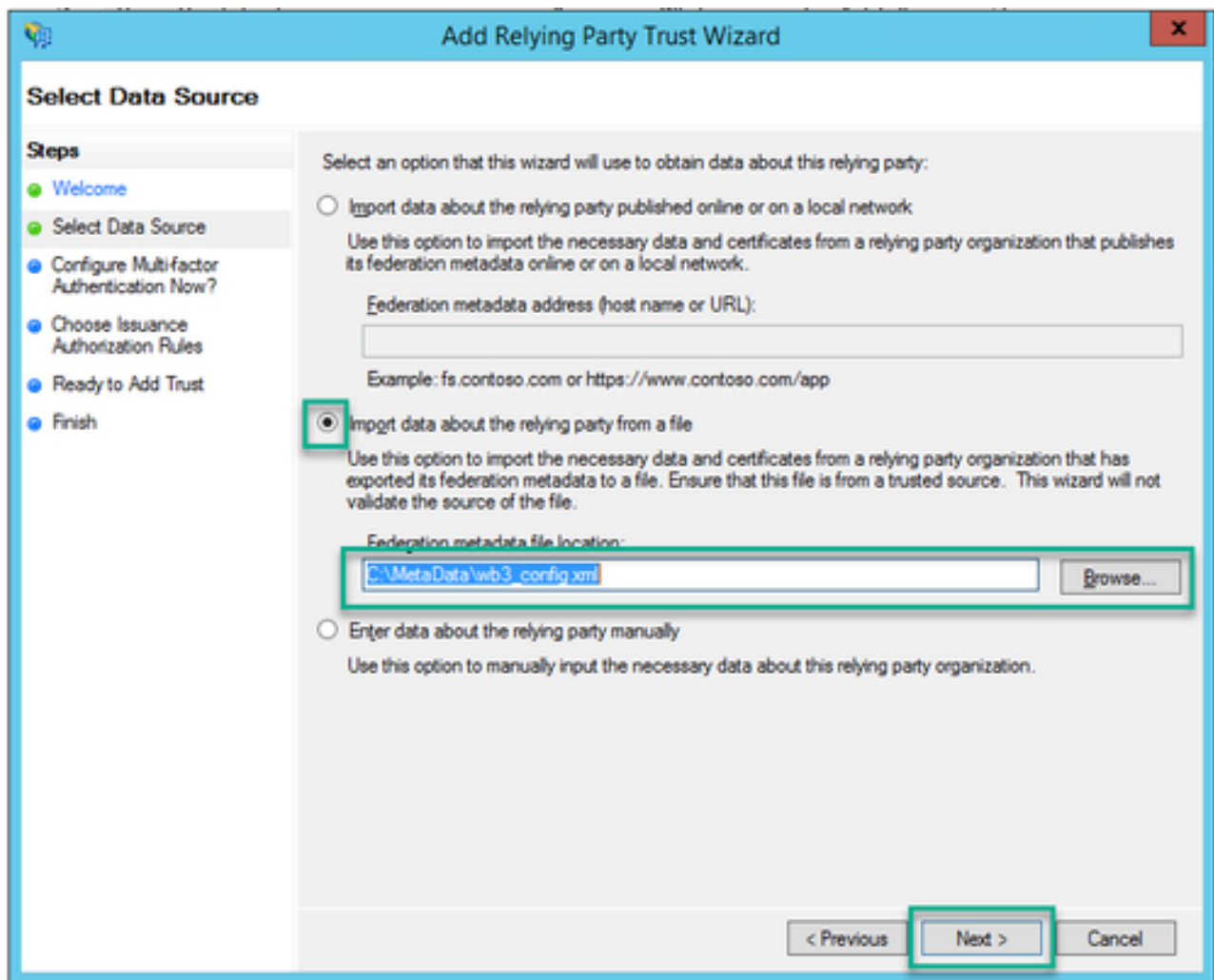
4. En el panel derecho de la consola de administración de ADFS, seleccione la opción Agregar confianza de usuario de confianza... .



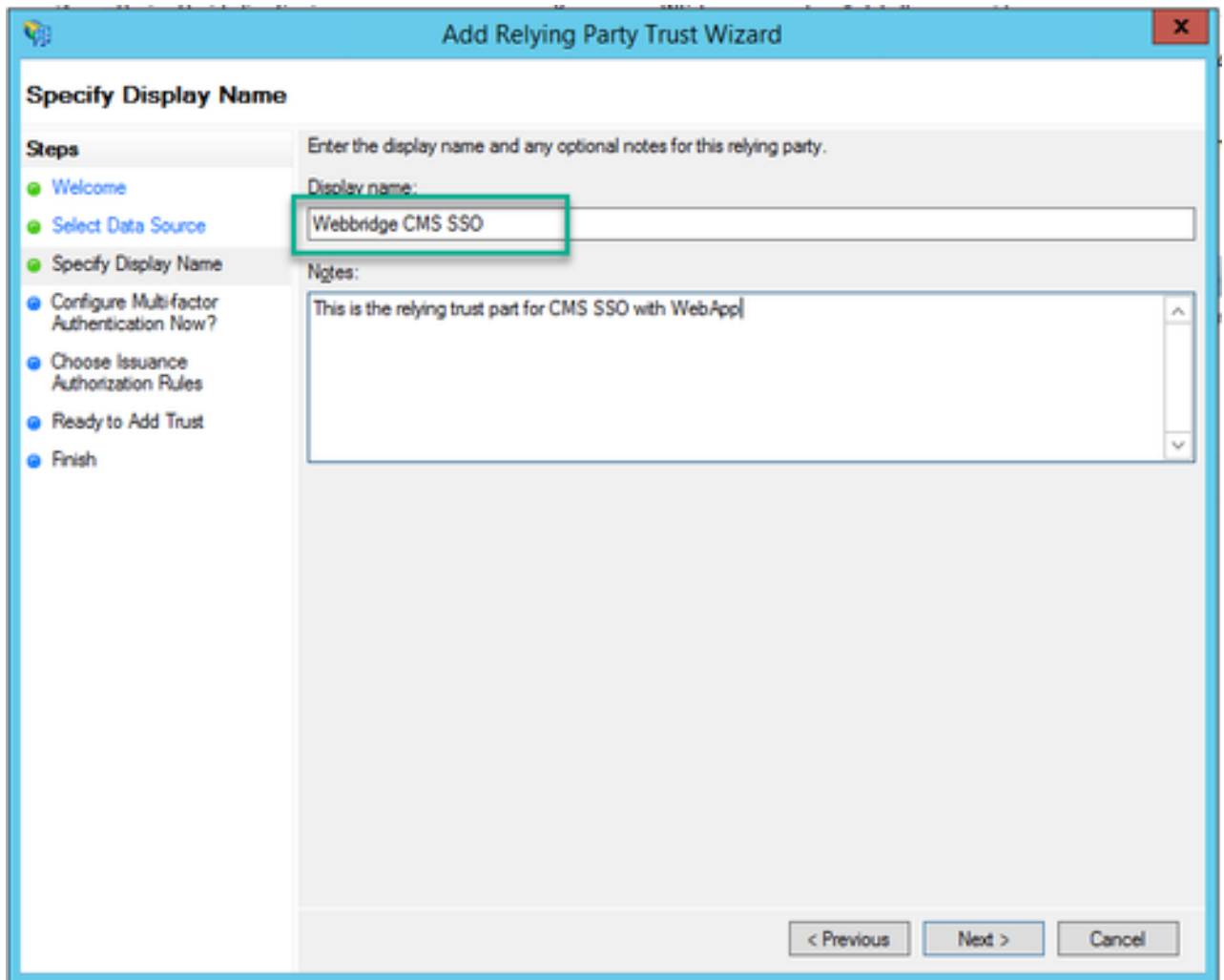
5. Después de seleccionar esta opción, se abre el Asistente de Adición de Confianza de Usuario de Confianza. Seleccione la opción Start.



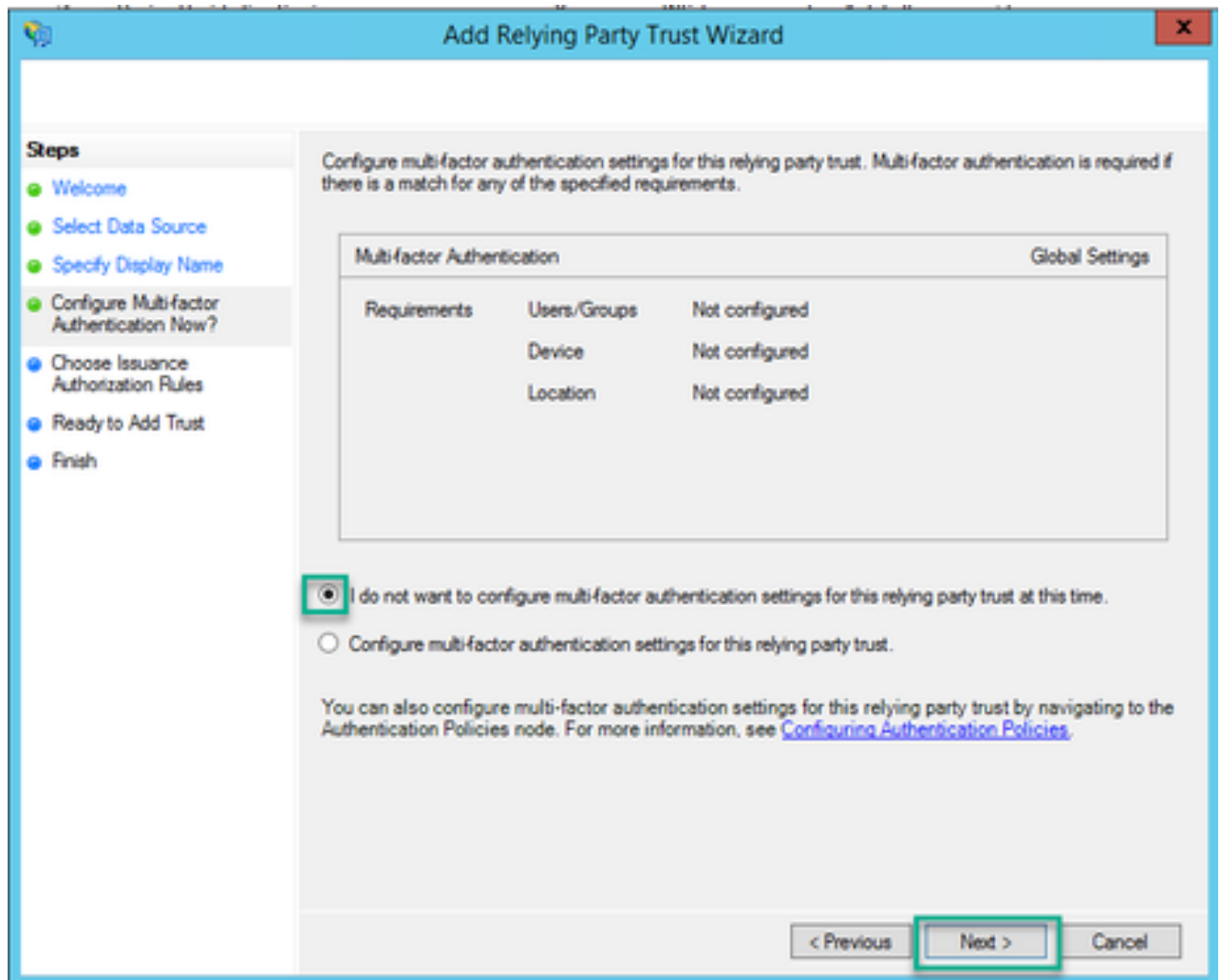
6. En la página Seleccionar Origen de Datos, seleccione el botón de radio Importar Datos sobre la persona de confianza desde un archivo y seleccione Examinar y desplácese hasta la ubicación del archivo de metadatos de Webbridge.



