

# De WebApp SSO op CMS configureren en problemen oplossen

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Configureren](#)

[Netwerkdigram](#)

[ADFS-installatie en initiële installatie](#)

[Toewijzing van CMS-gebruikers aan identiteitsprovider \(IDP\)](#)

[Creëer Webbridge Metadata XML voor IdP](#)

[Metagegevens voor Webbridge importeren naar Identity Provider \(IDP\)](#)

[Creëer Claim Regels voor de Webbridge Service op de IDp](#)

[ZIP-bestand voor SSO-archiefbestand maken voor Webbridge:](#)

[Verkrijg en vorm idp\\_config.xml](#)

[Het configuratie.json bestand met inhoud maken](#)

[Stel de sso\\_sign.key in \(OPTIONEEL\)](#)

[Stel de sso\\_encrypt.key in \(OPTIONEEL\)](#)

[Het SSO ZIP-bestand maken](#)

[Upload de SSO Zip-bestand\(en\) naar Webbridge](#)

[Gemeenschappelijke toegangkaart \(CAC\)](#)

[Inloggen via WebApp](#)

[Probleemoplossing](#)

[Basis probleemoplossing](#)

[Microsoft ADFS-foutcodes](#)

[Verwerving verificatie-ID mislukt](#)

[Geen bewering doorgegeven/gematched in validatie](#)

[Aanmelden mislukt in webapp:](#)

[Scenario 1:](#)

[Scenario 2:](#)

[Scenario 3:](#)

[Gebruikersnaam wordt niet herkend](#)

[Scenario 1:](#)

[Scenario 2:](#)

[Webbridge log toont werklog in voorbeeld. Geproduceerd voorbeeld met ?trace=true in de samengevoegde URL:](#)

[Gerelateerde informatie](#)

---

# Inleiding

Dit document beschrijft hoe u de Cisco Meeting Server (CMS) Web App-implementatie van Single Sign On (SSO) kunt configureren en problemen kunt oplossen.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis van deze onderwerpen te hebben:

- CMS Callbridge versie 3.1 of hoger
- CMS Webbridge versie 3.1 of hoger
- Active Directory-server
- Identificatieprovider (IDP)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrond


CMS 3.1 en later introduceerde de mogelijkheid voor gebruikers om in te loggen met behulp van een SSO zonder de noodzaak om hun wachtwoord in te voeren elke keer dat de gebruiker inlogt, omdat er één sessie wordt gemaakt met de Identify-provider.

Deze functie gebruikt de Security Assertion Markup Language (SAML) versie 2.0 als het SSO-mechanisme.

---

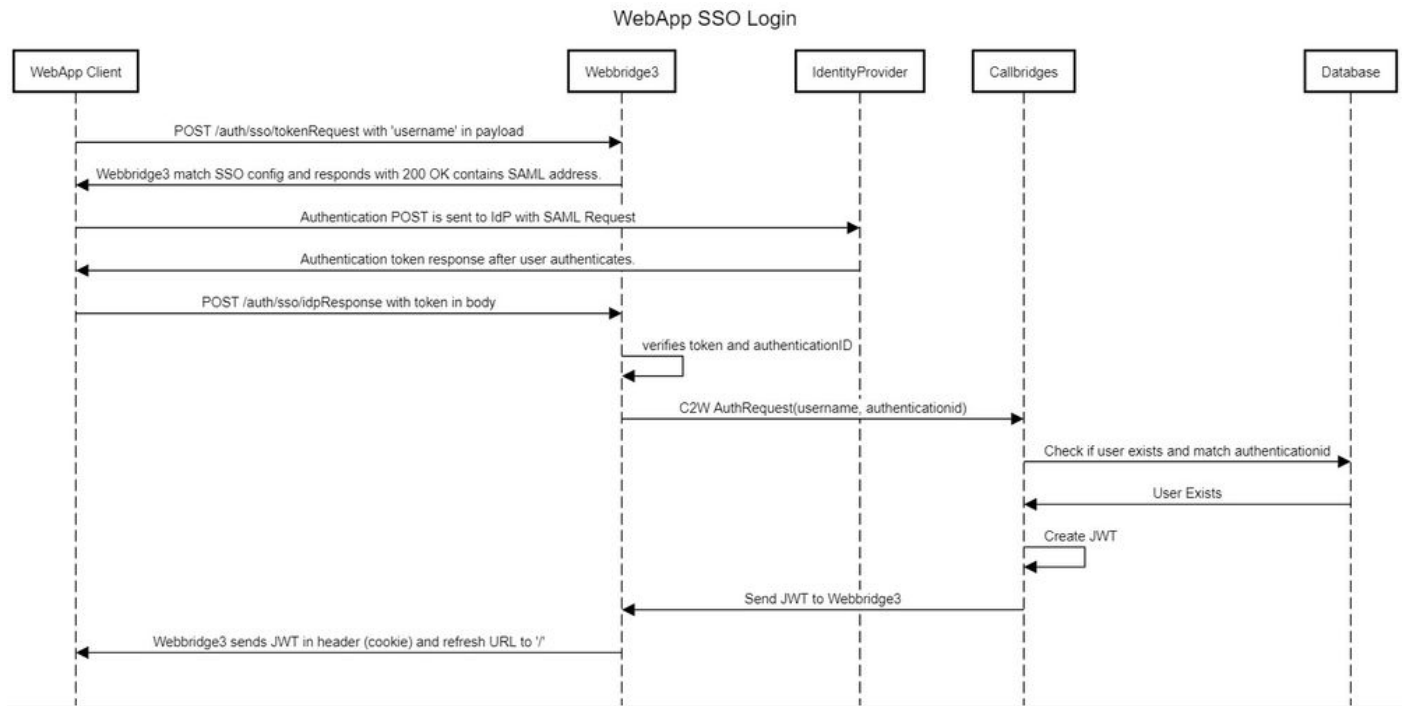
 **Opmerking:** CMS ondersteunt alleen HTTP-POST bindingen in de SAML 2.0 en wijst alle Identify Provider zonder HTTP-POST bindingen af.

---

 **Opmerking:** wanneer SSO is ingeschakeld, is eenvoudige LDAP-verificatie niet meer mogelijk.

## Configureren

## Netwerkdigram



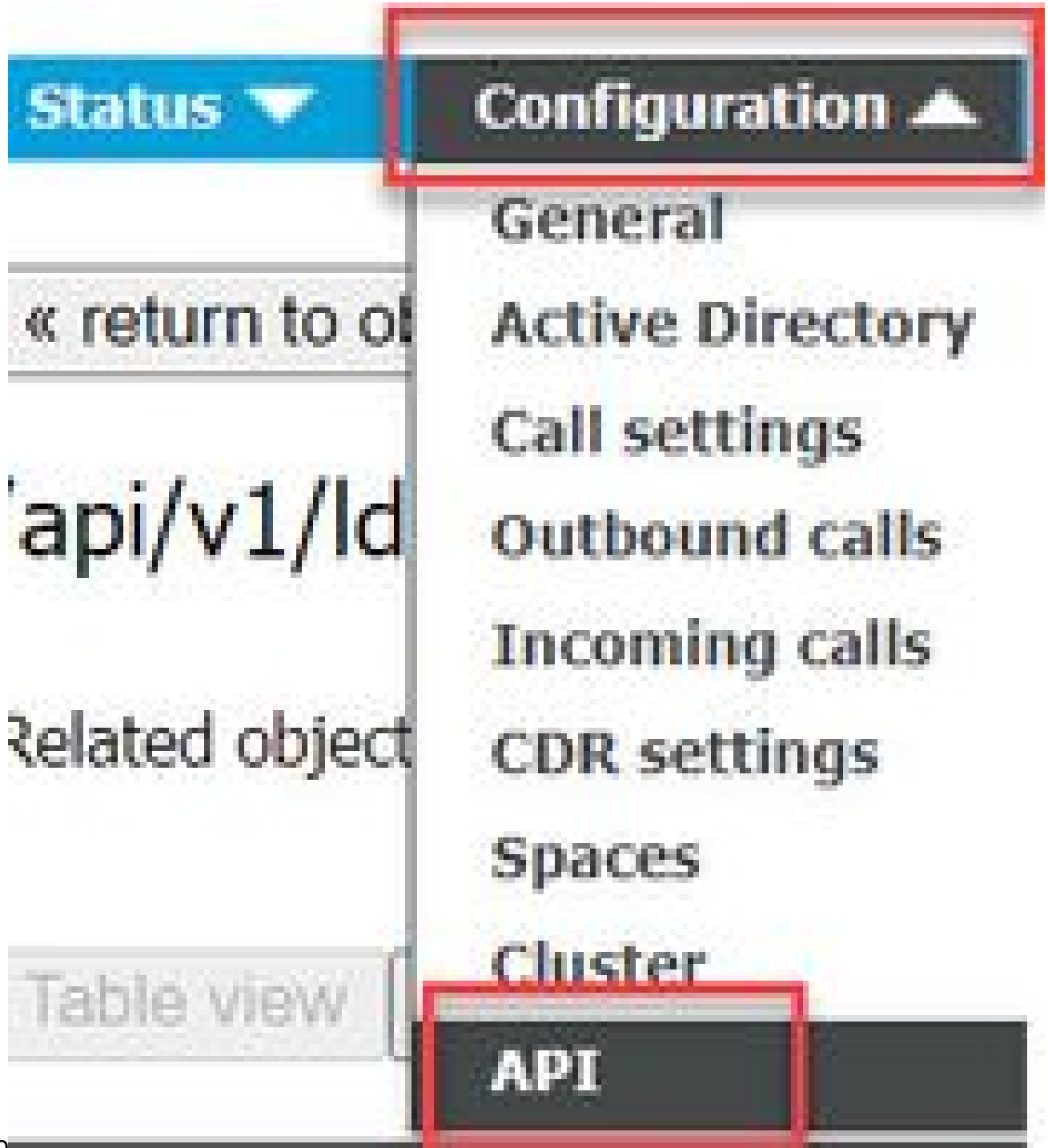
## ADFS-installatie en initiële installatie

In dit implementatiescenario worden Microsoft Active Directory Federation Services (ADFS) gebruikt als Identity Provider (IDP) en daarom wordt voorgesteld om een ADFS (of geplande IDP) te installeren en te laten werken voorafgaand aan deze configuratie.

## Toewijzing van CMS-gebruikers aan identiteitsprovider (IDP)

Om gebruikers geldige authenticatie te laten krijgen, moeten ze worden toegewezen in de Application Programming Interface (API) voor een correlatieveld dat door IdP wordt geleverd. De optie die hiervoor wordt gebruikt is de authenticationIdMapping in de IdapMapping van API.

1. Navigeer naar Configuration > API in de CMS Web Admin GUI



Co

2. Bestaande LDAP-toewijzing (of het maken van een nieuwe LDAP-toewijzing) vinden onder `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
<a href="#">458ad270-860b-4bac-9497-b74278ed2086</a>	\$sAMAccountName\$@brhuff.com

3. In het geselecteerde object ldapMapping werkt u de authenticatieIdMapping bij naar het kenmerk LDAP dat van de IdP wordt doorgegeven. In het voorbeeld wordt de optie \$sAMAccountName gebruikt als LDAP attribuut voor mapping.

**/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

 **Opmerking:** De authenticatieIdMapping wordt door de callbridge/database gebruikt om de claim te valideren die vanuit de IdP in de SAMLResponse is verzonden en de gebruiker een JSON Web Token (JWT) te geven.

4. Voer een LDAP-synchronisatie uit op de ldapSource die is gekoppeld aan de onlangs aangepaste ldapMapping:

Voorbeeld:

**/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>	

5. Nadat de LDAP-synchronisatie is voltooid, navigeer dan in de CMS API in Configuration > api/v1/users en selecteer een gebruiker die is geïmporteerd en controleer of de verificatie-ID correct is ingevuld.

Object configuration	
userId	jdoe@brhuff.com
name	John Doe
email	johndoe@brhuff.com
authenticationId	jdoe
userProfile	<a href="#">d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3</a>

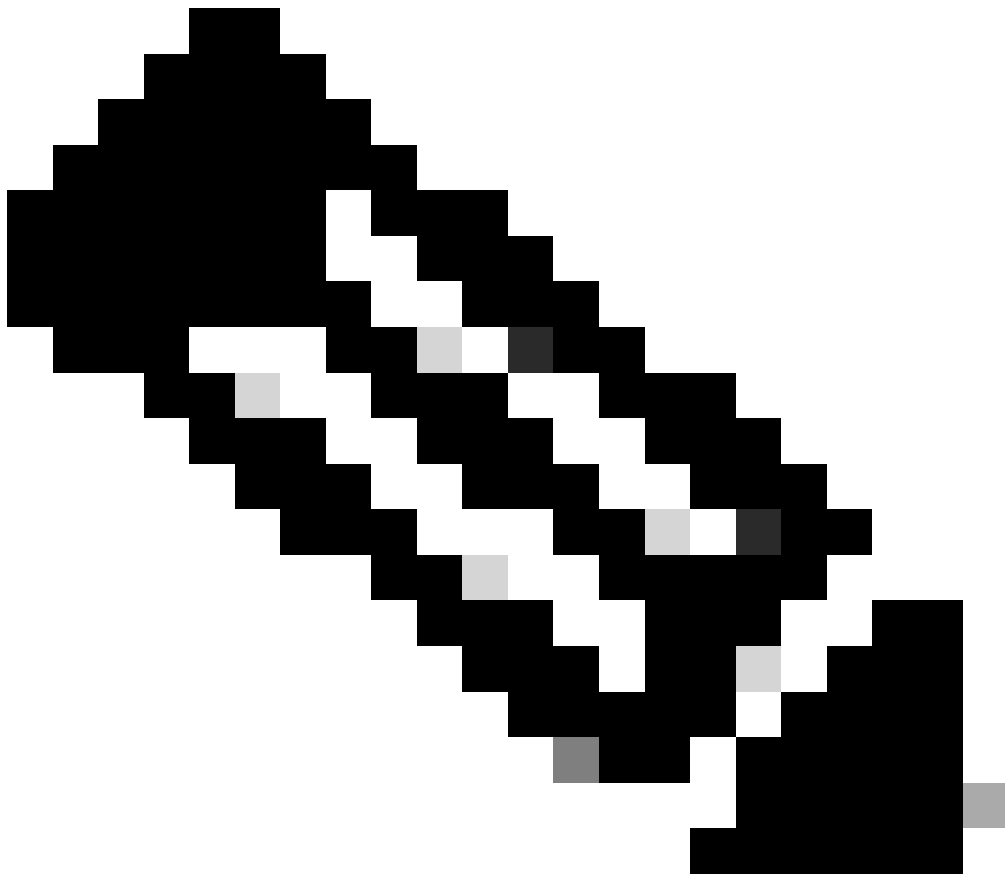
## Creëer Webbridge Metadata XML voor IdP

Met Microsoft ADFS kan een XML-bestand met metagegevens worden geïmporteerd als een Relying Trust Party om de serviceprovider te identificeren die wordt gebruikt. Er zijn een paar manieren om het XML-bestand met metagegevens voor dit doel te maken, maar er zijn een paar eigenschappen die in het bestand aanwezig moeten zijn:

Voorbeeld van Webbridge Metadata met vereiste waarden:

```
<?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 - Dit is het webbridge3-serveradres (FQDN/Hostname) en de bijbehorende poort die door browsers voor gebruikers kan worden bereikt.



Opmerking: als er meerdere webbruggen zijn die één URL gebruiken, moet dit een adres voor taakverdeling zijn.

---

2. Locatie - Dit is de locatie waarin de HTTP-POST AssertionConsumerService voor het Webbridge-adres. Dit is wat de IDp vertelt waar een geverifieerde gebruiker na aanmelding opnieuw te sturen. Dit moet worden ingesteld op de URL voor idpResponse:  
<https://<WebFQDN>:<port>/api/auth/sso/idpResponse>. Bijvoorbeeld  
<https://join.example.com:443/api/auth/sso/idpResponse>.
3. OPTIONEEL - Openbare sleutel voor Ondertekening - dit is de openbare sleutel (certificaat) voor ondertekening, die wordt gebruikt door de IdP om Authrequest van Webbridge te verifiëren. Dit MOET overeenkomen met de privé-sleutel 'sso\_sign.key' op de SSO-bundel die op Webbridge is geüpload, zodat de IDP de openbare sleutel (certificaat) kan gebruiken om de handtekening te verifiëren. U kunt een bestaand certificaat van uw implementatie gebruiken. Open het certificaat in een tekstbestand en kopieer de inhoud naar het bestand Webbridge Metadata. Gebruik de bijpassende sleutel voor het certificaat dat in uw sso\_xxxx.zip bestand wordt gebruikt als het sso\_sign.key bestand.

4. OPTIONEEL - Openbare sleutel voor versleuteling - dit is de openbare sleutel (certificaat) die de IDP gebruikt om SAML-informatie te versleutelen die naar Webbridge wordt teruggestuurd. Dit MOET overeenkomen met de privé-sleutel 'sso\_encrypt.key' op de SSO-bundel die op Webbridge is geüpload, zodat Webbridge kan ontcijferen wat door IdP wordt teruggestuurd. U kunt een bestaand certificaat van uw implementatie gebruiken. Open het certificaat in een tekstbestand en kopieer de inhoud naar het bestand Webbridge Metadata. Gebruik de bijbehorende sleutel voor het certificaat dat in het bestand sso\_xxxx.zip wordt gebruikt als het bestand sso\_encrypt.key.

Voorbeeld van Webbridge Metadata die in IdP moeten worden geïmporteerd met optionele public key (certificaat) data:

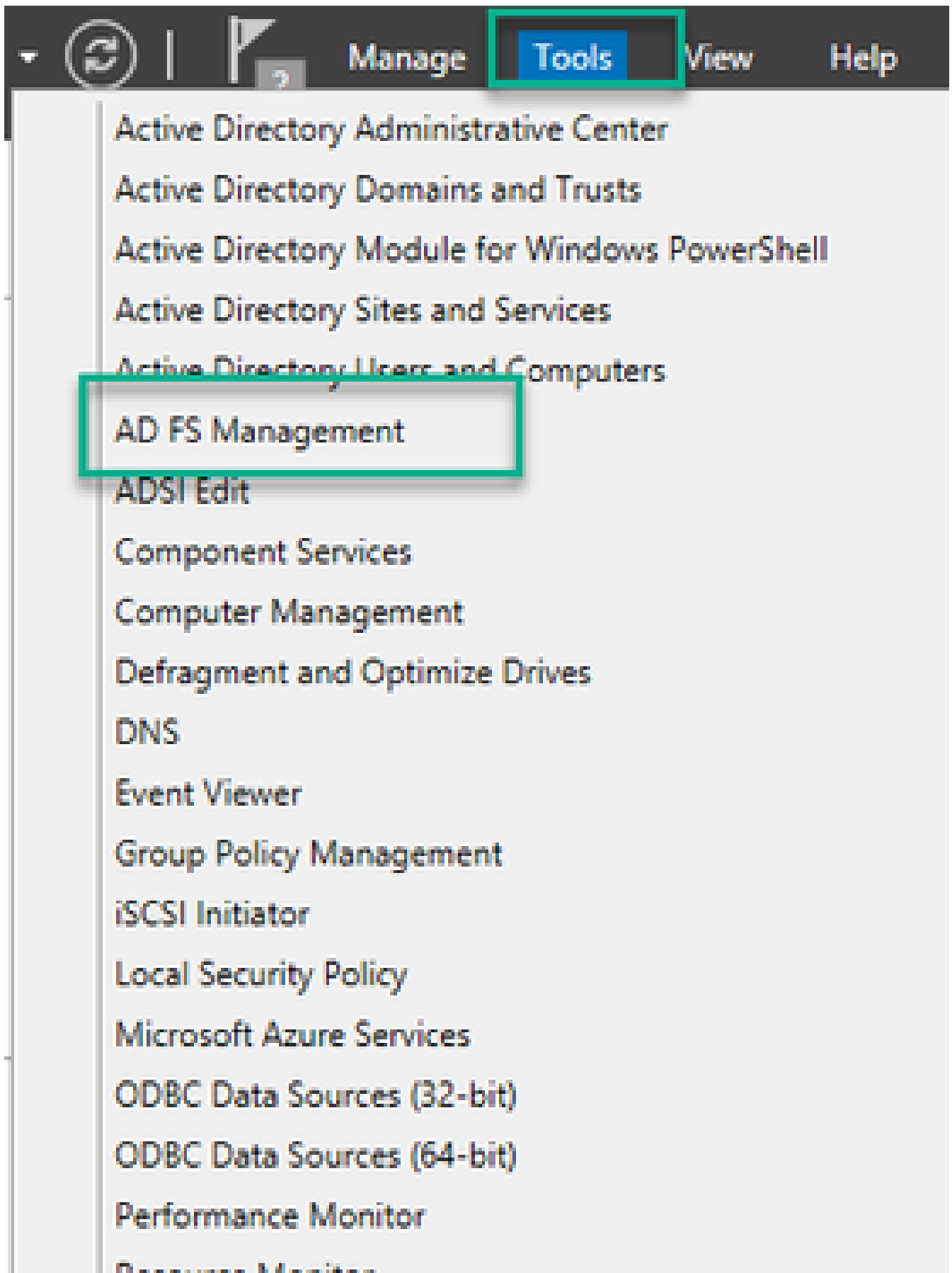
```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
- <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
- <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: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>
```

## Metagegevens voor Webbridge importeren naar Identity Provider (IDP)

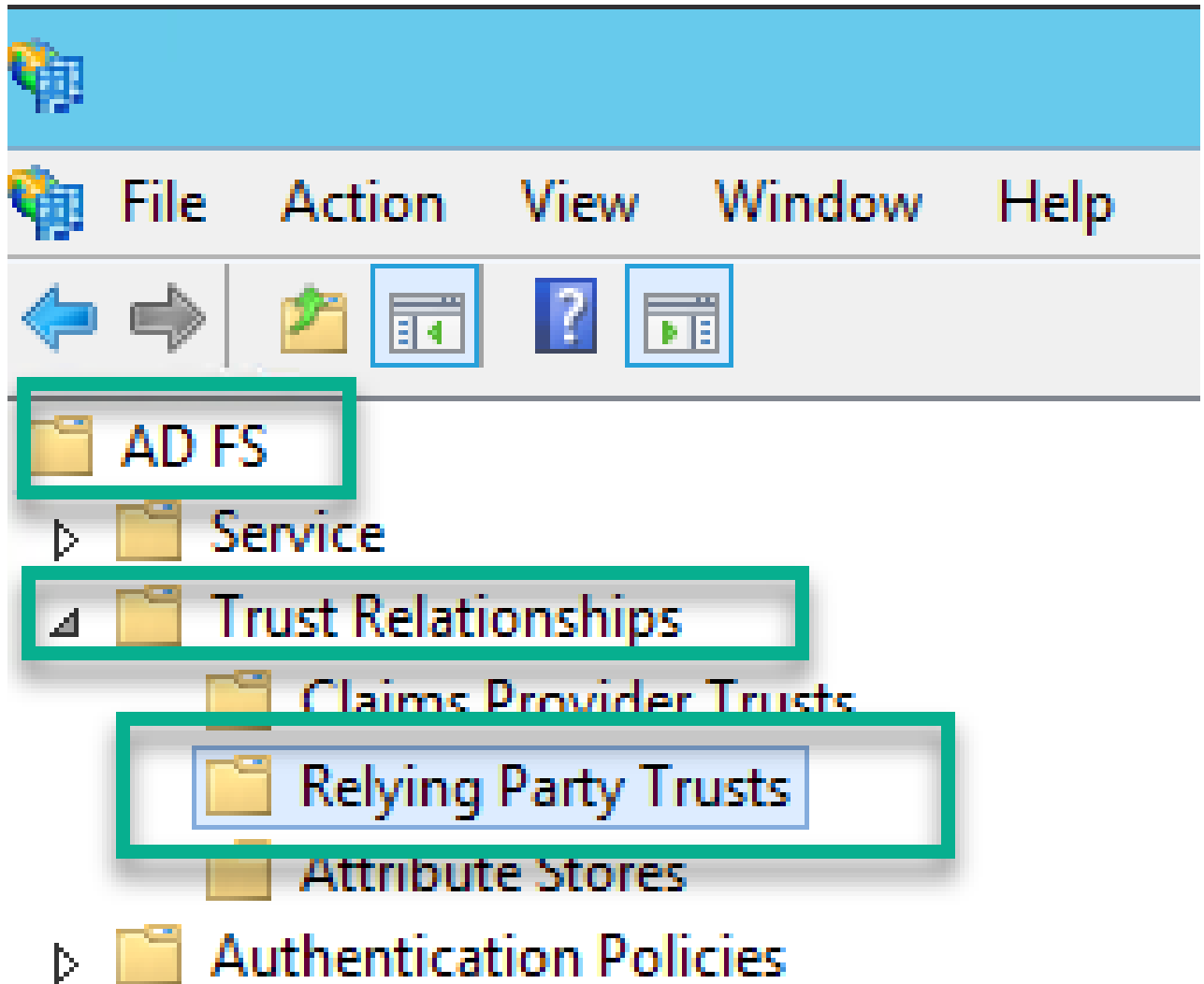
Zodra de Metadata XML is gemaakt met de juiste kenmerken, kan het bestand worden geïmporteerd in de Microsoft ADFS-server om een Relying Trust Party te maken.