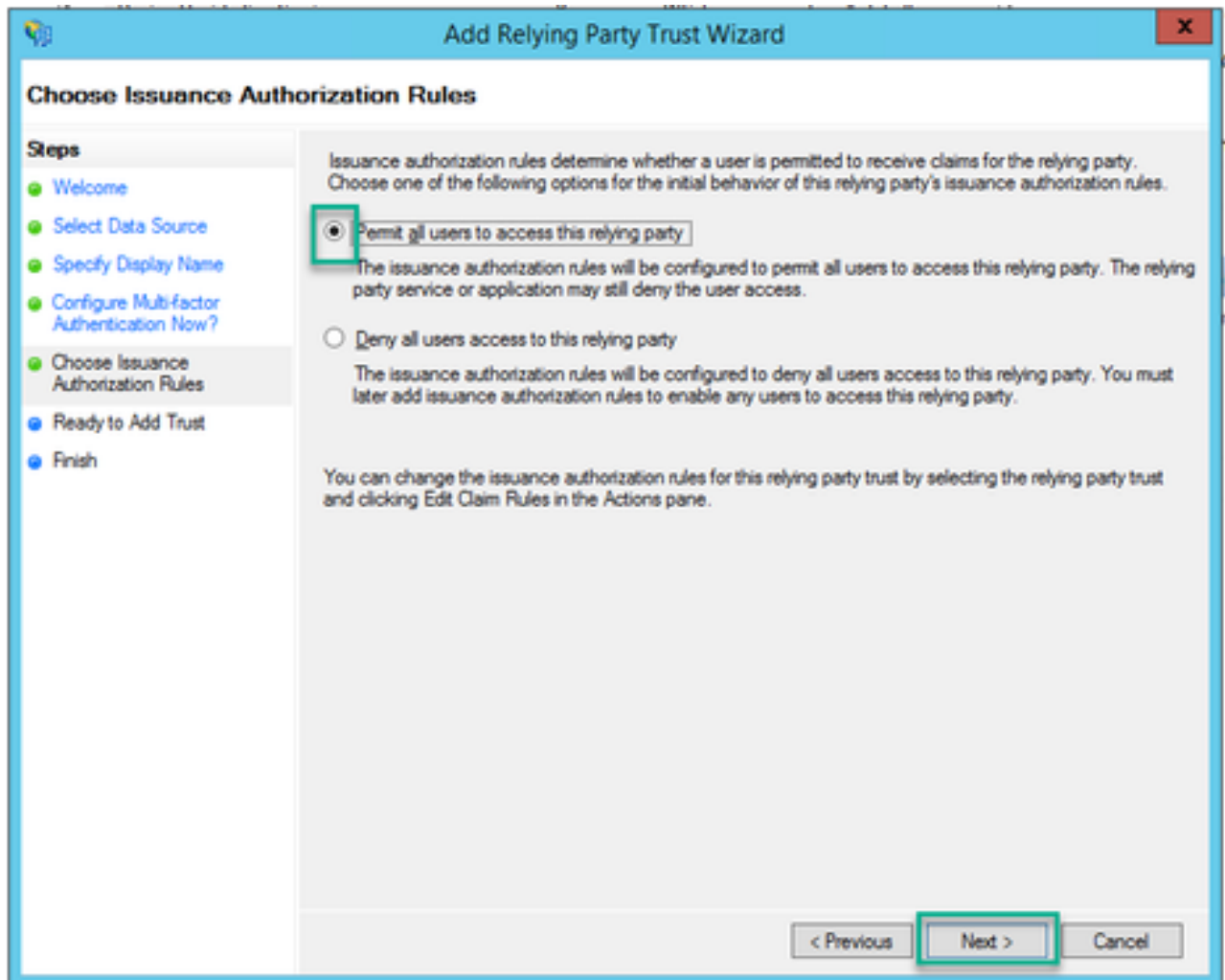
7. En la página Especificar Nombre para Mostrar, introduzca un nombre para mostrar para la entidad en ADFS (el nombre para mostrar no sirve para la comunicación de ADFS y es meramente informativo).



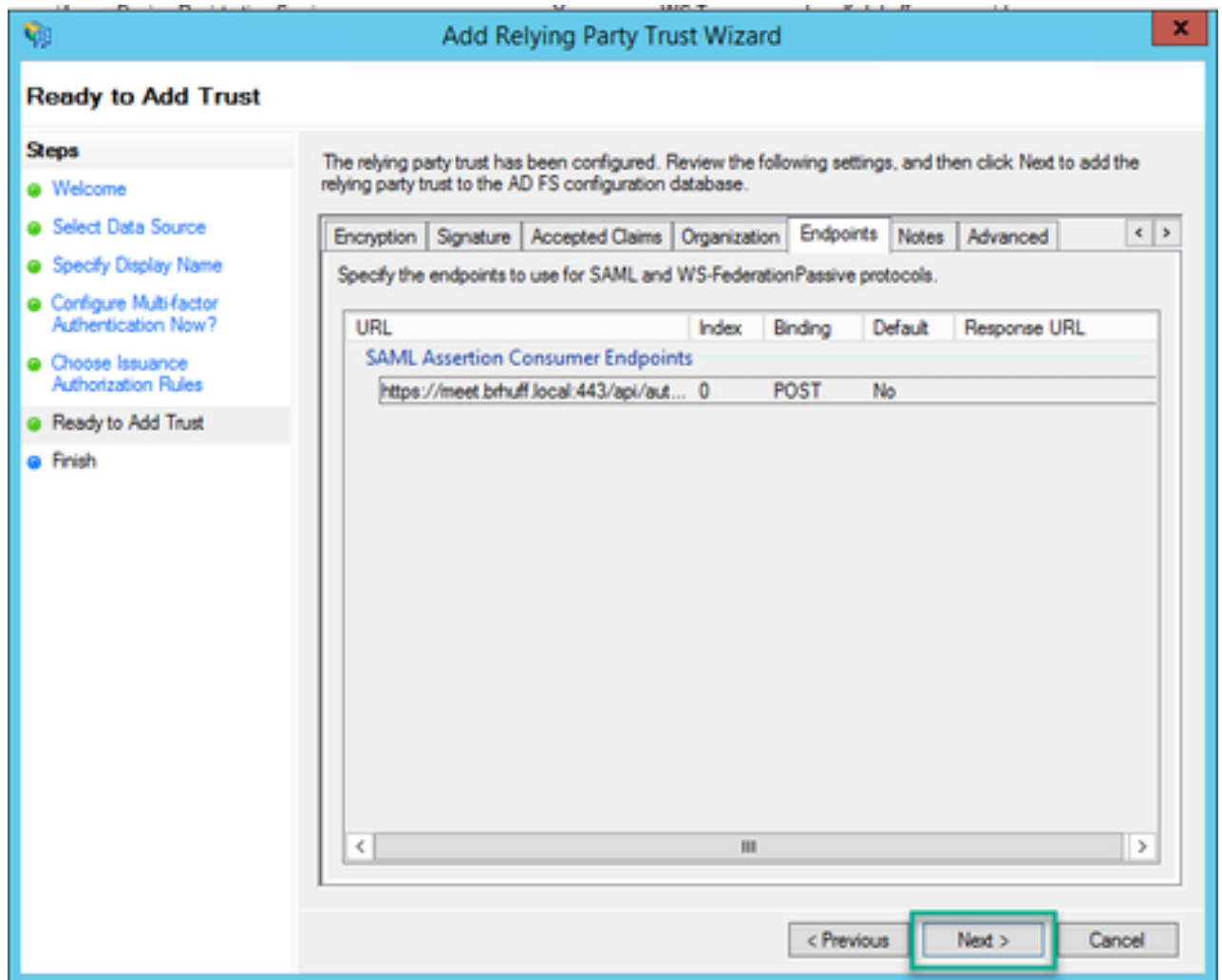
8. En la página Configure Multi-factor Authentication Now?, déjelo como valor predeterminado y seleccione Next.



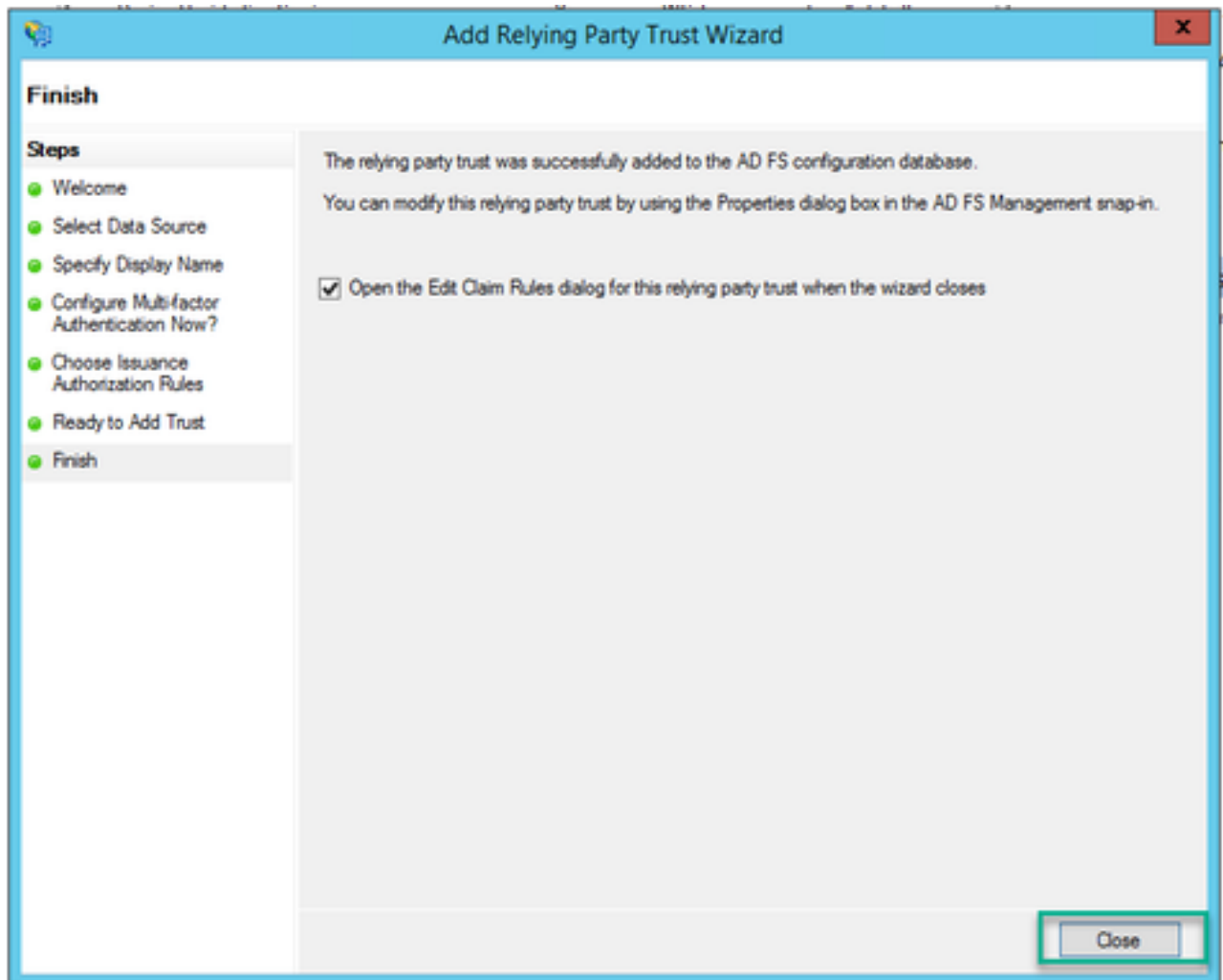
9. En la página Elegir Reglas de Autorización de Emisión, deje seleccionado Permitir a todos los usuarios acceder a esta persona de confianza.



10. En la página Ready to Add Trust, los detalles importados de la persona de confianza de confianza para Webbridge se pueden revisar en las pestañas. Verifique los Identificadores y los Terminales para los detalles de URL para el Proveedor de Servicios de Webbridge.



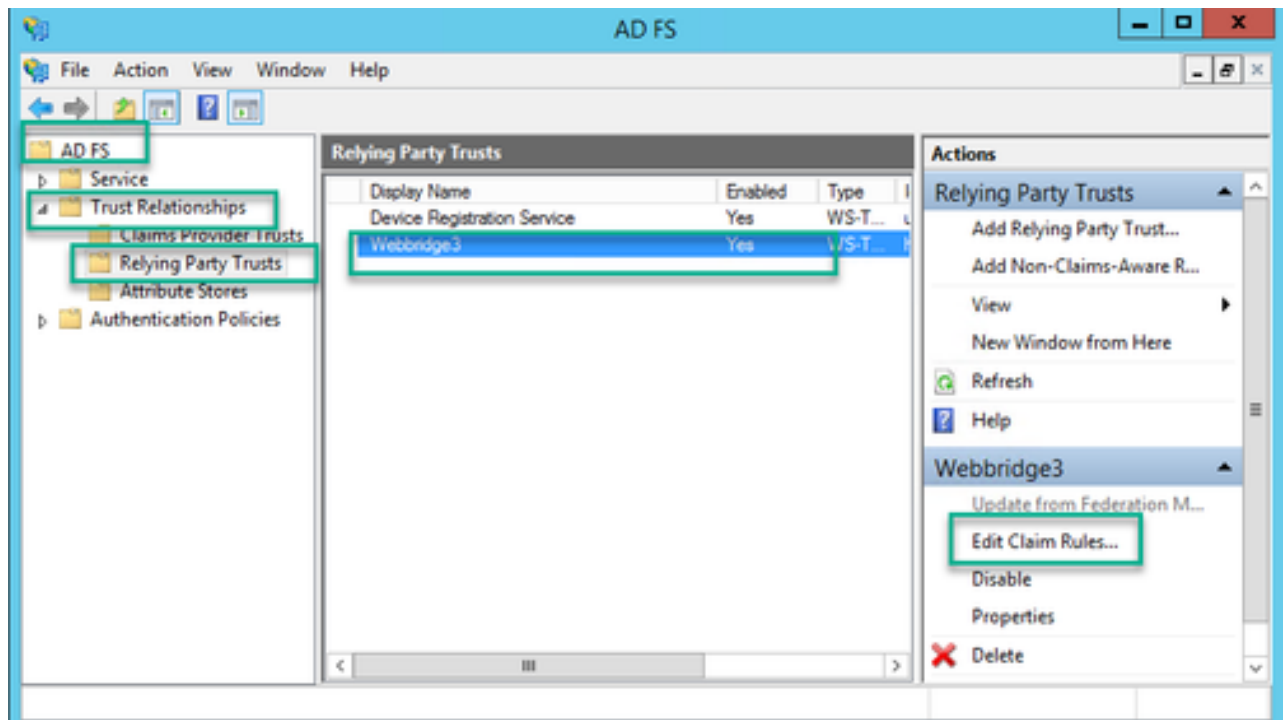
11. En la página Finish, seleccione la opción Close para cerrar el asistente y continuar con la edición de las reglas de reclamación.



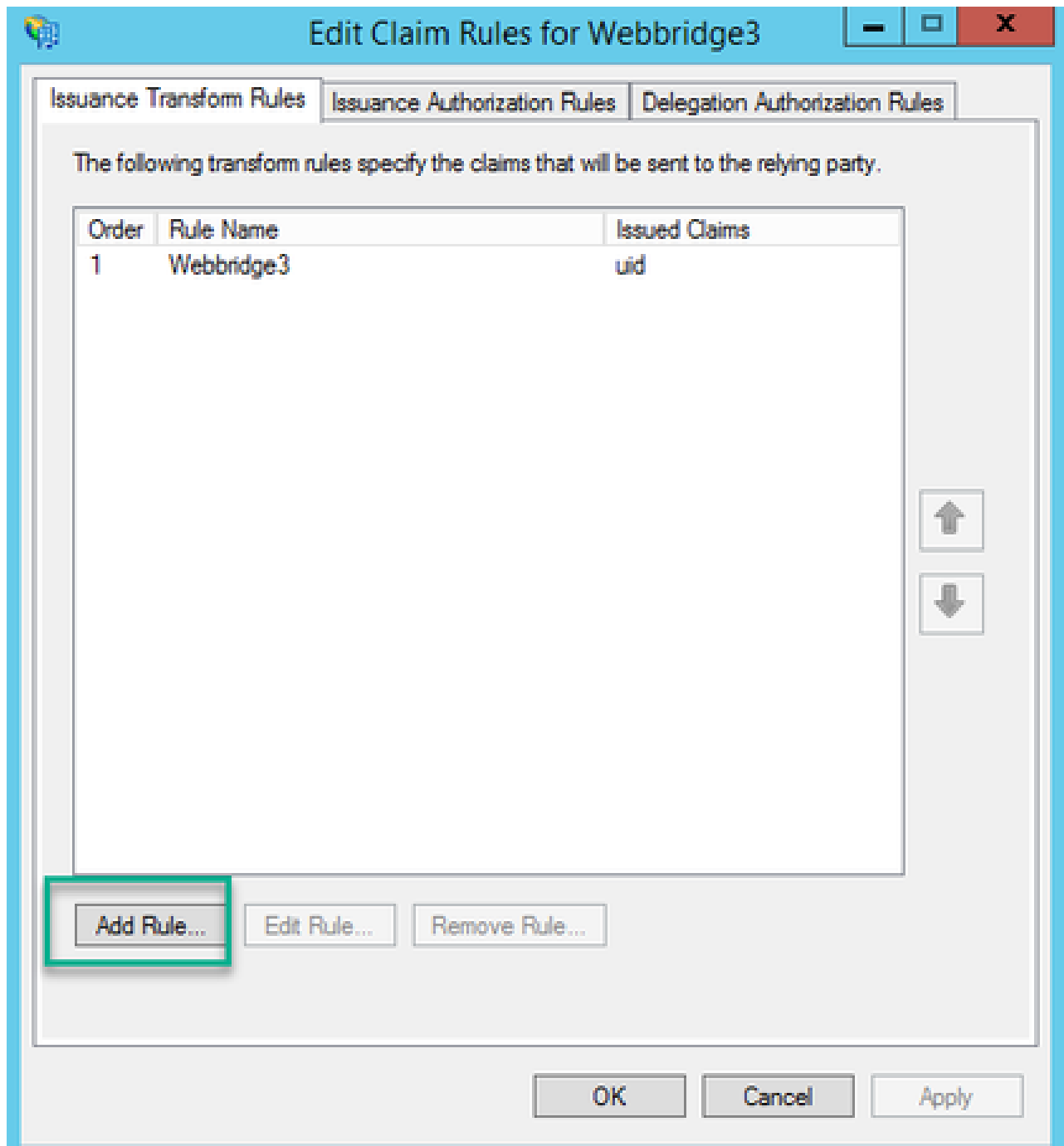
Creación de reglas de reclamación para el servicio Webbridge en el IdP

Ahora que se ha creado la confianza de usuario de confianza para Webbridge, se pueden crear reglas de notificaciones para hacer coincidir atributos LDAP específicos con tipos de notificaciones salientes que se proporcionarán a Webbridge en la respuesta SAML.

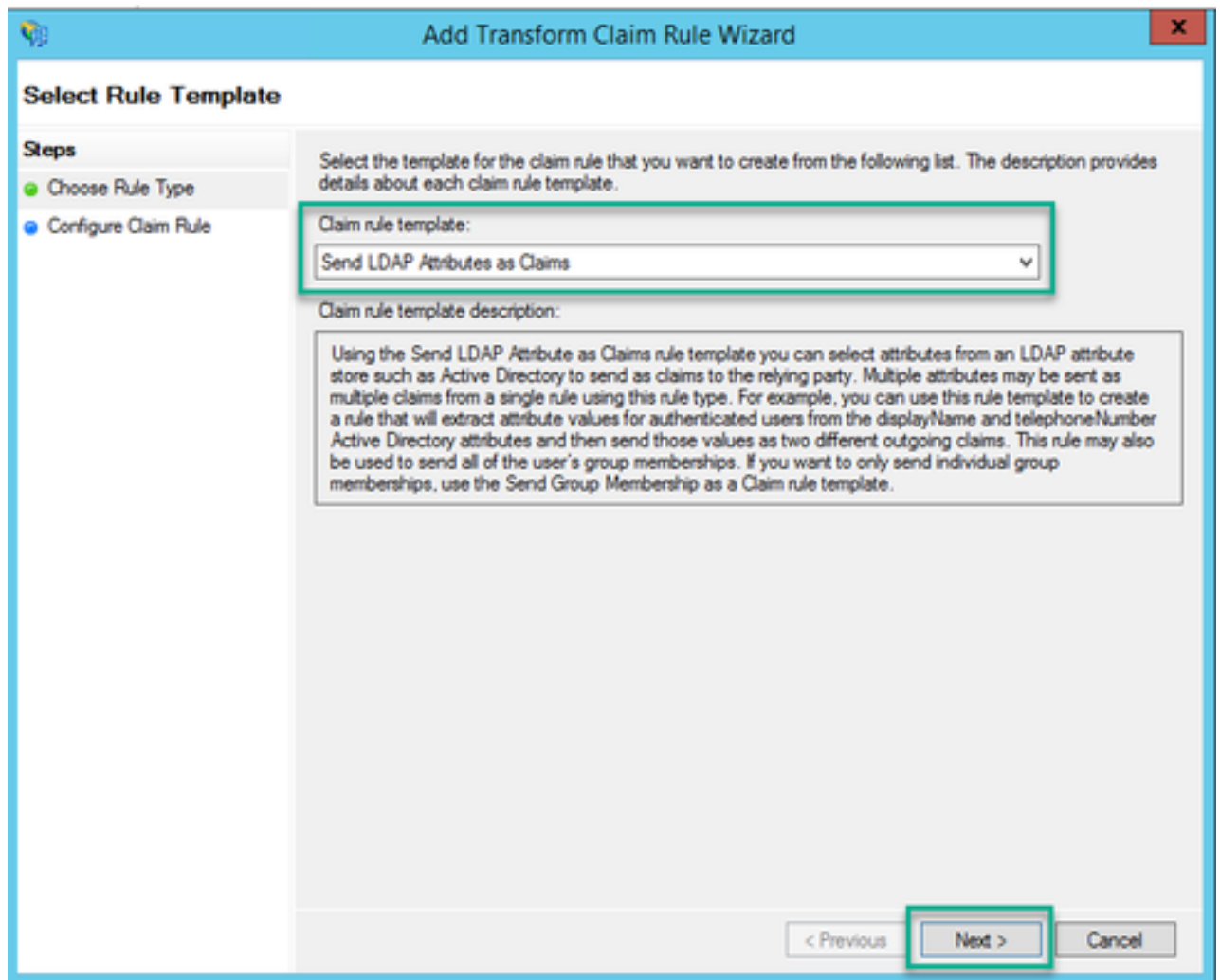
1. En la consola de administración de ADFS, resalte la Confianza del usuario de confianza para Webbridge y seleccione Editar reglas de reclamación en el panel derecho.



2. En la página Editar reglas de reclamación para <DisplayName>, seleccione Agregar regla...



3. En la página Asistente de Agregar Regla de Reclamación de Transformación, seleccione Enviar Atributos LDAP como Reclamaciones para la opción de plantilla de regla de reclamación y seleccione Siguiente.



4. En la página Configurar Regla de Reclamación, configure la regla de reclamación para la confianza de usuario de confianza con estos valores:

1. Nombre de regla de reclamación = debe ser un nombre asignado a la regla en ADFS (sólo para referencia a reglas)
2. Almacén de atributos = Active Directory
3. Atributo LDAP = Debe coincidir con authenticationIdMapping en la API Callbridge. (Por ejemplo, \$sAMAccountName\$.)
4. Tipo de notificación saliente = Debe coincidir con el authenticationIdMapping en Webbridge SSO config.json. (Por ejemplo, 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

Crear archivo ZIP de archivo SSO para Webbridge:

Esta configuración es a la que hace referencia Webbridge para validar la configuración de SSO para los dominios admitidos, la asignación de autenticación, etc. Estas reglas deben tenerse en cuenta para esta parte de la configuración:

- El archivo ZIP DEBE comenzar con sso_ con el prefijo del nombre del archivo (por ejemplo, sso_cmstest.zip).
- Una vez cargado este archivo, Webbridge deshabilita la autenticación básica y SÓLO se puede utilizar SSO para el Webbridge en el que se ha cargado.

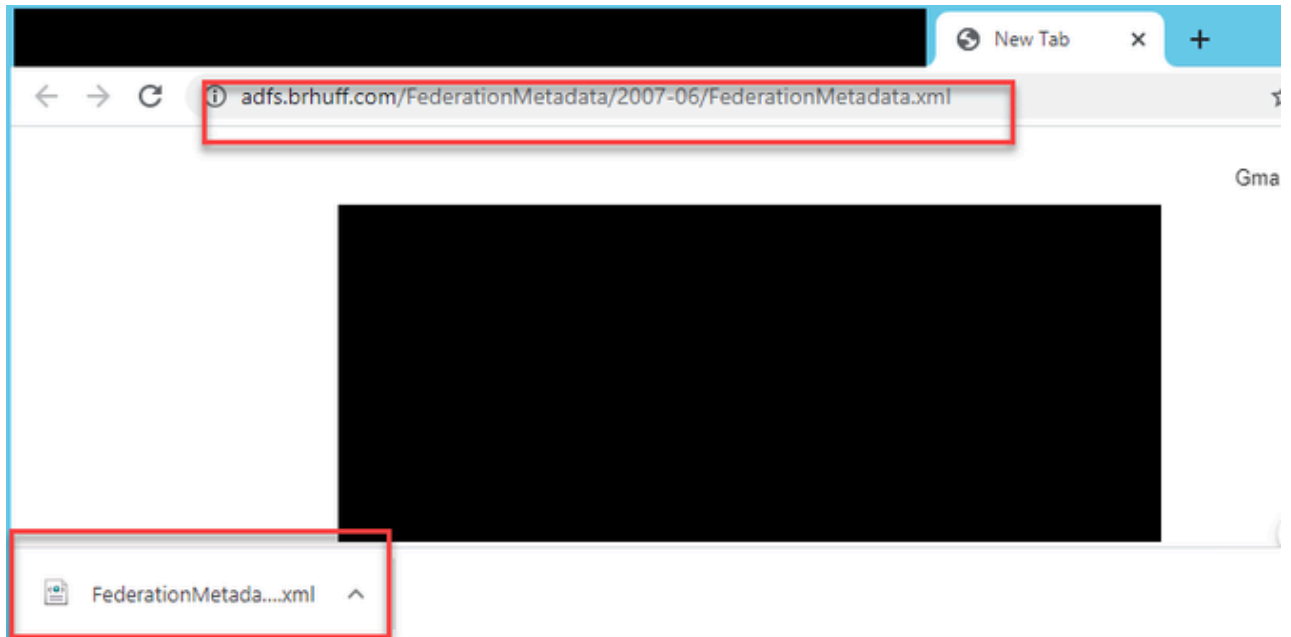
- Si se utilizan varios proveedores de identidad, se debe cargar un archivo ZIP independiente con un esquema de nomenclatura diferente (TODAVÍA con el prefijo sso_).
- Al crear el archivo zip, asegúrese de resaltar y comprimir el contenido del archivo y de no colocar los archivos necesarios en una carpeta y comprimir dicha carpeta.