1. Remote Desktop naar de Windows-server waarop de ADFS-services worden gehost
2. Open de AD FS-beheerconsole, waartoe u meestal toegang hebt via Serverbeheer.

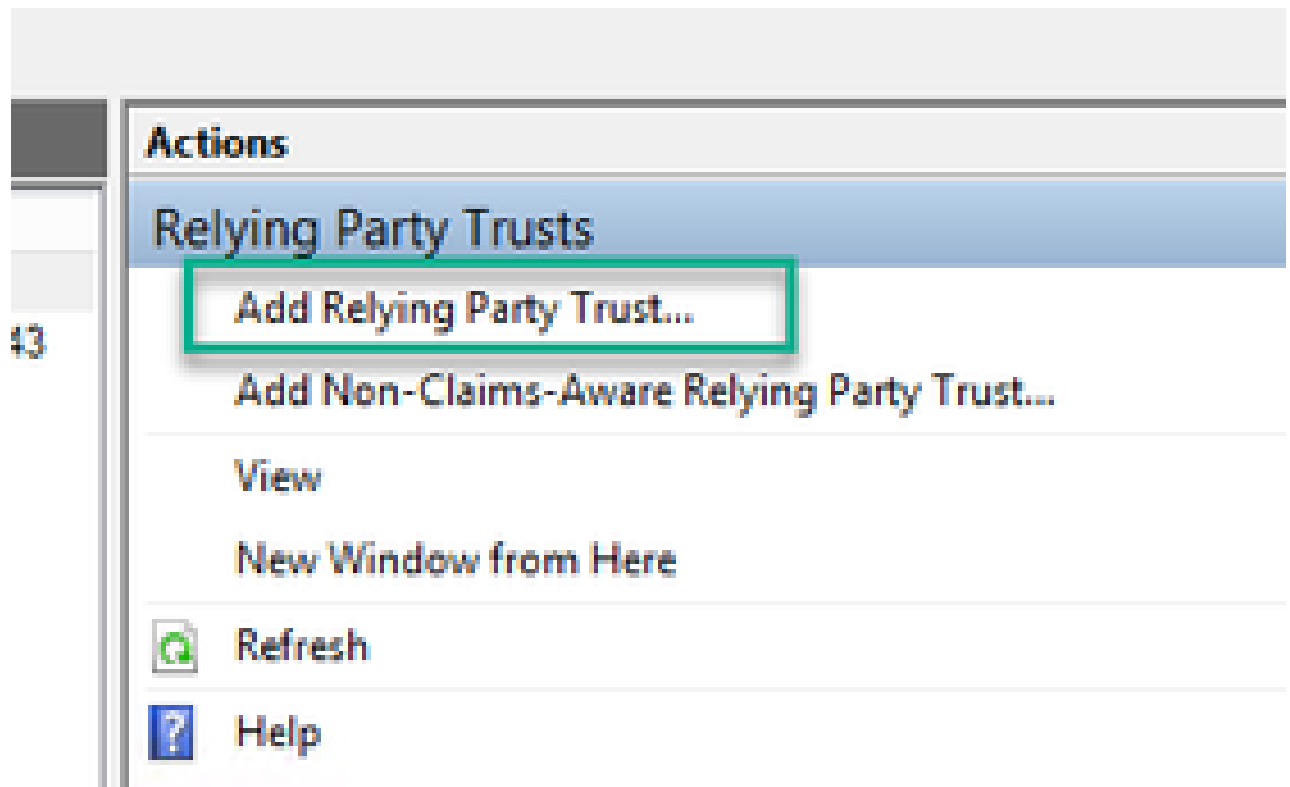




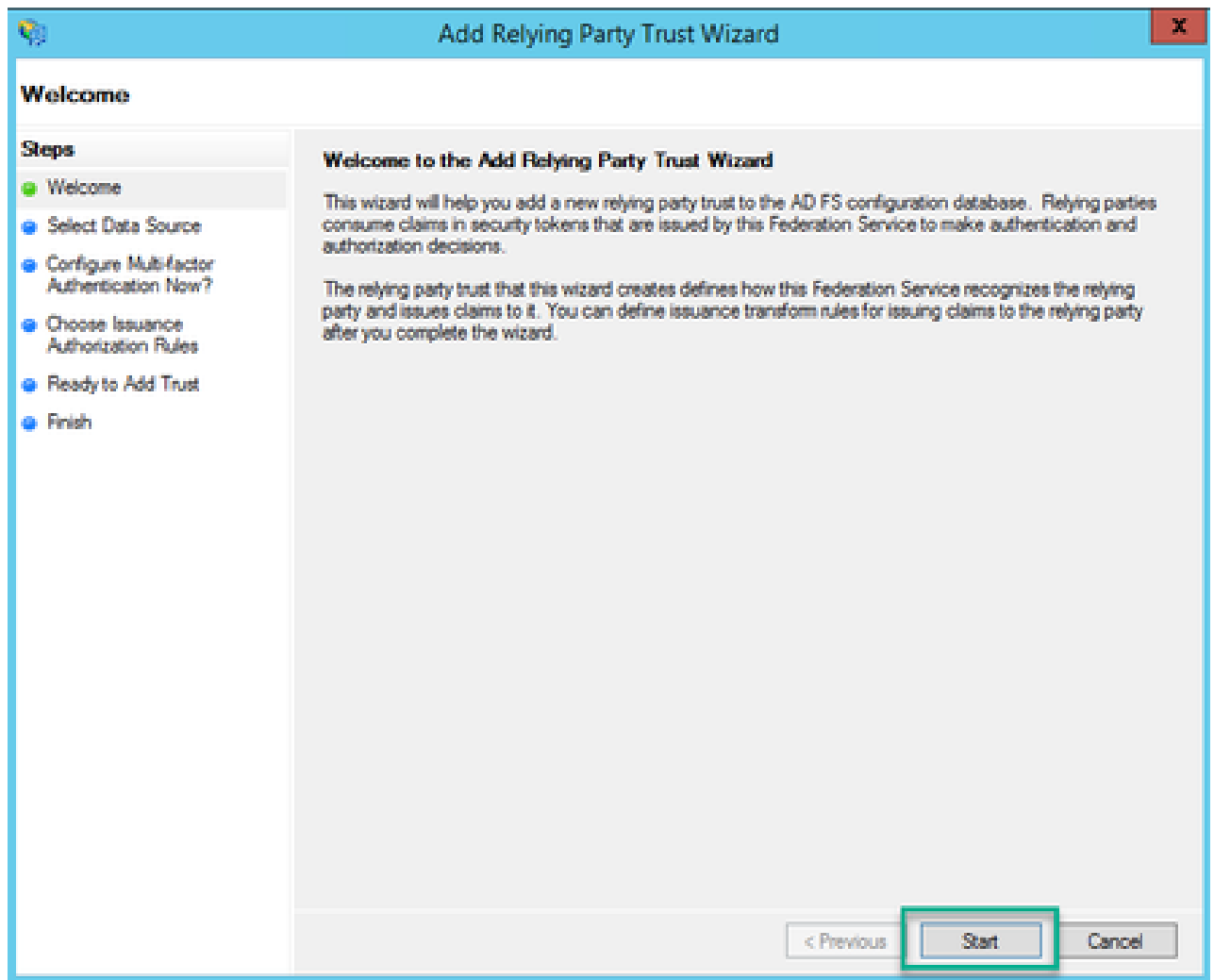
3. Eenmaal in de ADFS Management console, navigeer naar ADFS > Trust Relations > Relying Party Trust in het linker deelvenster.



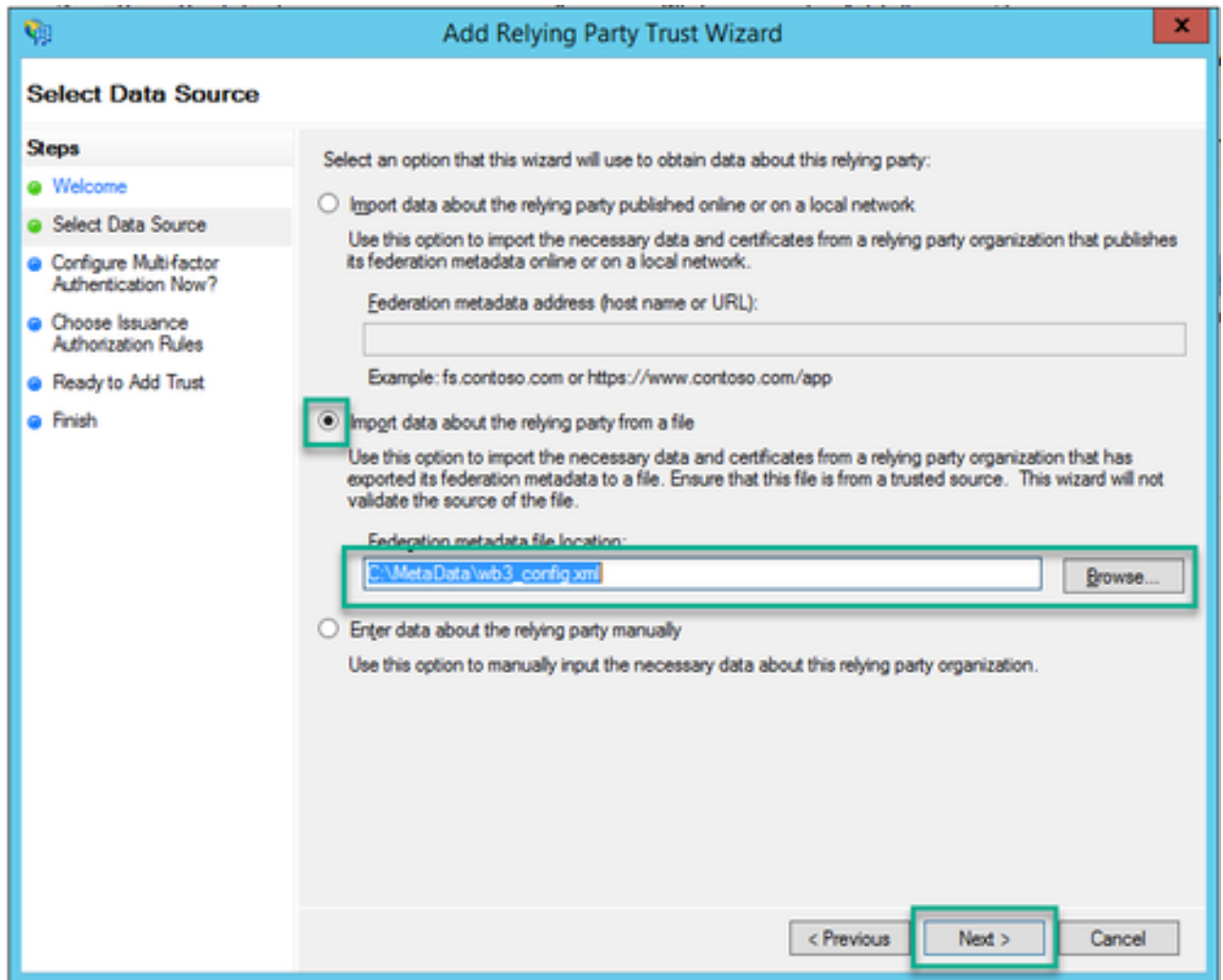
4. Selecteer in het rechterdeelvenster van de ADFS-beheerconsole de optie Relying Party Trust... toevoegen.



5. Nadat u deze optie hebt geselecteerd, wordt de Add Relying Party Trust Wizard geopend. Selecteer de optie Start.



6. Op de pagina Select Data Source selecteert u het keuzerondje voor het importeren van gegevens over de vertrouwende partij uit een bestand en selecteert u Bladeren en navigeert u naar de locatie van het Webbridge MetaData-bestand.



7. Op de pagina Weergavenaam opgeven, zet u een naam die voor de entiteit moet worden weergegeven in ADFS (de weergavenaam heeft geen serverfunctie voor de ADFS-communicatie en is louter informatie).

The image shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The current step is "Specify Display Name". On the left, a "Steps" list shows the progress: "Welcome" (completed), "Select Data Source" (completed), "Specify Display Name" (current step), "Configure Multi-factor Authentication Now?" (pending), "Choose Issuance Authorization Rules" (pending), "Ready to Add Trust" (pending), and "Finish" (pending). The main area contains a text box for "Display name:" with the value "Webbridge CMS SSO" entered. Below it is a "Notes:" text area containing the text "This is the relying trust part for CMS SSO with WebApp". At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

**Add Relying Party Trust Wizard**

**Specify Display Name**

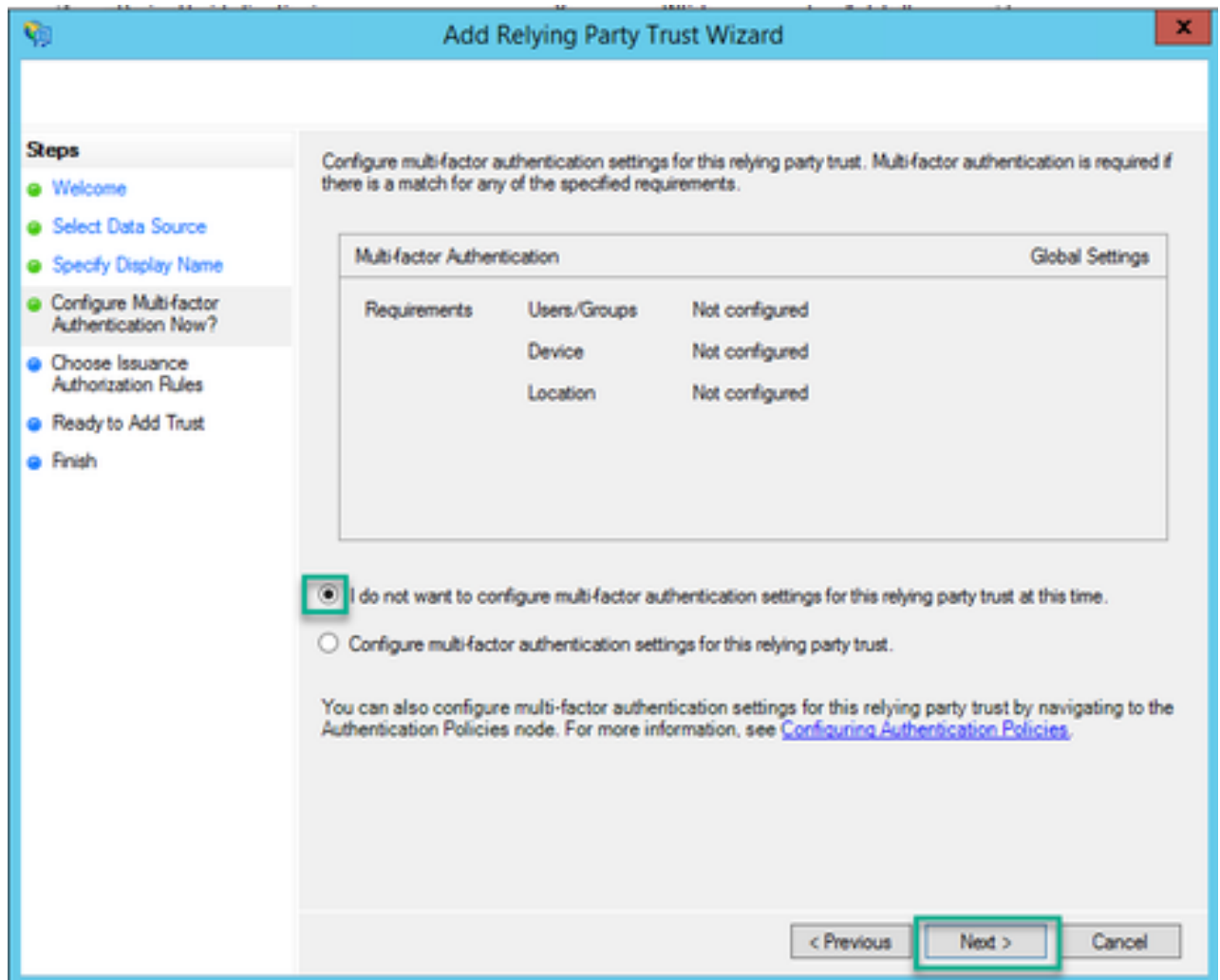
Enter the display name and any optional notes for this relying party.

Display name: Webbridge CMS SSO

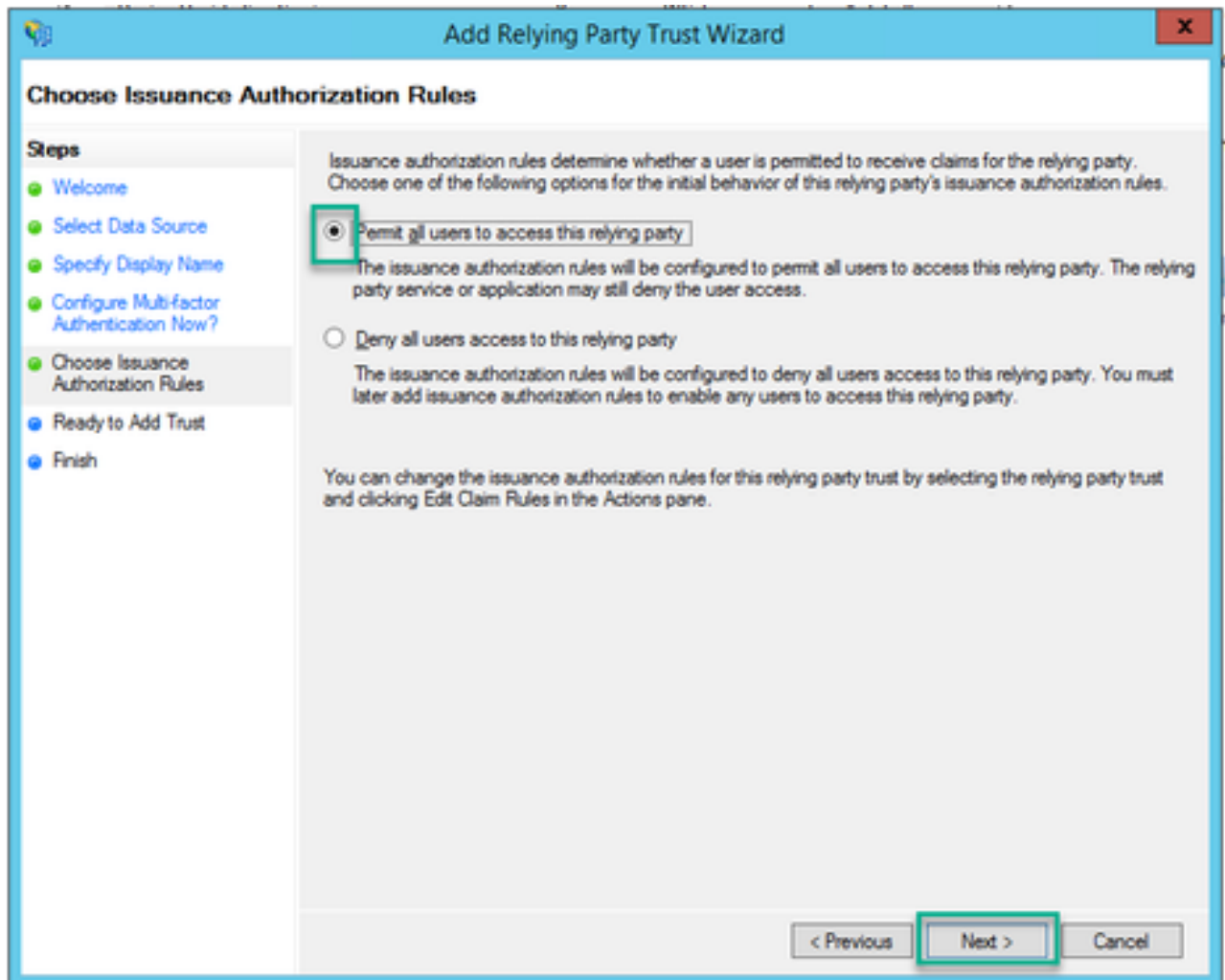
Notes: This is the relying trust part for CMS SSO with WebApp

< Previous   Next >   Cancel

8. Ga op de pagina "Nu verificatie met meerdere factoren configureren" als standaard naar veld en selecteer Volgende.

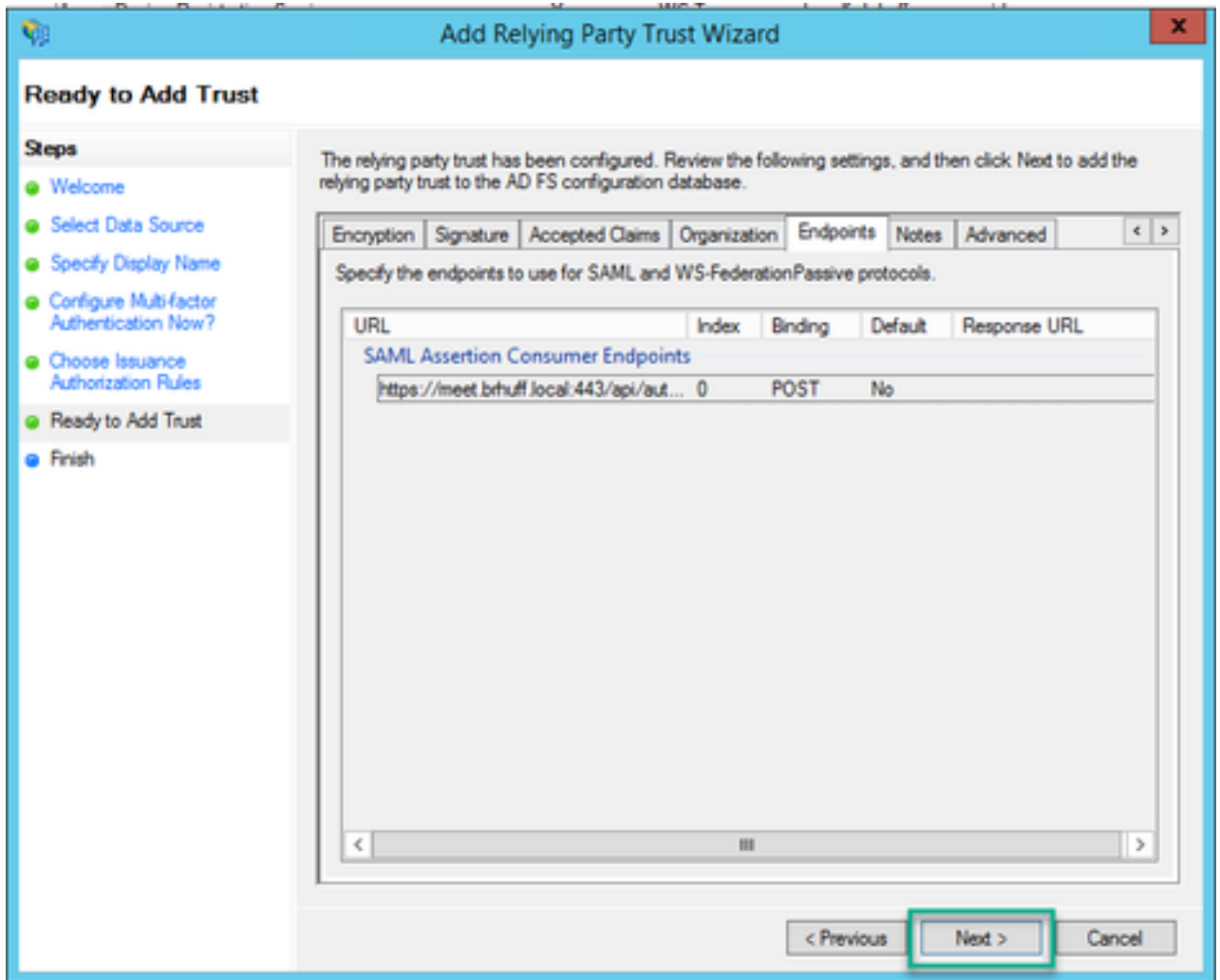


9. Ga op de pagina Kies de regels voor uitgifte als geselecteerd voor toestemming voor alle gebruikers om toegang te krijgen tot deze vertrouwende partij.

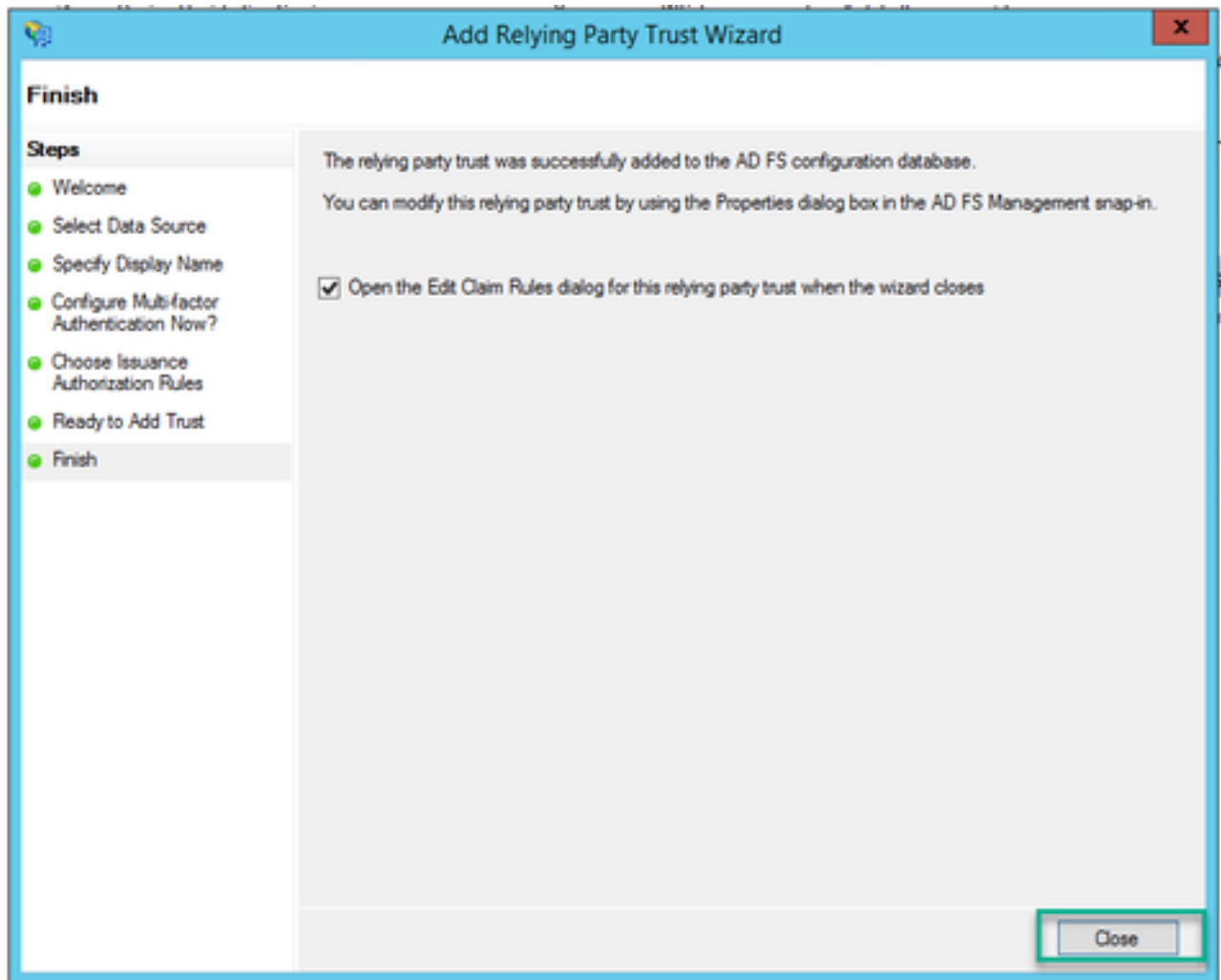


10. Op de pagina Klaar om vertrouwen toe te voegen, kunnen de geïmporteerde gegevens van de Relying Trust Party for Webbridge worden bekeken via de tabbladen. Controleer de identificatoren en endpoints op de URL-gegevens van Webbridge Service Provider.





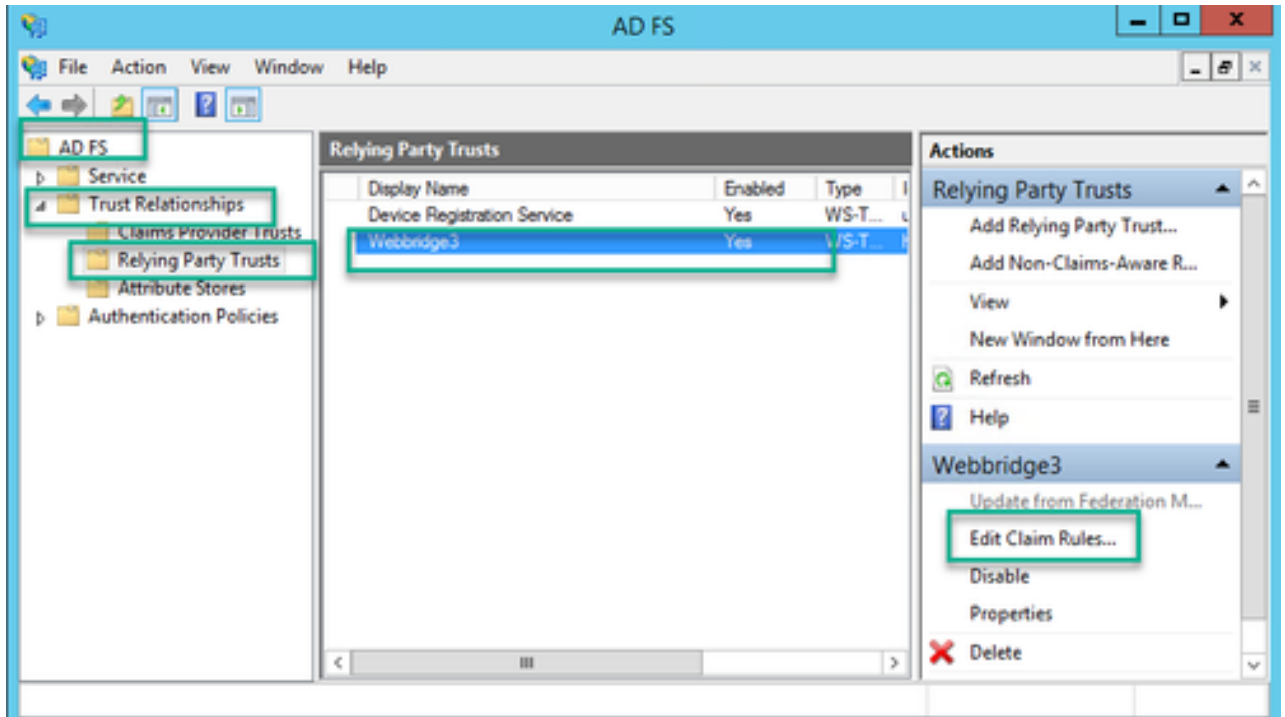
1. Selecteer op de pagina Voltoeien de optie Sluiten om de wizard te sluiten en door te gaan met het bewerken van de claimregels.



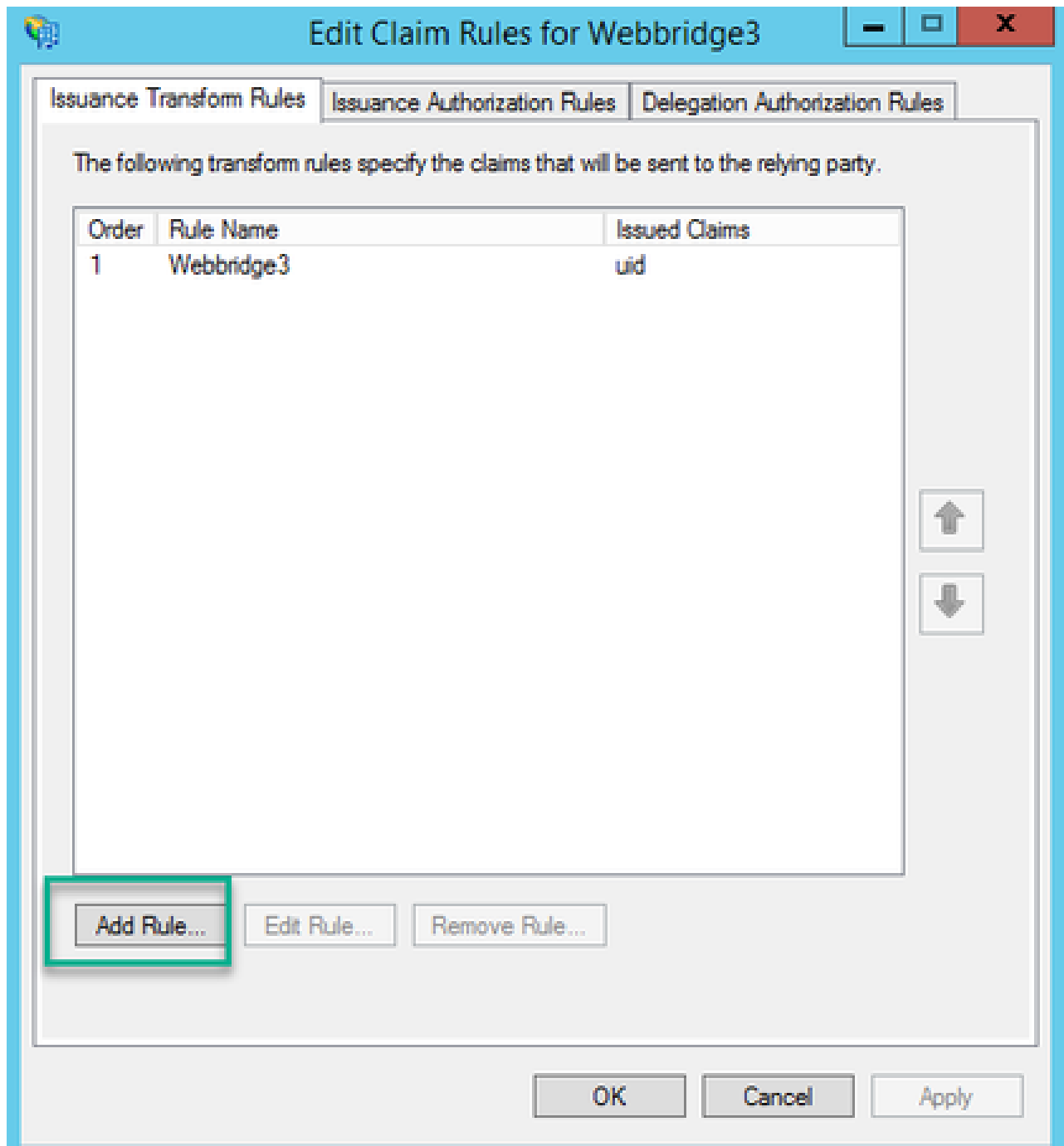
## Creëer Claim Regels voor de Webbridge Service op de IDp

Nu de Relying Party Trust is gecreëerd voor de Webbridge, kunnen claimregels worden gemaakt om specifieke LDAP-kenmerken te koppelen aan uitgaande claimtypen die in de SAML Response aan de Webbridge moeten worden geleverd.

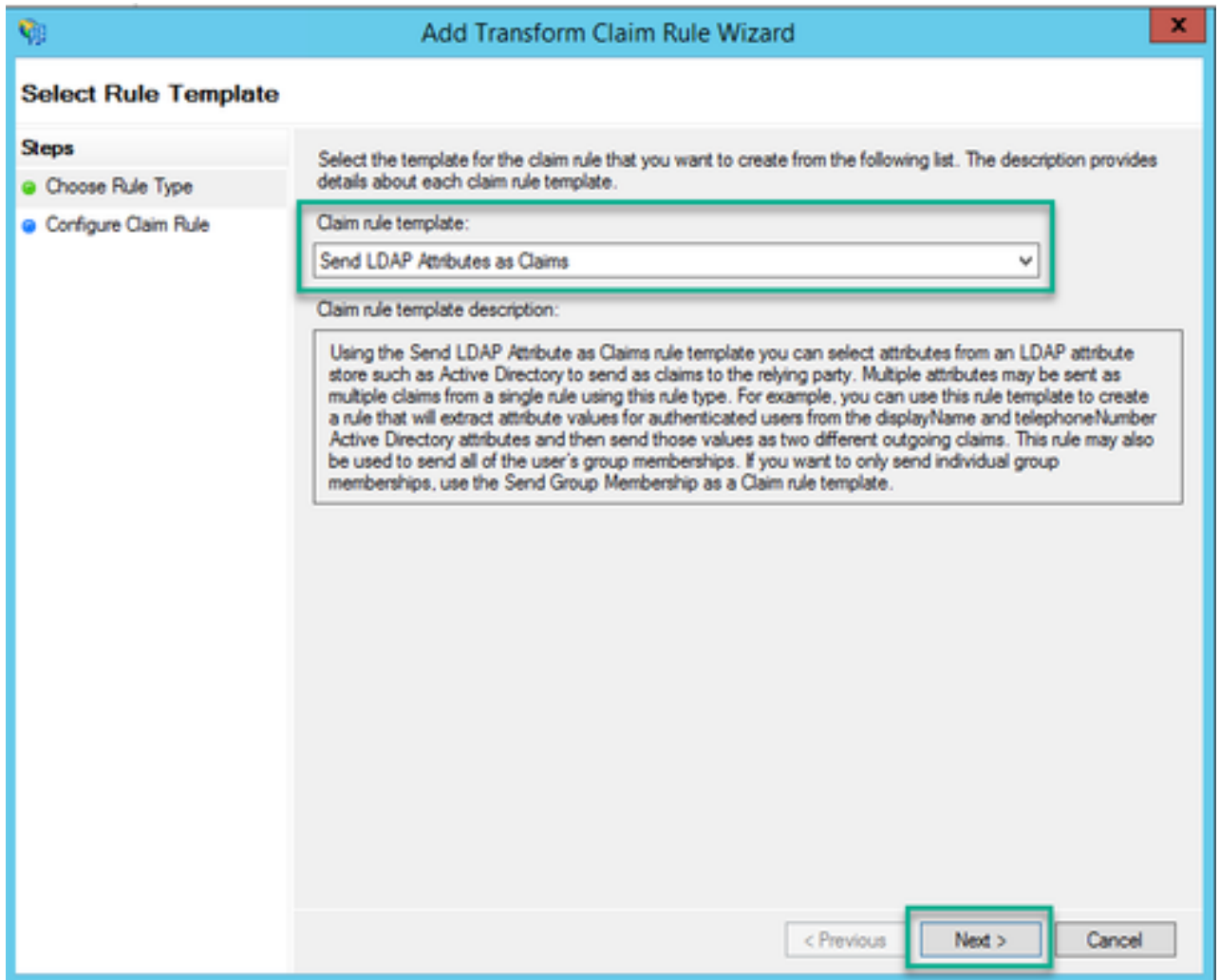
1. Markeer in de ADFS Management console de Relying Party Trust voor de Webbridge en selecteer Bewerken Claim Rules in het rechterdeelvenster.



2. Selecteer op de pagina Claimregels voor <DisplayName> bewerken de regel Toevoegen....



3. Op de pagina Add Transform Claim Rule Wizard selecteert u Send LDAP Attributes as Claims for the Claim rule template en selecteert u Next.



4. Op de pagina Claimregel configureren, configureer de claimregel voor het Relying Party Trust met deze waarden:

1. Claim rule name = dit moet een naam zijn die aan de regel is gegeven in ADFS (alleen voor regelverwijzing)
2. Attribuut Store = Active Directory
3. LDAP Attribute = Dit moet overeenkomen met de authenticatieIdMapping in de CallBridge API. (Bijvoorbeeld \$sAMAccountName\$.)
4. Uitgaande Claim Type = Dit moet overeenkomen met de authenticatieIdMapping in de Webbridge SSO config.json. (Bijvoorbeeld, 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

## ZIP-bestand voor SSO-archiefbestand maken voor Webbridge:

Deze configuratie is wat de verwijzingen Webbridge om de configuratie SSO voor ondersteunde domeinen, authenticatieafbeelding, etc. te bevestigen. Voor dit deel van de configuratie moeten deze regels in acht worden genomen:

- Het ZIP-bestand MOET beginnen met sso\_prefix aan de bestandsnaam (bijvoorbeeld sso\_cmmost.zip).
- Zodra dit bestand is geüpload, schakelt Webbridge basisverificatie uit en kan ALLEEN SSO worden gebruikt voor de Webbridge waarnaar dit is geüpload.

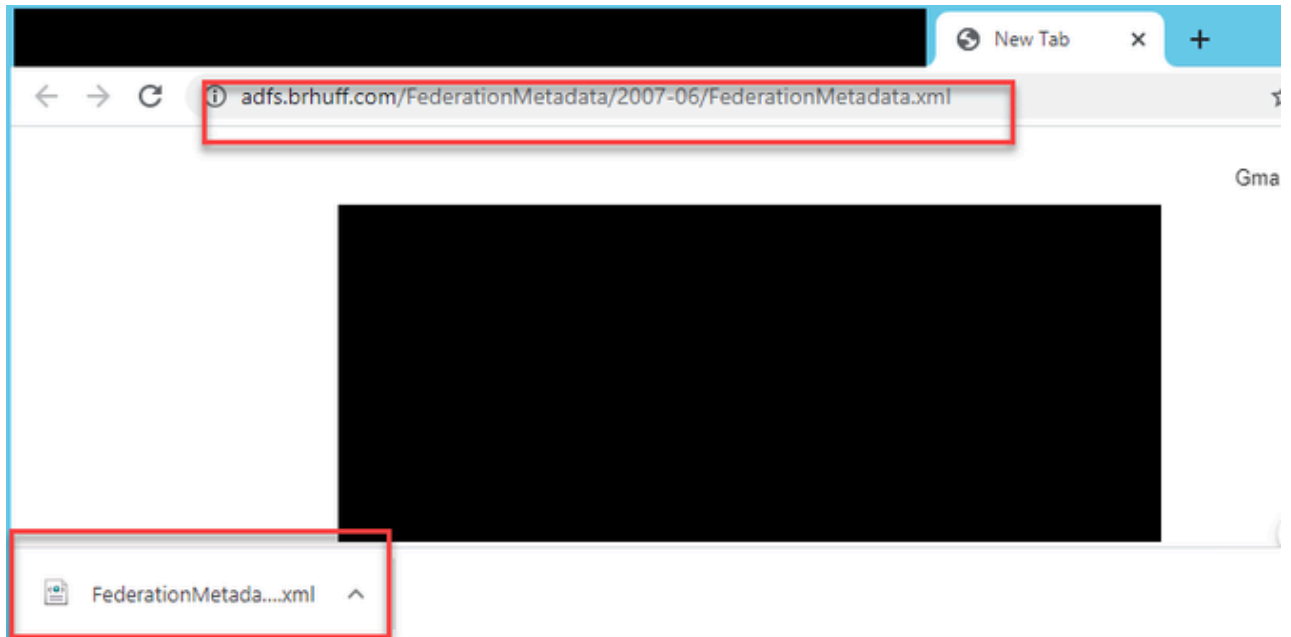
- Als er meerdere Identity Providers worden gebruikt, moet er een apart ZIP-bestand geüpload worden met een ander naamgevingsschema (nog steeds vooraf ingesteld met de sso\_).
- Wanneer u een zip-bestand maakt, moet u de inhoud van het bestand markeren en zippen, en de gewenste bestanden niet in een map stoppen en die map zippen.

De inhoud van het zip-bestand bestaat uit 2 tot 4 bestanden, afhankelijk van het feit of er wel of geen encryptie wordt gebruikt.

Bestandsnaam	Beschrijving	Vereist?