El contenido del archivo zip se compone de 2 a 4 archivos, dependiendo de si se está utilizando o no el cifrado.

Nombre de Archivo	Descripción	Necesario?
idp_config.xml	Este es el archivo MetaData que el idP puede recopilar. En ADFS, esto se puede encontrar en <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml .	Sí
config.json	Este es el archivo JSON en el que Webbridge utiliza para validar los dominios admitidos, la asignación de autenticación para SSO.	Sí
sso_sign.key	Ésta es la clave privada para la clave de firma pública configurada en el proveedor de identidad. Solo es necesario para proteger los datos firmados	NO
sso_encrypt.key	Se trata de la clave privada para la clave de cifrado pública configurada en el proveedor de identidad. Solo es necesario para proteger los datos cifrados	NO

Obtenga y configure idp_config.xml

1. En el servidor ADFS (o en una ubicación que tenga acceso a ADFS), abra un explorador web.
2. En el explorador web, introduzca la URL: <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml> (también puede utilizar localhost en lugar del FQDN si se encuentra localmente en el servidor ADFS). Esto descarga el archivo FederationMetadata.xml.



3. Copie el archivo descargado en una ubicación donde se esté creando el archivo zip y cambie el nombre a 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

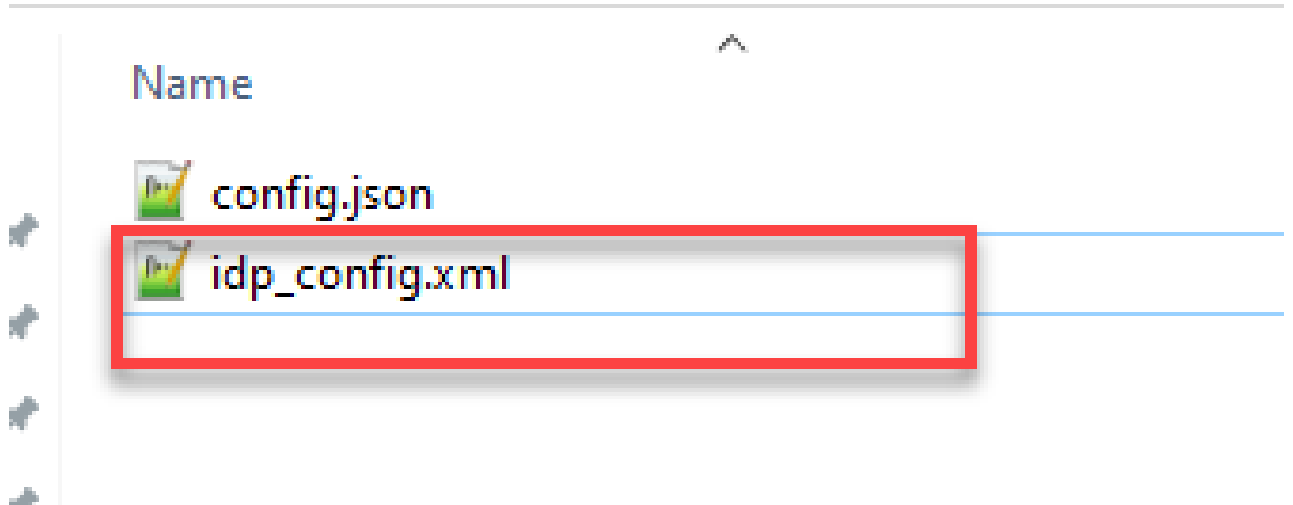
Create shortcut

Delete

Rename

Properties

Local Disk (D:) > brentssoconfig > SSOconfig



Crear el archivo config.json con contenido

El archivo config.json contiene estos 3 atributos y deben estar incluidos entre corchetes, { }:

1. supportedDomains - Esta es una lista de dominios que se verifican para la autenticación SSO contra el IdP. Varios dominios pueden separarse mediante una coma.
2. authenticationIdMapping: parámetro que se devuelve como parte de la regla de reclamación saliente desde ADFS/IdP. Debe coincidir con el valor del nombre del tipo de reclamación saliente en el IdP. Regla de reclamación.
3. ssoServiceProviderAddress: URL de FQDN a la que el proveedor de identidad envía las respuestas SAML. Debe ser el FQDN de Webbridge.

Configured as 'uid' to match outgoing claim on ADFS

supported domain of 'brhuff.com' for SSO authentication

the URL of Webbridge for IdP to send response to

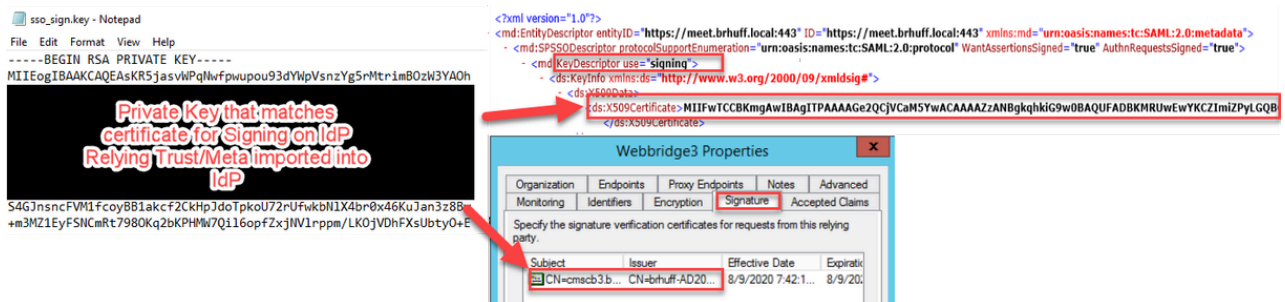
Make sure the LDAP attribute used in ADFS for the Claim rule matches the authenticationIdMapping in the CMS API

Establezca sso_sign.key (OPCIONAL)

Este archivo debe contener la clave privada del certificado utilizado para firmar en los metadatos de Webbridge importados al IdP. El certificado utilizado para la firma se puede establecer durante la importación de los metadatos de Webbridge en ADFS rellenando X509Certificate con la información del certificado en la sección <KeyDescriptor use=signing>. También se puede ver (e importar) en ADFS en la Parte de Confianza de Confianza de Webbridge bajo Propiedades > Firma.

En el siguiente ejemplo, puede ver el certificado de callbridge (CN=cmscb3.brhuff.local), que se agregó a los metadatos de Webbridge antes de importarse a ADFS. La clave privada insertada en sso_sign.key es la que coincide con el certificado cmscb3.brhuff.local.

Esta es una configuración opcional y solo es necesaria si se pretende cifrar las respuestas SAML.

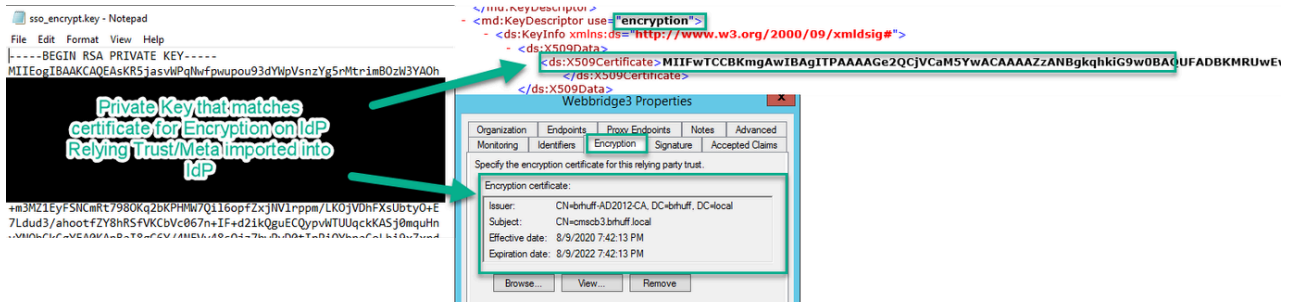


Establezca sso_encrypt.key (OPCIONAL)

Este archivo debe contener la clave privada del certificado utilizado para el cifrado en los metadatos de webbridge que se importaron al IdP. El certificado utilizado para el cifrado se puede establecer durante la importación de los metadatos de Webbridge en ADFS rellenando el certificado X509 con la información del certificado en la sección <KeyDescriptor use=encryption>. También se puede ver (e importar) en ADFS en el Confianza de Confianza de Webbridge bajo Propiedades > Cifrado.

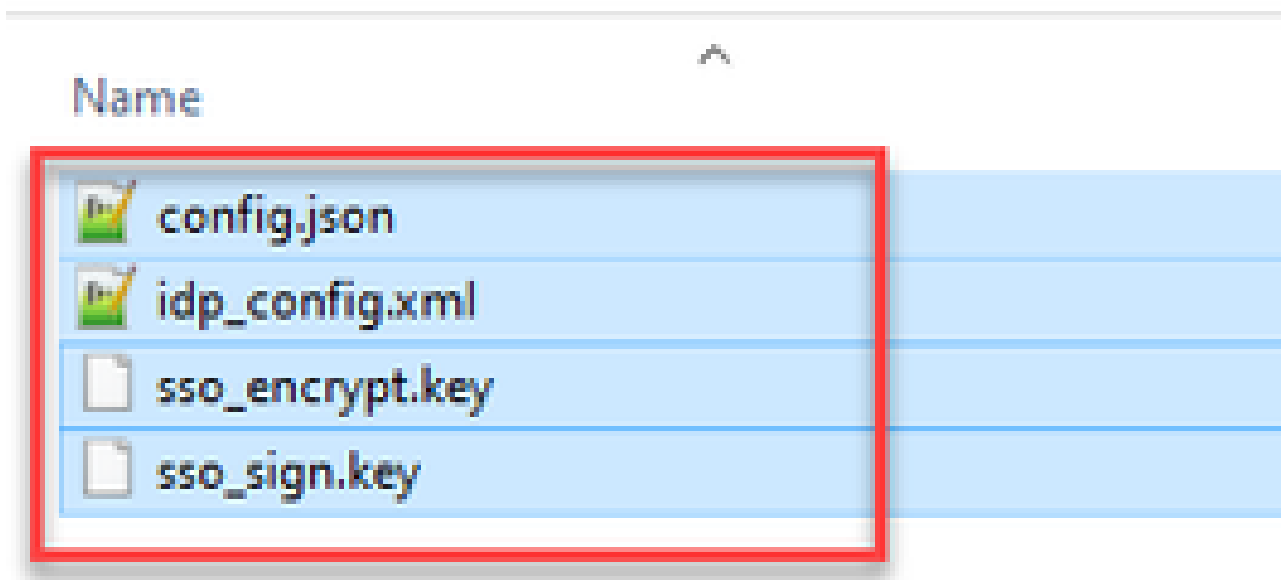
En el siguiente ejemplo, puede ver el certificado de callbridge (CN=cmscb3.brhuff.local), que se agregó a los metadatos de Webbridge antes de importarse a ADFS. La clave privada insertada en 'sso_encrypt.key' es la que coincide con el certificado cmscb3.brhuff.local.

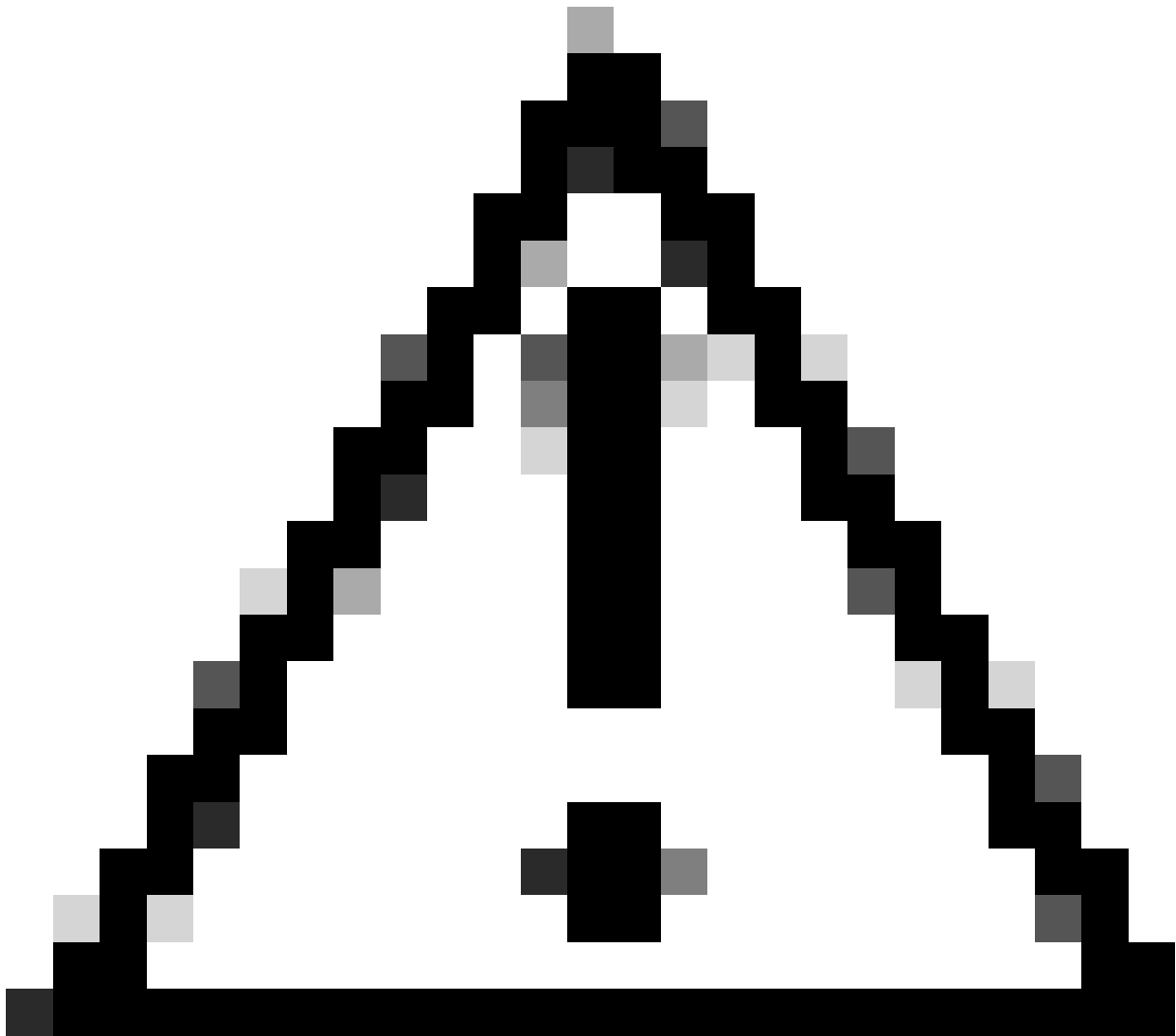
Esta es una configuración opcional y sólo es necesaria si pretende cifrar las respuestas SAML.