idp_config.xml	Dit is het MetaData-bestand dat kan worden verzameld door de idP. In ADFS kan dit worden gevonden door naar <a href="https://&lt;ADFSFQDN&gt;/FederationMetadata/2007-06/FederationMetadata.xml">https://&lt;ADFSFQDN&gt;/FederationMetadata/2007-06/FederationMetadata.xml</a> te gaan.	JA
config.json	Dit is het JSON-bestand waarin Webbridge gebruikt om de ondersteunde domeinen te valideren, authenticatie mapping voor SSO.	JA
sso_sign.key	Dit is de privé-sleutel voor openbare ondertekeningsleutel die op de Identify-provider is geconfigureerd. Alleen nodig voor het beveiligen van de ondertekende gegevens	NEE
sso_encrypt.key	Dit is de privé-sleutel voor de openbare versleutelingsleutel die op de Identificatieprovider is geconfigureerd. Alleen nodig voor het beveiligen van de versleutelde gegevens	NEE

## Verkrijg en vorm idp\_config.xml

1. Open op de ADFS-server (of een locatie die toegang heeft tot de ADFS) een webbrowser.
2. Voer in de webbrowser URL in: <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml> (u kunt ook localhost gebruiken in plaats van FQDN als u lokaal op de ADFS-server bent). Dit downloadt het bestand FederationMetadata.xml.



3. Kopieer het gedownloade bestand naar een locatie waar het zip-bestand wordt gemaakt en hernoem het naar 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

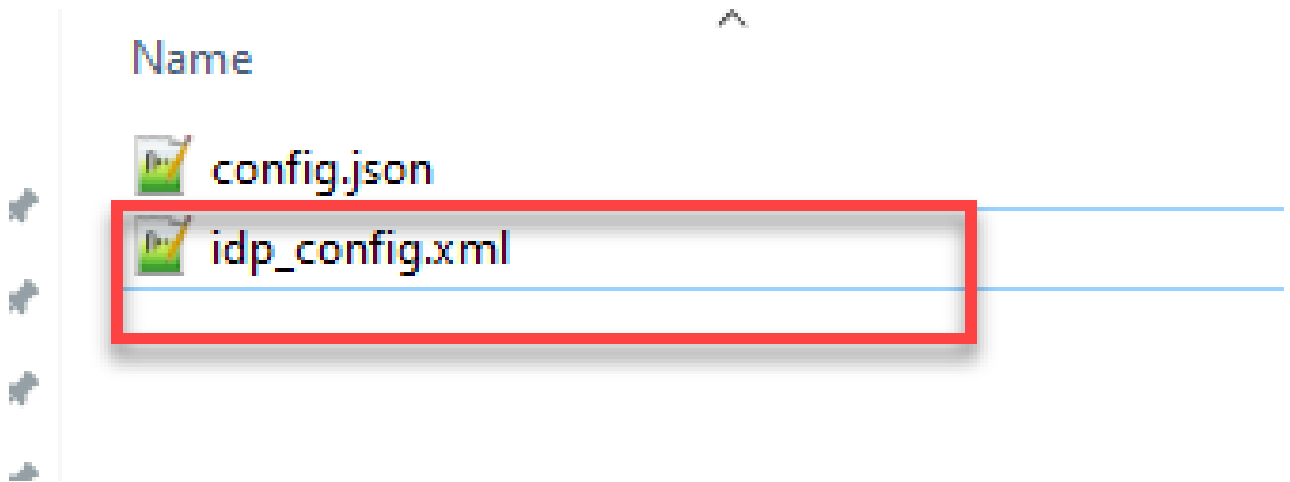
Copy

Create shortcut

Delete

Rename

Properties



### Het configuratie.json-bestand met inhoud maken

De config.json bevat deze 3 eigenschappen en ze moeten tussen haakjes geplaatst worden, {}:

1. SupportDomains - Dit is een lijst van domeinen die worden gecontroleerd op SSO-verificatie tegen de IDp. Er kunnen meerdere domeinen van elkaar worden gescheiden door een komma.
2. authenticatielDMapping - Dit is de parameter die wordt doorgegeven als deel van de uitgaande claimregel van de ADFS/IdP. Dit moet overeenkomen met de naamwaarde van het type uitgaande claim op de IDp. Claimregel.
3. ssoServiceProviderAddress - Dit is de FQDN URL waarop de Identify Provider de SAML antwoorden verstuurt. Dit moet de Webbridge FQDN zijn.

**Configured as 'uid' to match outgoing claim on ADFS**

**the URL of Webbridge for IdP to send response to**

**supported domain of 'brhuff.com' for SSO authentication**

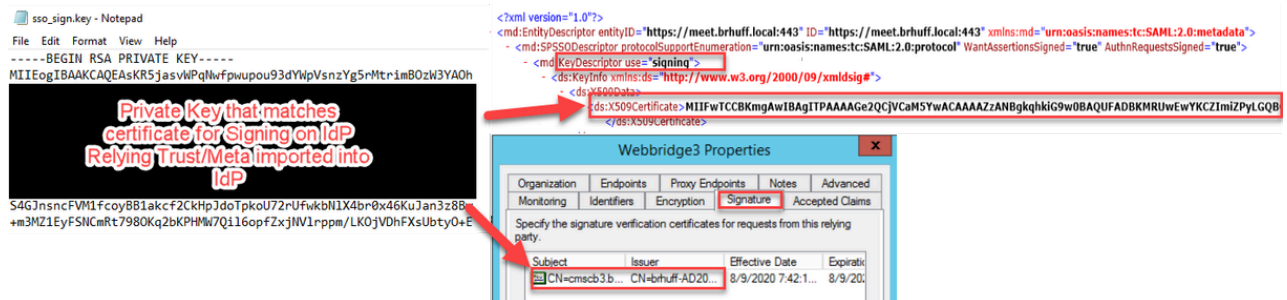
**Make sure the LDAP attribute used in ADFS for the Claim rule matches the authenticationIdMapping in the CMS API**

## Stel de sso\_sign.key in (OPTIONEEL)

Dit bestand moet de privé-sleutel bevatten van het certificaat dat wordt gebruikt voor het ondertekenen in de Webbridge-metagegevens die in de IdP zijn geïmporteerd. Het certificaat dat wordt gebruikt voor ondertekening kan worden ingesteld tijdens het importeren van de Webbridge-metagegevens in de ADFS door het X509Certificate te vullen met de certificaatinformatie onder de sectie <KeyDescriptor use=sign>. Het kan ook worden bekeken (en geïmporteerd) op ADFS in de Webbridge Relying Trust Party onder Properties > Signature.

In het volgende voorbeeld, kunt u het callbridge certificaat (CN=cmscb3.brhuff.local) zien, dat aan de meta-gegevens Webbridge voorafgaand aan wordt ingevoerd in ADFS werd toegevoegd. De privésleutel die in de sso\_sign.key is ingebracht is die die het cmscb3.brhuff.local certificaat aanpast.

Dit is een optionele configuratie en is alleen nodig als u de SAML Responses wilt versleutelen.

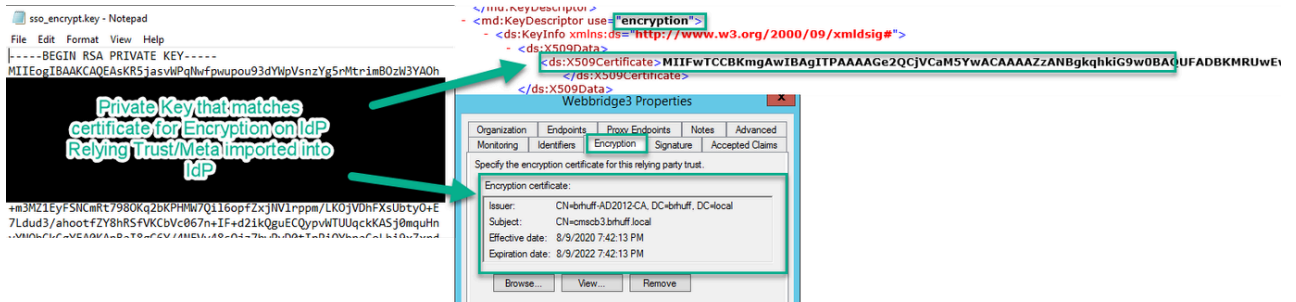


## Stel de sso\_encrypt.key in (OPTIONEEL)

Dit bestand moet de privé-sleutel bevatten van het certificaat dat wordt gebruikt voor de versleuteling in de webbridge-metadata die in de IdP is geïmporteerd. Het certificaat dat voor versleuteling wordt gebruikt, kan worden ingesteld tijdens het importeren van de Webbridge-metagegevens in de ADFS door het X509Certificate te vullen met de certificaatinformatie onder de sectie <KeyDescriptor use=encryptie>. Het kan ook worden bekeken (en geïmporteerd) op ADFS in de Webbridge Relying Trust Party onder Properties > Encryption.

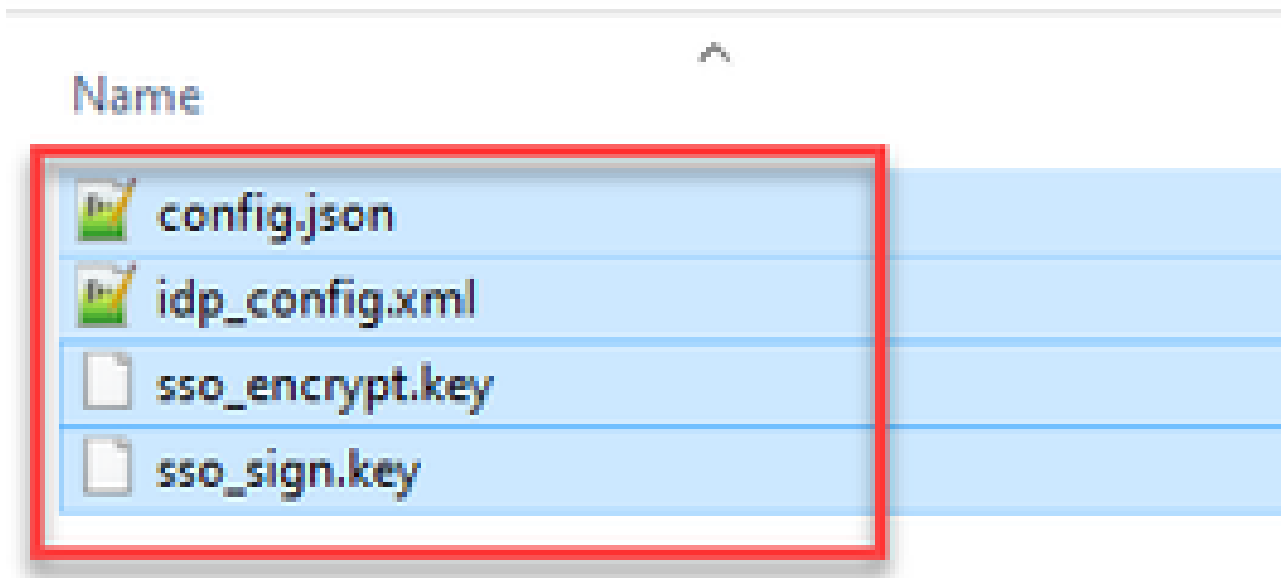
In het volgende voorbeeld, kunt u het callbridge certificaat (CN=cmscb3.brhuff.local) zien, dat werd toegevoegd aan de Webbridge-metagegevens voorafgaand aan de invoer in ADFS. De privé-sleutel die in de 'sso\_encrypt.key' wordt ingevoegd, is degene die overeenkomt met het cmscb3.brhuff.local certificaat.

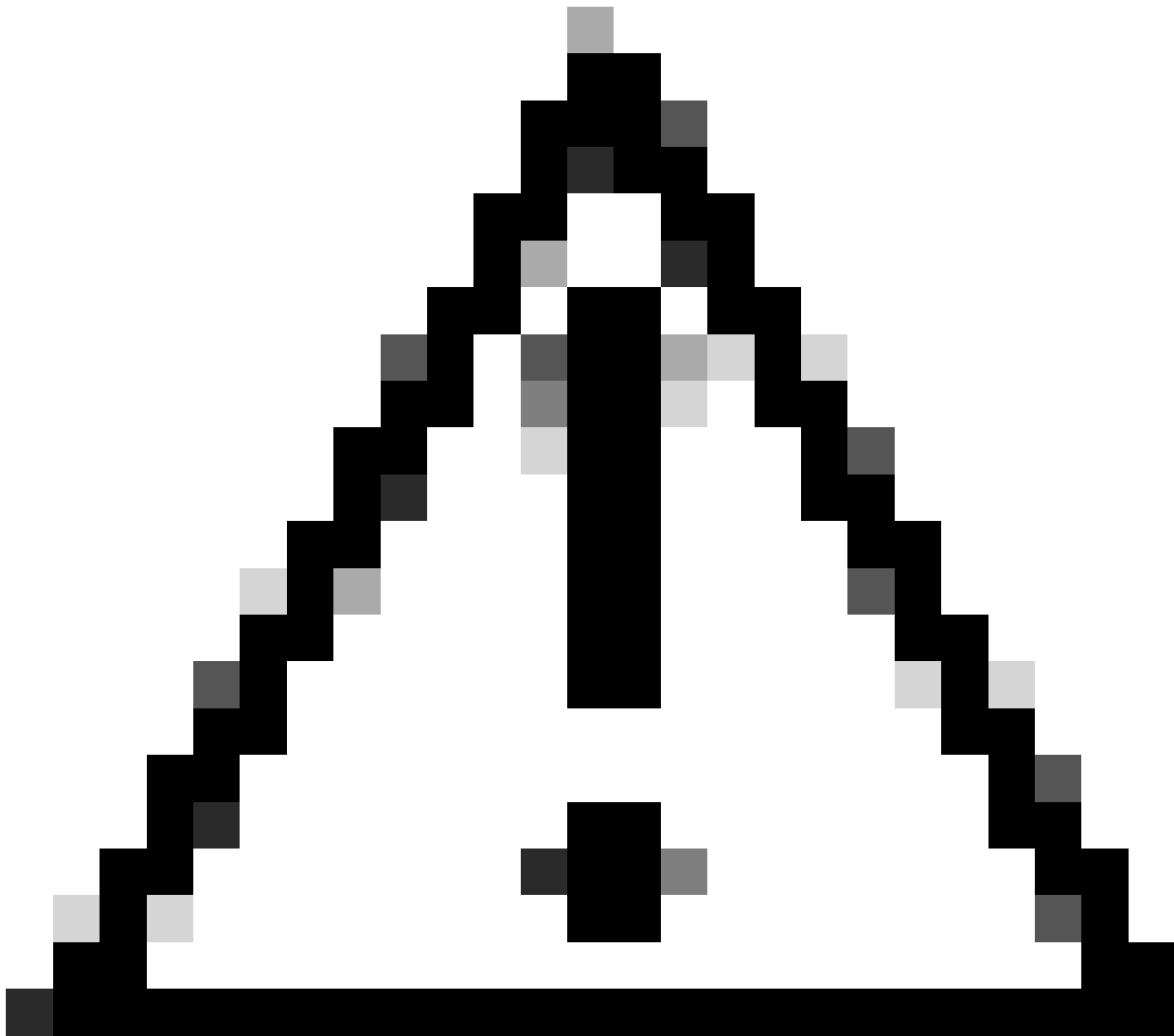
Dit is een optionele configuratie en deze is alleen nodig als u de SAML Responses wilt versleutelen.



## Het SSO ZIP-bestand maken

1. Markeer alle bestanden die bedoeld zijn om te worden gebruikt voor het SSO-configuratiebestand.

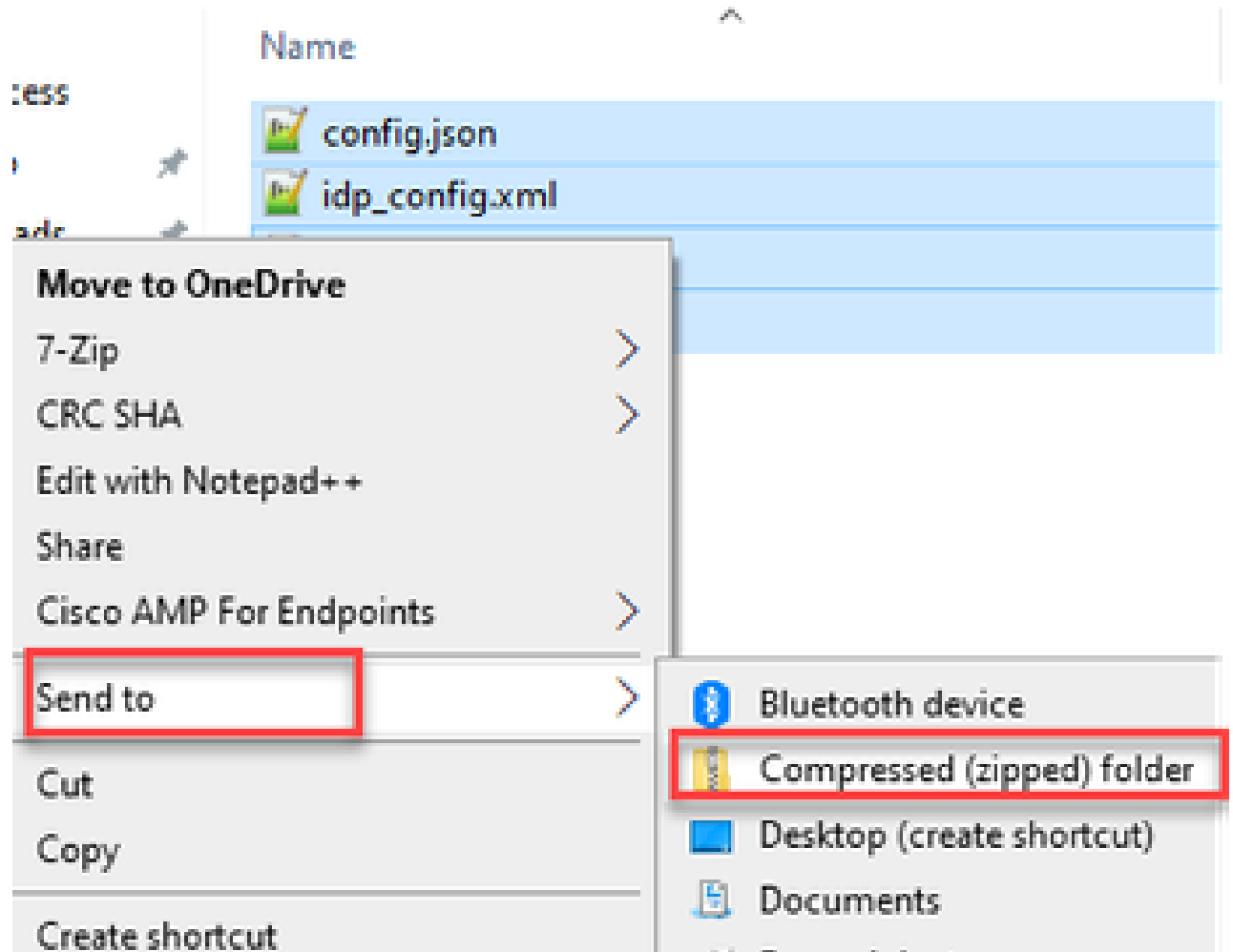




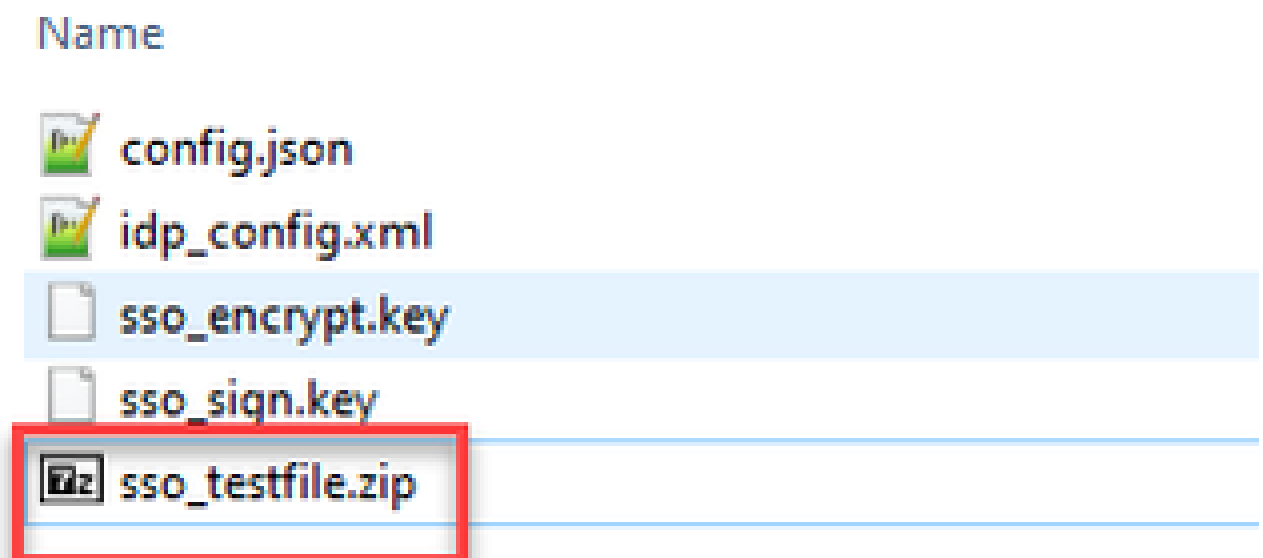
Waarschuwing: zip de map met de bestanden niet omdat dit ertoe leidt dat de DSB niet werkt.

---

2. Klik met de rechtermuisknop op de gemarkeerde bestanden en selecteer Verzenden naar > Gecomprimeerde map.



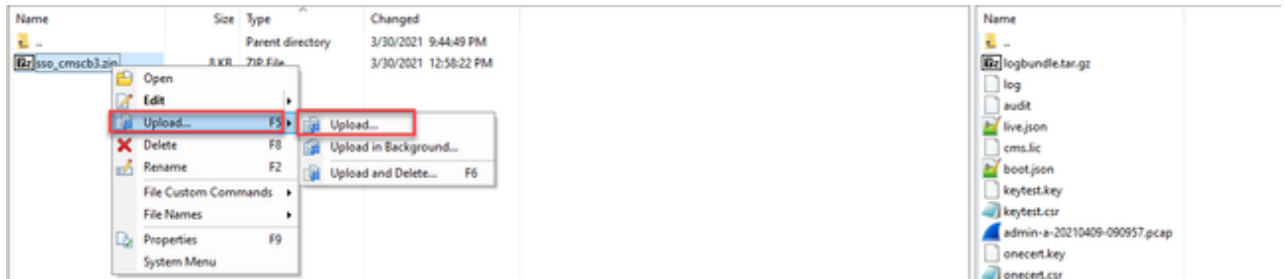
3. Nadat de bestanden zijn gezip, geeft u de gewenste naam door met het sso\_ prefix:



Upload de SSO Zip-bestand(en) naar Webbridge

Open een SFTP/SCP-client, in dit voorbeeld wordt WinSCP gebruikt en maak verbinding met de server die Webbridge3 host.

1. Navigeer in het linkerdeelvenster naar de locatie waar het ZIP-bestand zich bevindt en klik met de rechtermuisknop op Upload of sleep het bestand.



2. Wanneer het bestand volledig naar de Webbridge3-server is geüpload, opent u een SSH-sessie en voert u de opdracht webbridge3 opnieuw uit.