Creación del archivo ZIP de SSO

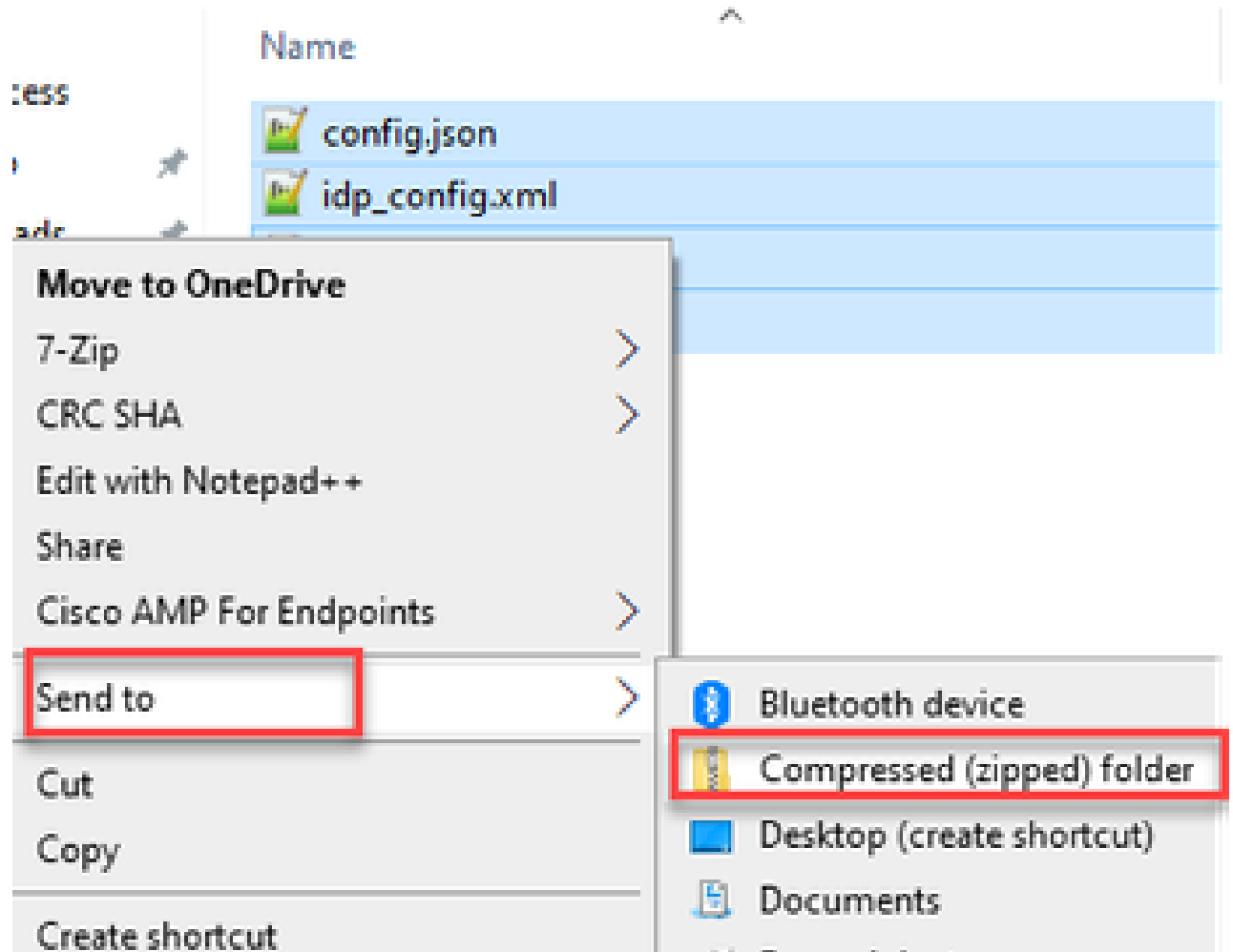
1. Resalte todos los archivos que se utilizarán para el archivo de configuración de SSO.



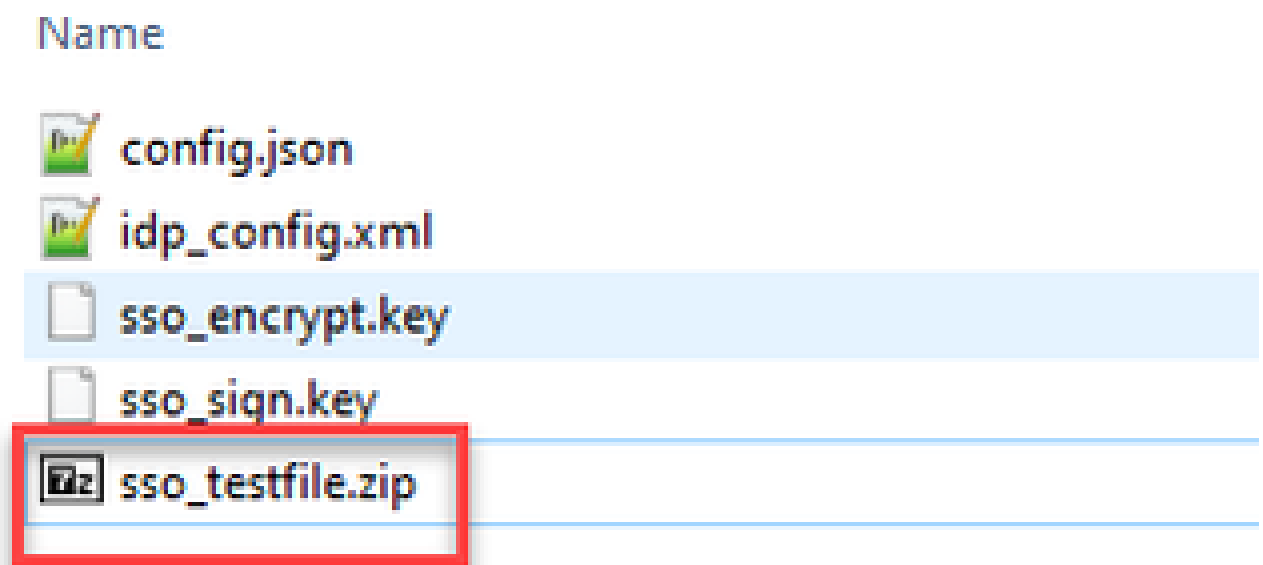


Precaución: no comprima la carpeta que contiene los archivos porque esto hace que el SSO no funcione.

2. Haga clic con el botón derecho del ratón en los archivos resaltados y seleccione Enviar a > Carpeta comprimida (en zip).



3. Después de que los archivos se hayan comprimido, cámbielos al nombre deseado con el sso_ prefix:



Cargue los archivos zip de SSO en Webbridge

Abra un cliente SFTP/SCP, en este ejemplo WinSCP se está utilizando, y conéctese al servidor que aloja Webbridge3.

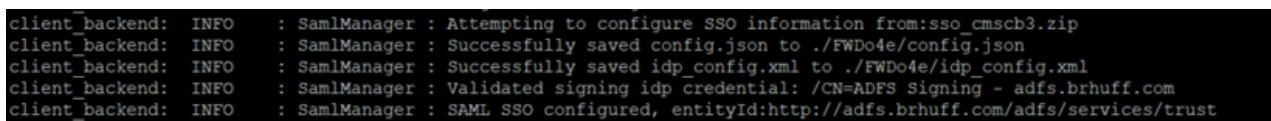
1. En el panel izquierdo, navegue hasta la ubicación en la que reside el archivo Zip de SSO y haga clic con el botón derecho en Cargar o arrastre y suelte el archivo.



2. Una vez que el archivo se haya cargado completamente en el servidor Webbridge3, abra una sesión SSH y ejecute el comando webbridge3 restart.



3. En el syslog, estos mensajes indican que la habilitación de SSO fue exitosa:



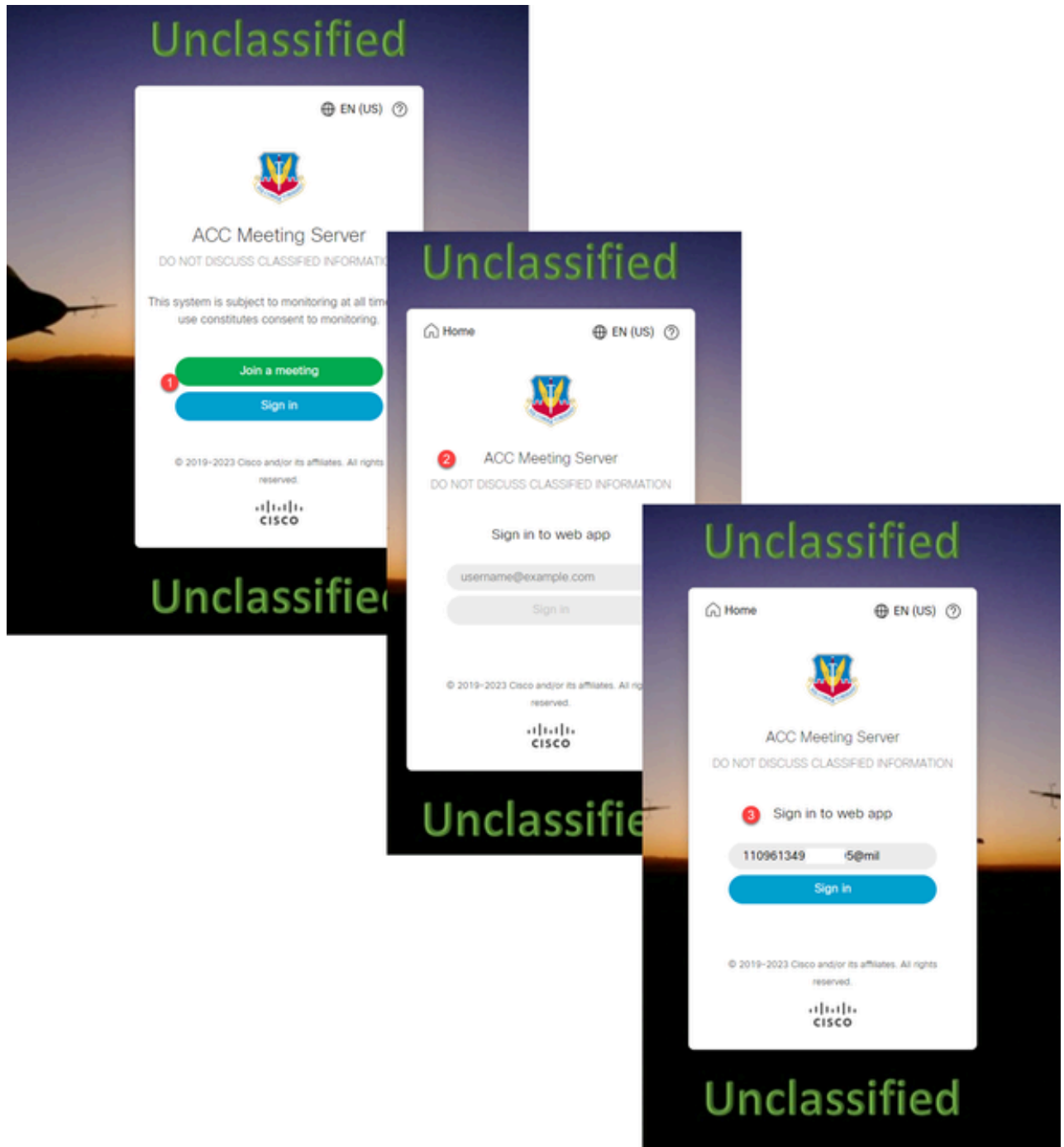
Tarjeta de acceso común (CAC)

Una tarjeta de acceso común (CAC) es una tarjeta inteligente que sirve como identificación estándar para el personal militar en servicio activo, los empleados civiles del Departamento de Defensa y el personal del contratista elegible.

Este es el proceso de inicio de sesión completo para los usuarios que utilizan tarjetas CAC:

1. Encienda el PC y pegue la tarjeta CAC
2. Inicie sesión (a veces seleccione cert) e introduzca Pin

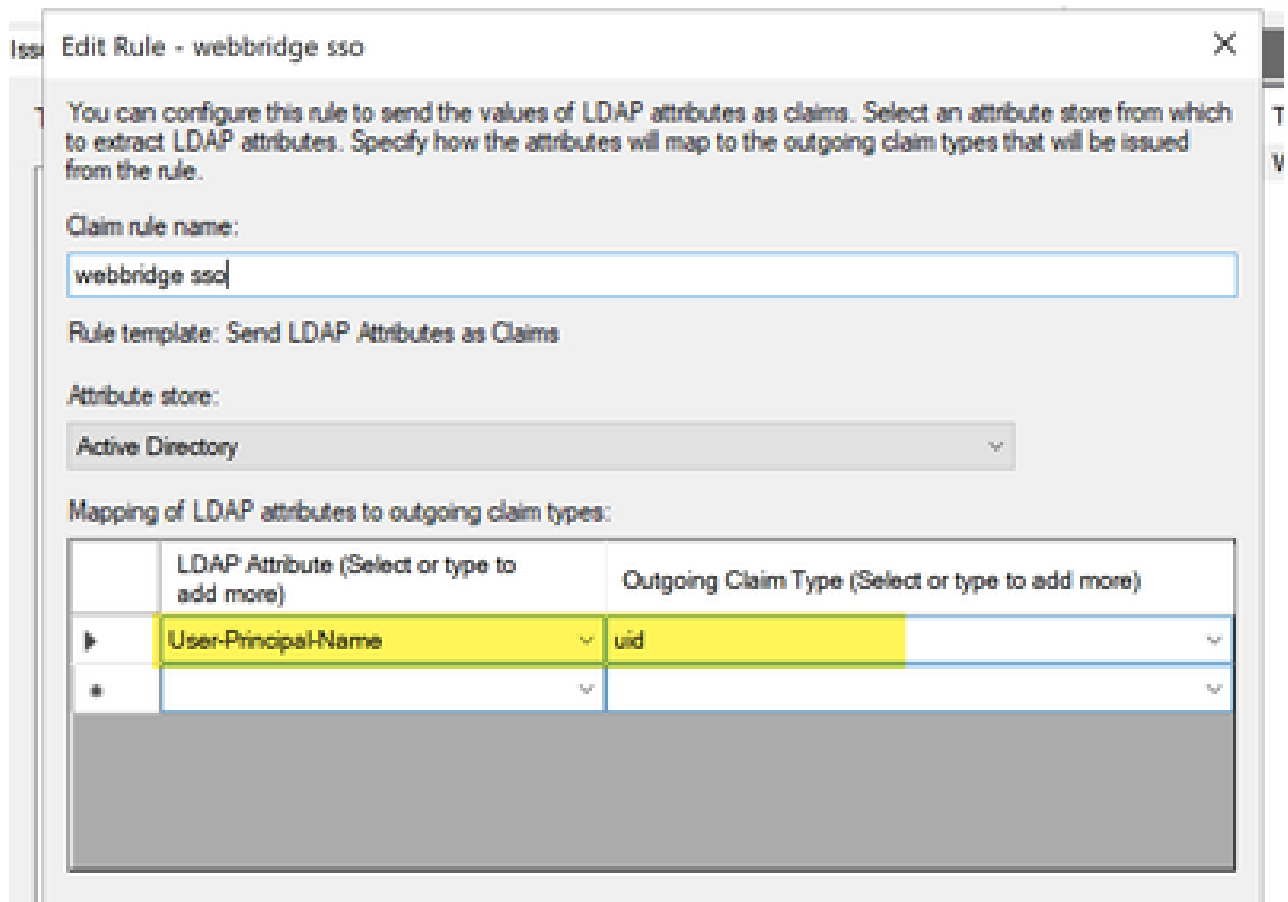
3. Abrir explorador
4. Desplácese hasta la URL para unirse y vea las opciones Unirse a una reunión o Iniciar sesión
5. Iniciar sesión: Introduzca el nombre de usuario configurado como jidMapping y Active Directory esperará un inicio de sesión CAC
6. Pulse Iniciar sesión
7. La página ADFS aparece brevemente y se rellena automáticamente
8. El usuario se conectará en este momento



Configure jidMapping (este es el nombre de inicio de sesión de los usuarios) en Ldapmapping igual que lo que ADFS utiliza para la tarjeta CAC. \$userPrincipalName\$ por ejemplo (distingue entre mayúsculas y minúsculas)

Establezca también el mismo atributo LDAP para que authenticationIdMapping coincida con el atributo que se utiliza en la regla de reclamación en ADFS.

En este caso, la regla de reclamación muestra que devolverá \$userPrincipalName\$ a CMS como UID.



155 Edit Rule - webbridge sso

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:
webbridge sso

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)
▶	User-Principal-Name	uid
#		

Prueba de SSO Inicie sesión mediante WebApp

Ahora que se ha configurado SSO, puede probar el servidor:

1. Navegue hasta la URL de Webbridge para la aplicación web y seleccione el botón Iniciar sesión.



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

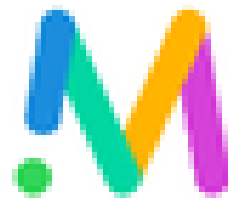
Join a meeting

Sign in

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



2. El usuario tiene la opción de introducir su nombre de usuario (observe que no hay opción de contraseña en esta página).

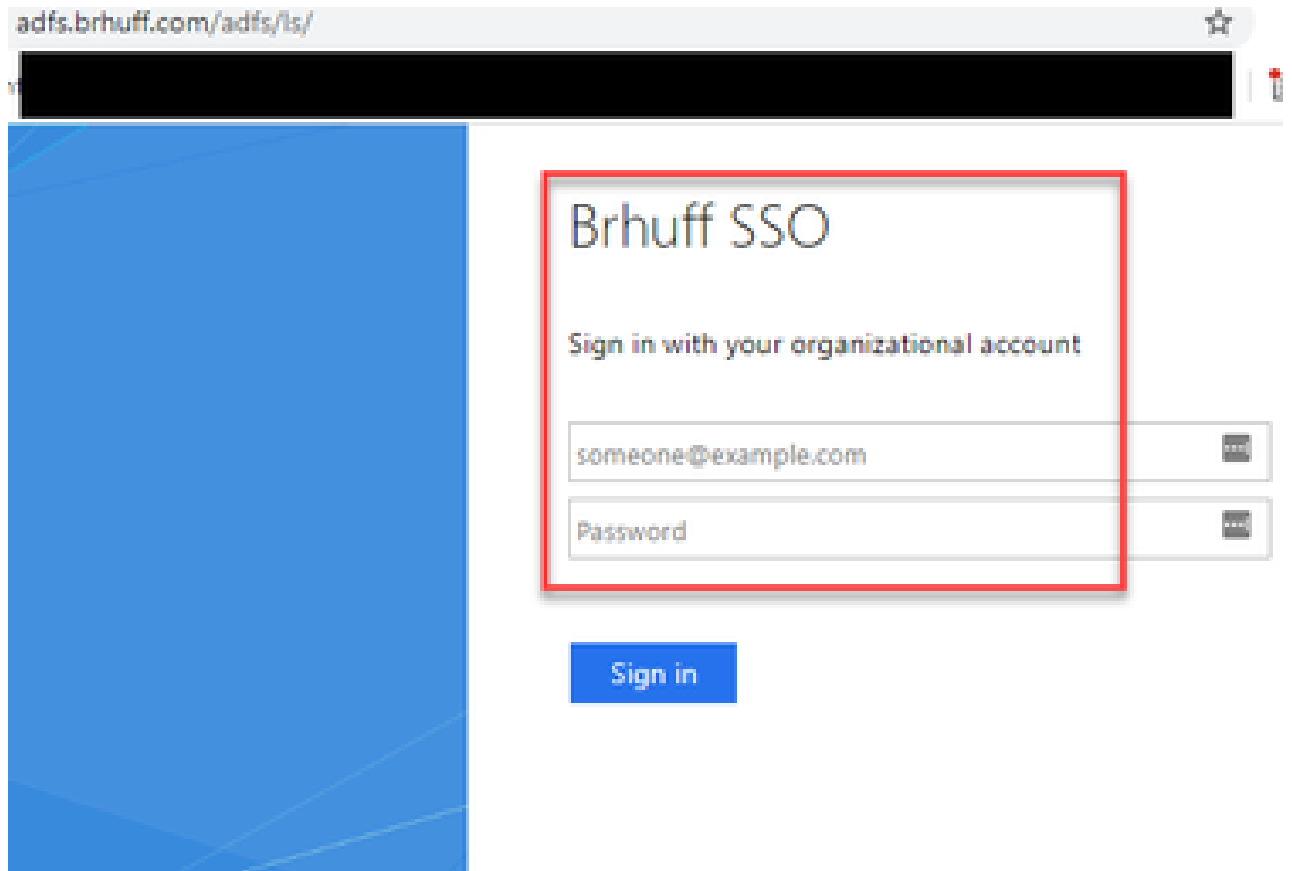


Cisco Meeting Server

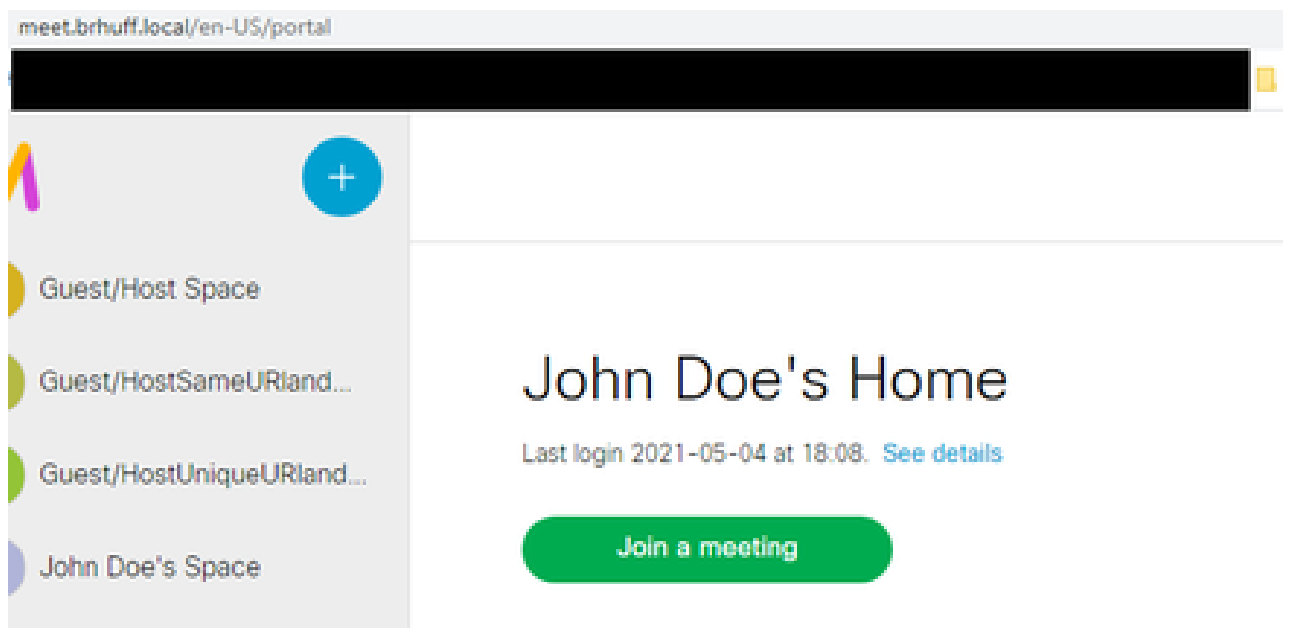
web app

Sign in to web app

3. El usuario es entonces redirigido a la página ADFS (después de introducir los detalles del usuario) donde el usuario debe ingresar sus credenciales para autenticarse a IdP.



4. El usuario, después de ingresar y validar credenciales con el IdP, es redirigido con el token para acceder a la página de inicio de la aplicación Web:



Resolución de problemas

Resolución de problemas básicos

Para la resolución básica de cualquier problema de SSO:

1. Asegúrese de que los metadatos construidos para Webbridge3 utilizados para importar como confianza de confianza en IdP estén configurados correctamente y que la URL configurada coincida exactamente con `ssoServiceProviderAddress` en `config.json`.
2. Asegúrese de que los metadatos proporcionados por el IdP y comprimidos en el archivo de configuración de Webbridge3 sean los más recientes desde el IdP, ya que si hubo cambios en el nombre de host del servidor, certificados, etc., debe volver a exportarse y comprimirse en el archivo de configuración.
3. Si utiliza claves privadas de firma y cifrado para cifrar datos, asegúrese de que las claves coincidentes correctas forman parte del archivo `sso_xxxx.zip` que cargó en webbridge. Si es posible, intente probar sin las claves privadas opcionales para ver si SSO funciona sin esta opción cifrada.
4. Asegúrese de que `config.json` esté configurado con los detalles correctos para los dominios de SSO, la URL de Webbridge3 Y la asignación de autenticación esperada que coincidan con la respuesta de SAML.

También sería ideal intentar la resolución de problemas desde la perspectiva del registro:

1. Cuando vaya a la URL de Webbridge, coloque `?trace=true` al final de la URL para habilitar un registro detallado en el registro del sistema de CMS. (por ejemplo, <https://join.example.com/en-US/home?trace=true>).
2. Ejecute el comando `syslog follow` en el servidor Webbridge3 para capturar en vivo durante la prueba o ejecute la prueba con la opción `trace` agregada a la URL y recopile el archivo `logbundle.tar.gz` de los servidores Webbridge3 y CMS Callbridge. Si webbridge y callbridge están en el mismo servidor, esto requiere solamente el archivo único `logbundle.tar.gz`.

Códigos de error de Microsoft ADFS

A veces, hay una falla para el proceso SSO que puede resultar en una falla para la configuración del IdP o su comunicación con el IdP. Si utiliza ADFS, sería ideal revisar el siguiente enlace para confirmar el fallo que se está observando y tomar medidas correctivas:

[Códigos de estado de Microsoft](#)

Un ejemplo de esto es:

```
client_backend: ERROR: SamlManager: error en la solicitud de autenticación SAML
_e135ca12-4b87-4443-abe1-30d396590d58 con motivo:
urn:oasis:names:tc:SAML:2.0:status:Responder
```

Este error indica que, según la documentación anterior, el error se produjo debido al IdP o ADFS y, por lo tanto, el administrador del ADFS debe manejarlo para resolverlo.

Error al obtener authenticationID

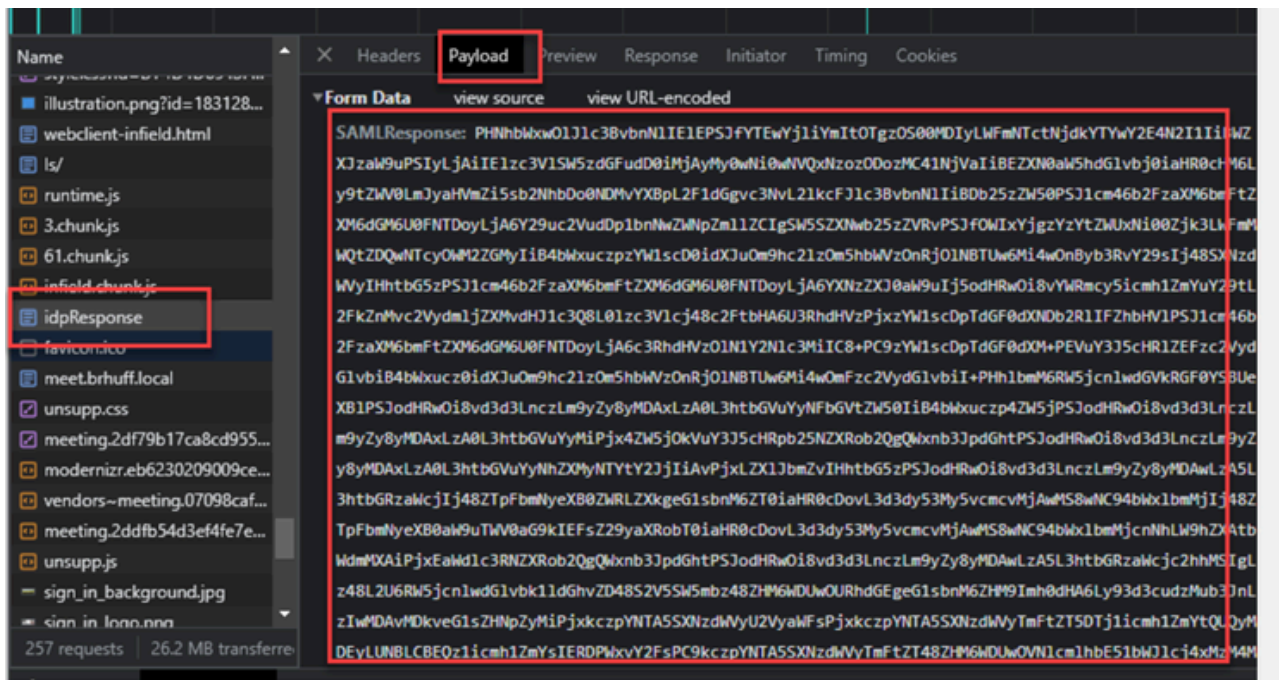
Puede haber casos en los que durante el intercambio de SAMLResponse desde el IdP, Webbridge pueda mostrar este mensaje de error en los registros con un error al iniciar sesión a través de SSO:

```
client_backend: INFO : SamlManager : [57dff9e3-862e-4002-b4fa-683e4aa6922c] Error al
obtener authenticationId
```

Lo que esto indica es que al revisar los datos de SAMLResponse transferidos desde el IdP durante el intercambio de autenticación, Webbridge3 no encontró un atributo coincidente válido en la respuesta comparado con su config.json para authenticationId.

Si la comunicación no está cifrada con el uso de las claves privadas de firma y cifrado, la respuesta SAML se puede extraer del registro de red de herramientas de desarrollo a través de un navegador web y descodificarse utilizando base64. Si la respuesta está cifrada, puede solicitar la respuesta SAML descifrada desde el lado IdP.

En la salida de registro de red de herramientas del desarrollador, también conocida como datos HAR, busque idpResponse en la columna name y seleccione Payload para ver la respuesta SAML. Como se mencionó anteriormente, esto se puede decodificar utilizando el decodificador base64.



Cuando reciba los datos de SAMLResponse, verifique la sección de <AttributeStatement> para localizar los nombres de atributo devueltos y dentro de esta sección puede encontrar los tipos de reclamación configurados y enviados desde el IdP. Por ejemplo:

```

<AttributeStatement>
  <Attribute Name="<URL de nombre común">
    <AttributeValue>usuarioDePrueba1</AttributeValue>
  </Atributo>
  <Attribute Name="<URL para NameID">
    <AttributeValue>usuarioDePrueba1</AttributeValue>
  </Atributo>
  <Attribute Name="uid">
    <AttributeValue>usuarioDePrueba1</AttributeValue>
  </Atributo>
</AttributeStatement>

```

Revisando los nombres anteriores, puede verificar <AttributeName> en la sección Attribute Statement y comparar cada valor con lo que se establece en la sección authenticationIdmapping de SSO config.json.

En el ejemplo anterior, puede ver que la configuración para authenticationIdMapping NO coincide exactamente con lo que se pasa y, por lo tanto, da como resultado la falla al encontrar un authenticationId coincidente:

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

Para resolver este problema, hay dos métodos posibles para intentar:

1. La regla de reclamación saliente de IdP se puede actualizar para tener una reclamación coincidente que coincida exactamente con lo que se configura en

authenticationIdMapping de config.json en Webbridge3. (Regla de reclamación agregada en IdP para <http://example.com/claims/NameID>)

O

2. El archivo config.json se puede actualizar en Webbridge3 para que 'authenticationIdMapping' coincida exactamente con lo que está configurado como una de las reglas de notificación saliente configuradas en el IdP. (Es decir, 'authenticationIdMapping' se actualizará para coincidir con uno de los nombres de atributo, que podría ser "uid", "<URL>/NameID" o "<URL>/CommonName". Siempre que coincida (exactamente) con el valor esperado configurado en la API Callbridge cuando se pasa)

No se superó ni coincidió ninguna afirmación en la validación

A veces, durante el intercambio de SAMLResponse desde el IdP, Webbridge muestra este error indicando que hay una falla en la coincidencia de la afirmación y salta cualquier afirmación que no coincida con la configuración del servidor:

```
client_backend: ERROR: SamlManager: no se pasó ninguna aserción a la validación
client_backend: INFO : SamlManager : omitiendo aserción sin nosotros en la audiencia permitida
```

Lo que indica este error es que cuando se revisa la respuesta SAMLResponse desde el IdP, Webbridge no pudo encontrar ninguna afirmación coincidente y, por lo tanto, omitió las fallas no coincidentes y, en última instancia, dio lugar a un inicio de sesión SSO fallido.

Para localizar este problema, es ideal revisar la respuesta SAMLResponse desde el IdP. Si la comunicación no está cifrada con el uso de las claves privadas de firma y cifrado, la respuesta SAML se puede extraer del registro de red de herramientas de desarrollador a través de un navegador web y descodificarse usando base64. Si la respuesta está cifrada, puede solicitar la respuesta SAML descifrada desde el lado IdP.

Al revisar los datos de SAMLResponse, mirando la sección <AudienceRestriction> de la respuesta, puede encontrar todas las audiencias para las que esta respuesta está restringida:

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

Usando el valor de la sección <Audience> (<https://cisco.example.com>) puede compararlo con la ssoServiceProviderAddress en el config.json de la configuración de Webbridge y validar si es una coincidencia exacta. Para este ejemplo, puede ver que la razón del error es que la Audiencia NO coincide con la dirección del proveedor de servicios en la configuración, porque tiene el apéndice

:443:

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

Esto requiere una coincidencia exacta entre ellos para no dar lugar a una falla como esta. Para este ejemplo, la corrección sería para cualquiera de estos dos métodos:

1. :443 se podría eliminar de la dirección en la sección ssoServiceProviderAddress del archivo config.json, de modo que coincida con el campo Audience proporcionado en SAMLResponse del IdP.

O

2. Los metadatos O la parte de confianza de confianza de confianza para Webbridge3 en el IdP se pueden actualizar para tener el código :443 anexado a la dirección URL. (Si los metadatos se actualizan, se deben importar de nuevo como parte de confianza de confianza de confianza en el ADFS. Sin embargo, si usted modifica la persona de confianza de confianza desde el asistente de IdP directamente, no es necesario importarla nuevamente.)

Error de inicio de sesión en aplicación web:



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

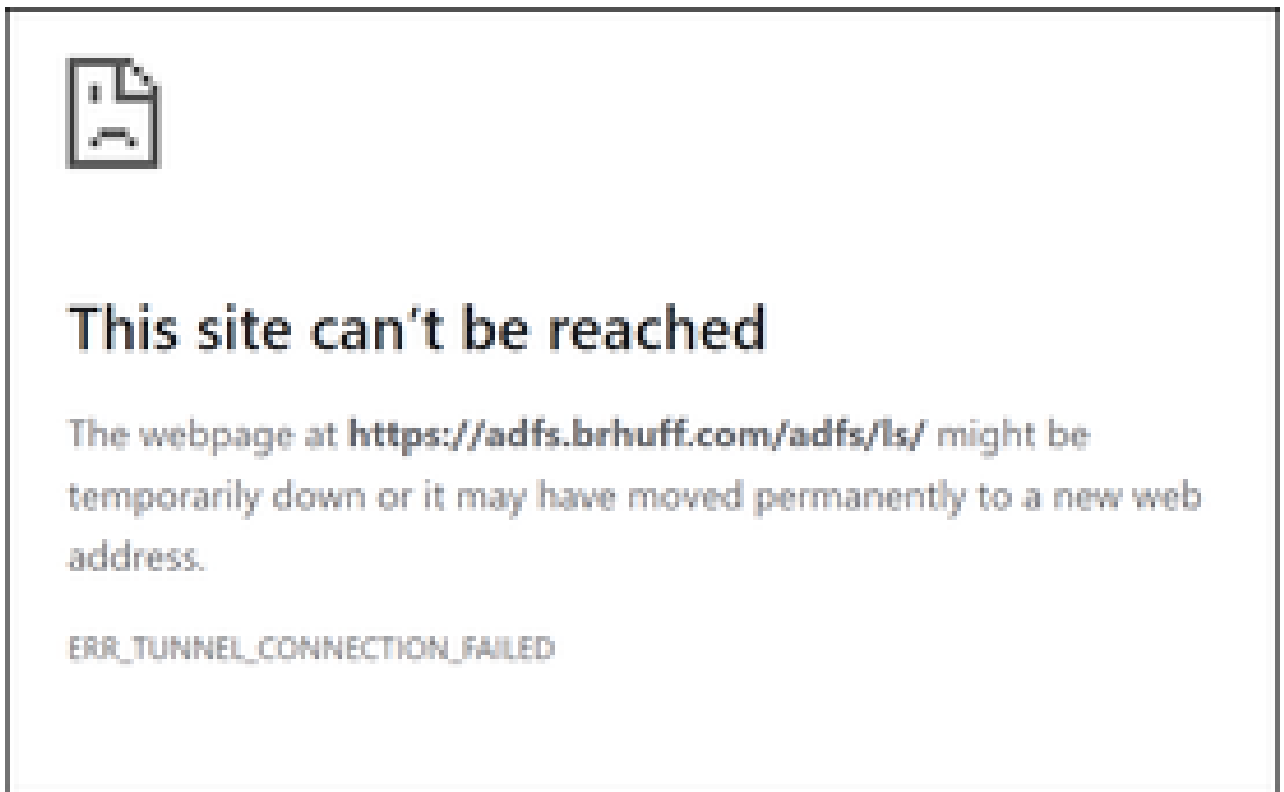
Sign in

 Sign in failed

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



), webbridge comprueba que el dominio utilizado coincide con uno del archivo config.json y, a continuación, envía la información SAML al cliente, indicándole dónde debe conectarse para la autenticación. El cliente intentará conectarse al IdP que está en el token SAML. En el ejemplo siguiente, el explorador muestra esta página porque no puede alcanzar el servidor ADFS.



Error en el explorador del cliente

Seguimientos de CMS Webbridge (mientras que se utiliza ?trace=true)

19 de marzo 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Coincidió con SSO sso_2024.zip en la solicitud de token de SAML

19 de marzo 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Intentando encontrar SSO en la solicitud de token de SAML

19 de marzo 10:47:07.930 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Token SAML generado correctamente

Escenario 2:

El usuario intentó iniciar sesión con un dominio que no está en el archivo zip de SSO en la página de inicio de sesión de webbridge. El cliente envía una petición de token con una carga del nombre de usuario que el usuario ha introducido. Webbridge detiene el intento de inicio de sesión inmediatamente.

Seguimientos de CMS Webbridge (mientras que se utiliza ?trace=true)

18 de marzo 14:54:52.698 user.err cmscb3-1 client_backend: ERROR: SamlManager: intento de inicio de sesión SSO no válido

18 de marzo 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Error al encontrar un SSO en la solicitud de token de SAML

18 de marzo 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Intentando encontrar SSO en la solicitud de token de SAML

Escenario 3:

El usuario ha introducido el nombre de usuario correcto y se le presenta la página de inicio de sesión de SSO. El usuario también introduce aquí el nombre de usuario y la contraseña correctos, pero sigue obteniendo el mensaje Error de inicio de sesión

Seguimientos de CMS Webbridge (mientras que se utiliza ?trace=true)

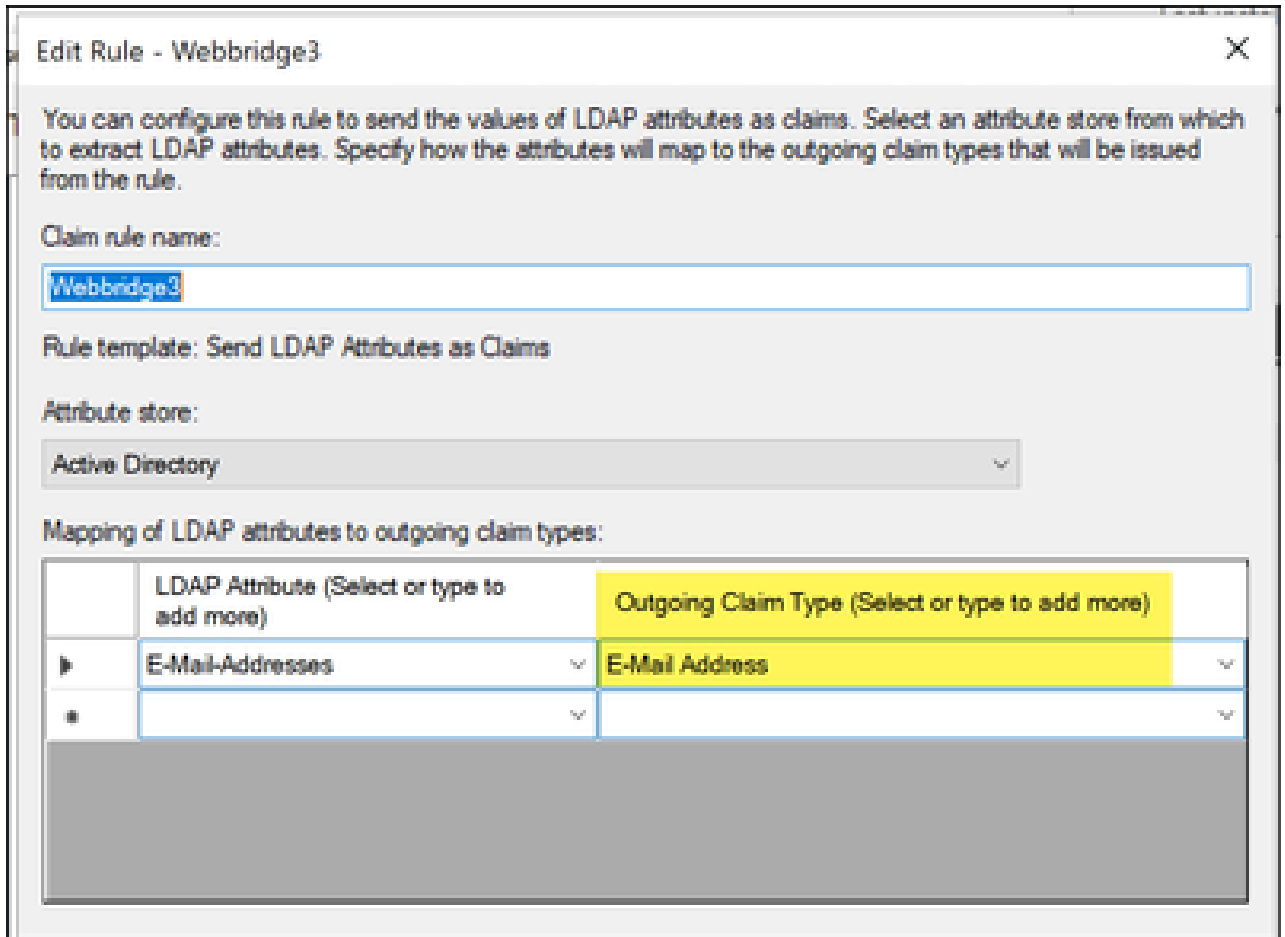
19 de marzo 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Coincidió con SSO sso_2024.zip en la solicitud de token de SAML

19 de marzo 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Intentando encontrar SSO en la respuesta IDP de SAML

19 de marzo 16:39:17.720 user.err cmscb3-1 client_backend: ERROR : SamlManager : No se ha encontrado ningún elemento asignado authenticationId en las aserciones SAML firmadas

19 de marzo 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Error al obtener un authenticationID

La causa del escenario 3 fue que la regla de reclamación en el IdP estaba usando un tipo de reclamación que no coincidía con authenticationIdMapping en el archivo config.json utilizado en el archivo zip de SSO que se cargó en webbridge. Webbridge examina la respuesta SAML y espera que el nombre de atributo coincida con lo configurado en config.json.



Regla de reclamación en ADFS



ejemplo de config.json

El nombre de usuario no se reconoce

Escenario 1:

El usuario ha iniciado sesión con un nombre de usuario incorrecto (el dominio coincide con el contenido del archivo zip de SSO que se cargó en webbridge3, pero el usuario no 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.



en CMS ldapmapping no coincide con el atributo LDAP configurado utilizado para la regla de reclamación en ADFS. La línea siguiente que dice "AuthenticationID:darmckin@brhuff.com obtenido correctamente" indica que ADFS tiene una regla de reclamación configurada con un atributo que obtiene darmckin@brhuff.com de Active Directory, pero AuthenticationID en CMS API > Users muestra que espera darmckin. En CMS ldapMappings, el AuthenticationID se configura como \$sAMAccountName\$, pero la regla de reclamación en ADFS se configura para enviar las direcciones de correo electrónico, por lo que esto no coincide.

Cómo solucionar este problema:

Siga uno de estos procedimientos:

1. Cambie el AuthenticationID en la asignación ldap de CMS para que coincida con lo que se utiliza en la regla de reclamación en ADFS y realice una nueva sincronización
2. Cambie el atributo LDAP utilizado en la regla de reclamación ADFS para que coincida con lo configurado en la asignación LDAP de CMS

Related objects: </api/v1/ldapMappings>

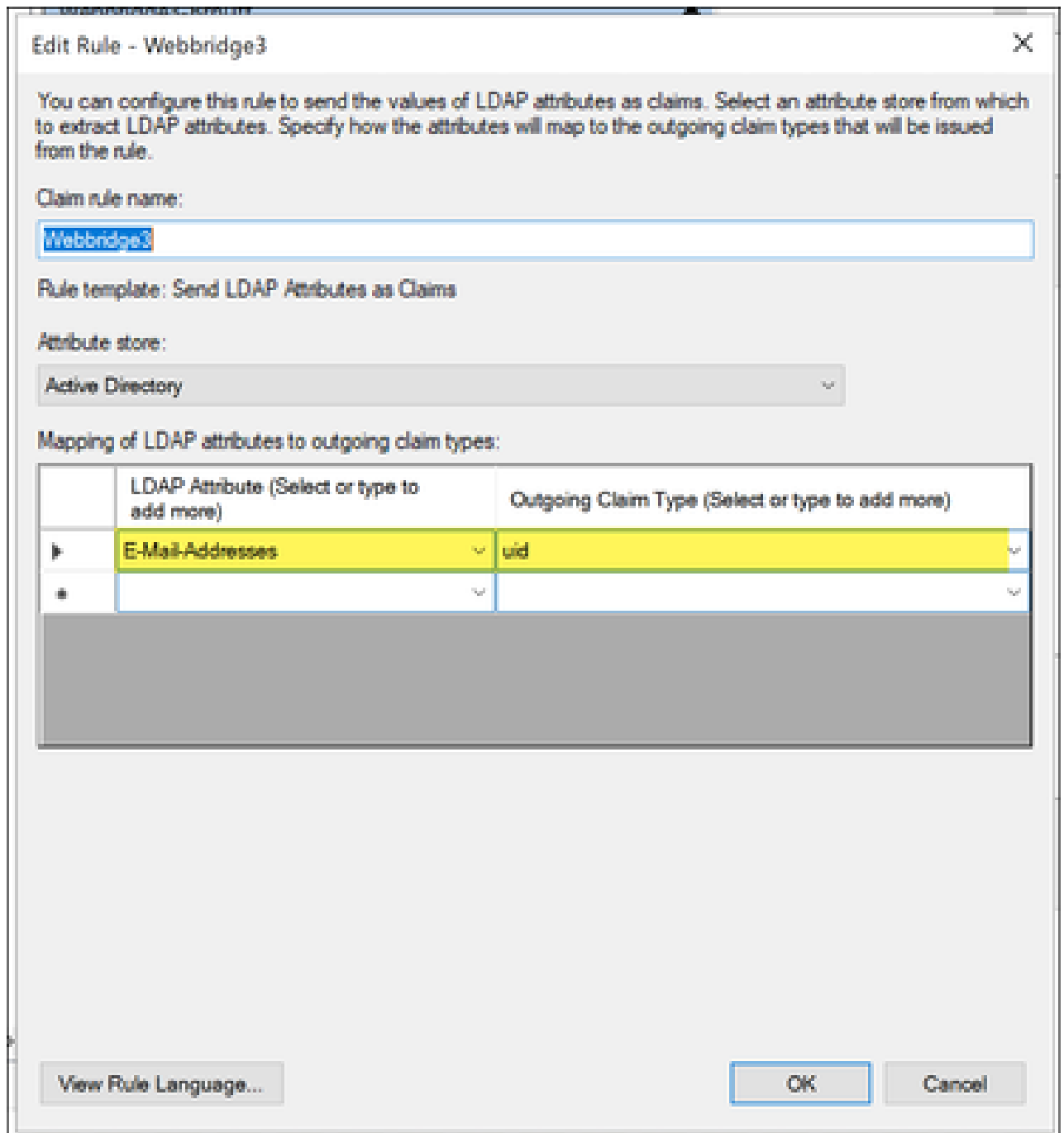
Table view XML view

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

Ejemplo de usuario de API



Regla de reclamación de ADFS

Ejemplo de registro de Webbridge que muestra el registro de trabajo. Ejemplo generado mediante `?trace=true` en la URL de combinación:

18 de marzo 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Coincidió con SSO sso_2024.zip en la solicitud de token de SAML

18 de marzo 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Intentando encontrar SSO en la respuesta de IDP de SAML

18 de marzo 14:24:01.101 user.info cmscb3-1 client_backend: INFO : SamlManager :

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

18 de marzo 14:24:01.102 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-022 72-42a1-b125-136fdf5612a5 (usuario=darmckin@brhuff.com)

18 de marzo 14:24:01.130 user.info cmscb3-1 host:server: INFO: solicitud de inicio de sesión correcta desde darmckin@brhuff.com

18 de marzo 14:24:01.130 user.info cmscb3-1 host:servidor: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] que emite el identificador JWT e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

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

18 de marzo 14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25.247 - [18/Mar/2024:18:24:01 +0000 0] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "<https://adfs.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" to upstream 192.0 2.2:9000: upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).