```
cmscb3> webbridge3 restart
SUCCESS: HTTPS Key and certificate pair match
SUCCESS: HTTPS full chain of certificates verifies correctly
SUCCESS: C2W Key and certificate pair match
SUCCESS: C2W full chain of certificates verifies correctly
SUCCESS: Webbridge3 enabled
cmscb3>
```

3. In de syslog geven deze berichten aan dat de SSO-functie is geslaagd:

```
client_backend: INFO : SamlManager : Attempting to configure SSO information from:sso_cmscb3.zip
client_backend: INFO : SamlManager : Successfully saved config.json to ./FWDo4e/config.json
client_backend: INFO : SamlManager : Successfully saved idp_config.xml to ./FWDo4e/idp_config.xml
client_backend: INFO : SamlManager : Validated signing idp credential: /CN=ADFS Signing - adfs.brhuff.com
client_backend: INFO : SamlManager : SAML SSO configured, entityId:http://adfs.brhuff.com/adfs/services/trust
```

## Gemeenschappelijke toegangkaart (CAC)

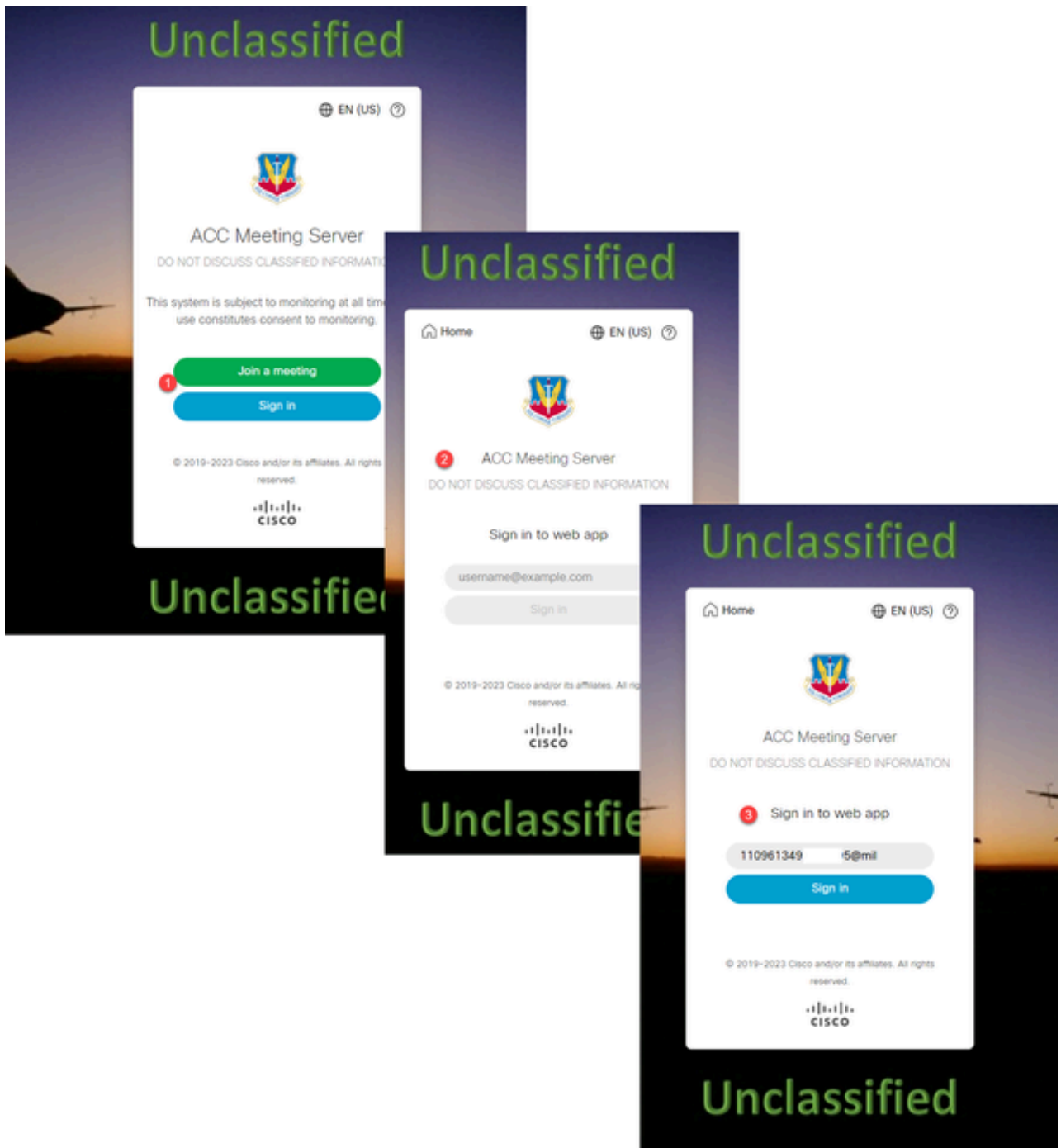
Een Common Access Card (CAC) is een slimme kaart die als standaard identificatie dient voor actieve militairen, civiele DoD-medewerkers en in aanmerking komend contractanten.

Hier is het gehele inlogproces voor gebruikers die CAC-kaarten gebruiken:

1. Zet PC aan en plak op de CAC-kaart
2. Log in (kies cert soms) en voer Pin in
3. Open browser
4. Navigeer naar de samengevoegde URL en zie de opties Samenvoegen bij een vergadering of Inloggen
5. Aanmelden: Voer de gebruikersnaam in die is ingesteld als jidMapping en de Active

Directory verwacht van een CAC-login

6. Hit sign in
7. ADFS-pagina wordt kort weergegeven en is automatisch ingevuld
8. Gebruiker wordt op dit punt aangemeld



Configureer `jidMapping` (dit is de gebruikers teken in naam) in `Ldapmapping` hetzelfde als wat ADFS gebruikt voor CAC-kaart. `$userPrincipalName$` bijvoorbeeld (hoofdlettergevoelig)

Stel ook dezelfde LDAP-eigenschap in voor de `authenticationMapping` om de eigenschap aan te passen die wordt gebruikt in de Claim-regel in ADFS.

Hier, de vorderingsregel toont het `$userPrincipalName$` terug naar CMS als UID zal verzenden.



150 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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

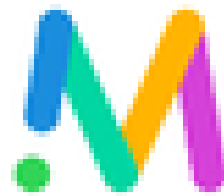
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-PrincipalName	uid
⊕		

## Inloggen via WebApp

Nu SSO is geconfigureerd, kunt u de server testen:

1. Navigeer naar Webbridge URL voor de Web App en selecteer de knop Aanmelden.



# Cisco Meeting Server

web app

Join meetings, anywhere, anytime

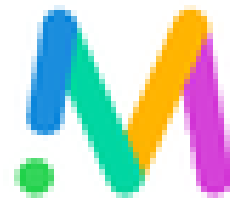
Join a meeting

Sign in

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



2. De gebruiker krijgt de optie om zijn of haar gebruikersnaam in te voeren (zie geen wachtwoordoptie op deze pagina).



# Cisco Meeting Server

web app

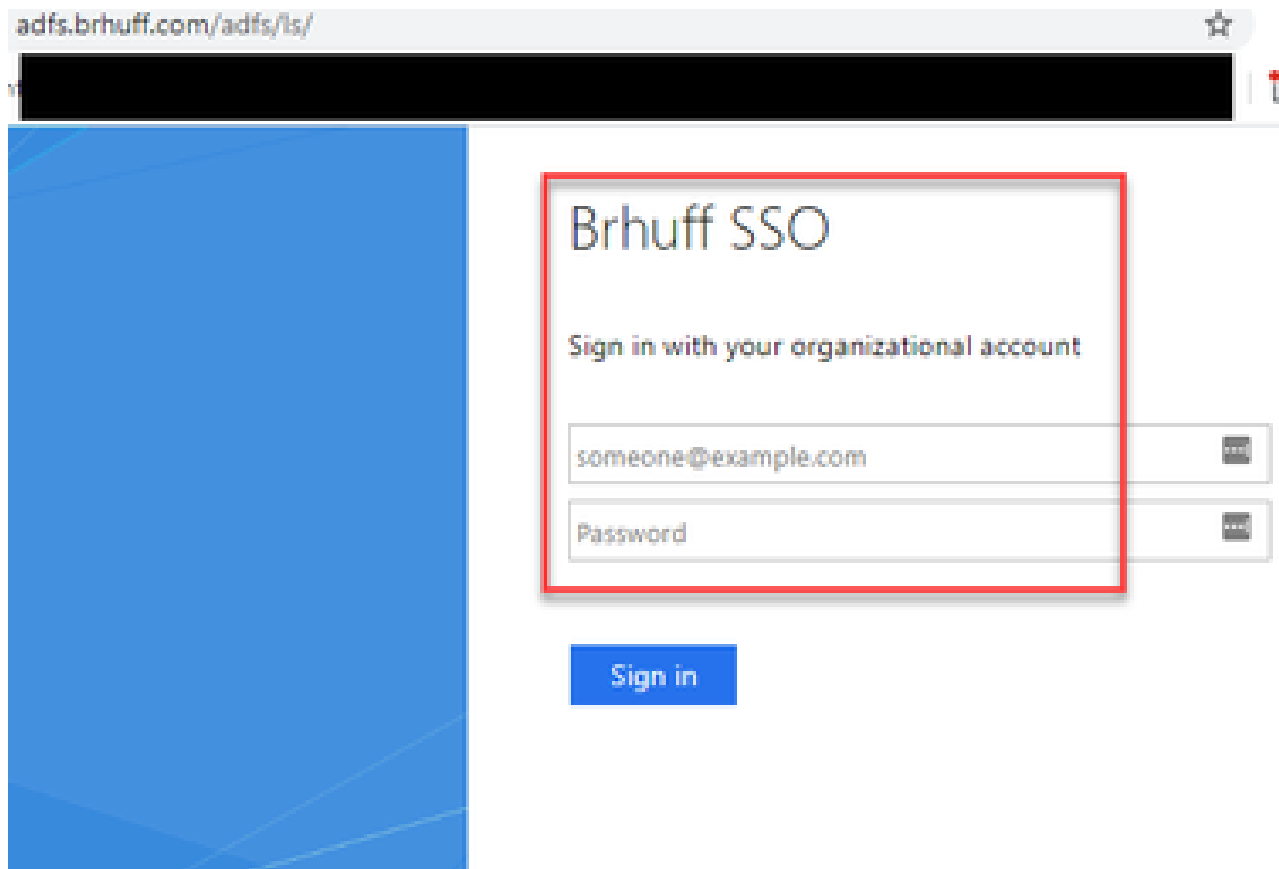
Sign in to web app

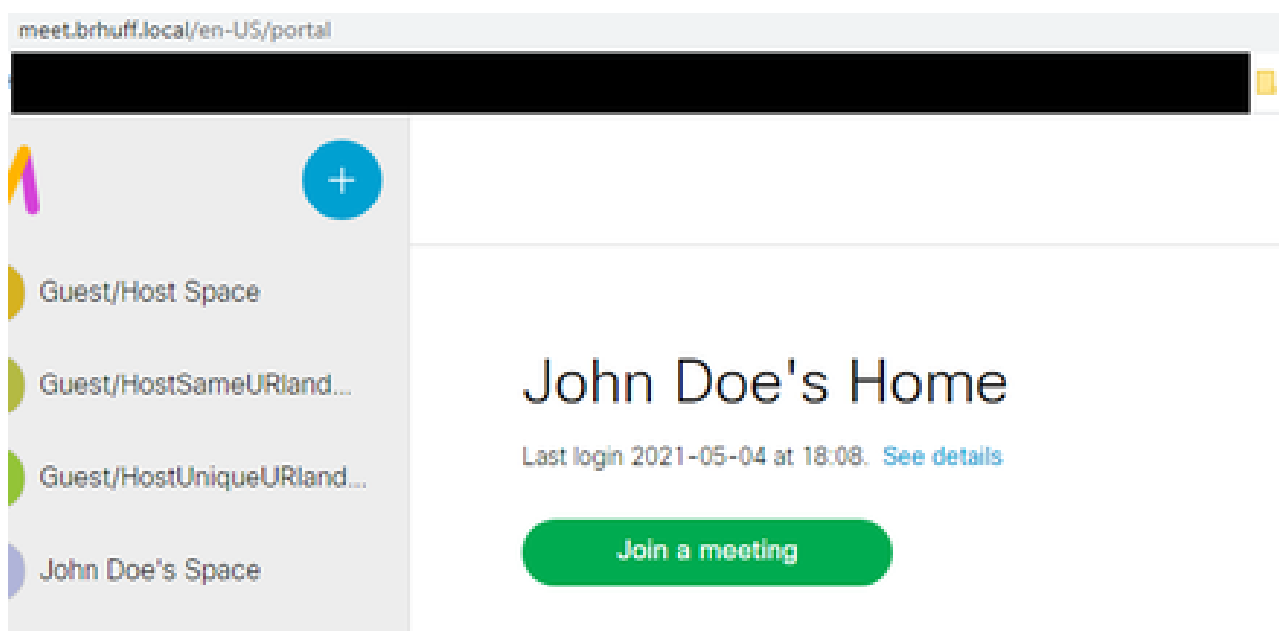
© 2020 Cisco and/or its affiliates. All rights reserved.



3. De gebruiker wordt vervolgens doorgestuurd naar de ADFS-pagina (na het invoeren van gebruikersdetails) waar de gebruiker zijn referenties moet invoeren om te verifiëren op IDp.



4. De gebruiker, na het invoeren en valideren van referenties met de IDP wordt met het token omgeleid naar de Web App startpagina:



# Probleemoplossing

## Basis probleemoplossing

Voor eenvoudige probleemoplossing bij een SSO-probleem:

1. Zorg ervoor dat de samengestelde metagegevens voor de Webbridge3 gebruikt om te importeren als een Relying Trust in IdP correct is geconfigureerd en de URL geconfigureerd overeenkomsten precies zoals het soServiceProviderAddress in config.json.
2. Zorg ervoor dat de metagegevens die door de IdP worden verstrekt en in het configuratiebestand van Webbridge3 worden gezipt, het laatste bestand van de IdP zijn, alsof er wijzigingen zijn in de serverhostnaam, de certificaten, enzovoort. Het moet opnieuw worden geëxporteerd en in het configuratiebestand worden gezipt.
3. Als u persoonlijke sleutels gebruikt voor het versleutelen van gegevens, zorg er dan voor dat de juiste sleutels deel uitmaken van het bestand sso\_XXXX.zip dat u naar webbridge hebt geüpload. Probeer indien mogelijk te testen zonder de optionele privésleutels om te zien of SSO werkt zonder deze versleutelde optie.
4. Zorg ervoor dat de config.json is geconfigureerd met de juiste gegevens voor SSO-domeinen, Webbridge3 URL EN verwachte authenticatie-mapping om aan te sluiten op de SAMLResponse.

Het zou ook ideaal zijn om het oplossen van problemen te proberen vanuit het logboekperspectief:

1. Bij het navigeren naar de Webbridge URL, plaats ?trace=true aan het eind van de URL om een uitgebreide logboekregistratie op het CMS-systeem mogelijk te maken. (bijvoorbeeld <https://join.example.com/en-US/home?trace=true>).
2. Voer de syslog follow op de Webbridge3-server uit om tijdens het testen live op te nemen of de test uit te voeren met de traceoptie toegevoegd aan de URL en de logbundle.tar.gz van de Webbridge3- en CMS Callbridge-servers te verzamelen. Als webbridge en callbridge op dezelfde server staan, is hiervoor slechts één logbundle.tar.gz-bestand vereist.

## Microsoft ADFS-foutcodes

Soms, is er een mislukking voor het proces SSO dat in een mislukking voor de configuratie IdP of zijn communicatie met IdP kan resulteren. Als het gebruiken van ADFS, zou het ideaal zijn om de volgende verbinding te herzien om de mislukking te bevestigen die worden gezien en saneringsactie te voeren:

## [Microsoft Status-codes](#)

Een voorbeeld hiervan:

```
client_backend: FOUT: SAMLManager: SAML-verificatieaanvraag _e135ca12-4b87-4443-abe1-30d396590d58 mislukt met reden: urn:oasis:namen:tc:SAML:2.0:status:Responder
```

Deze fout geeft aan dat volgens de vorige documentatie de fout is opgetreden door de IDp of ADFS en dus door de beheerder van de ADFS moet worden opgelost.

## Verwerving verificatie-ID mislukt

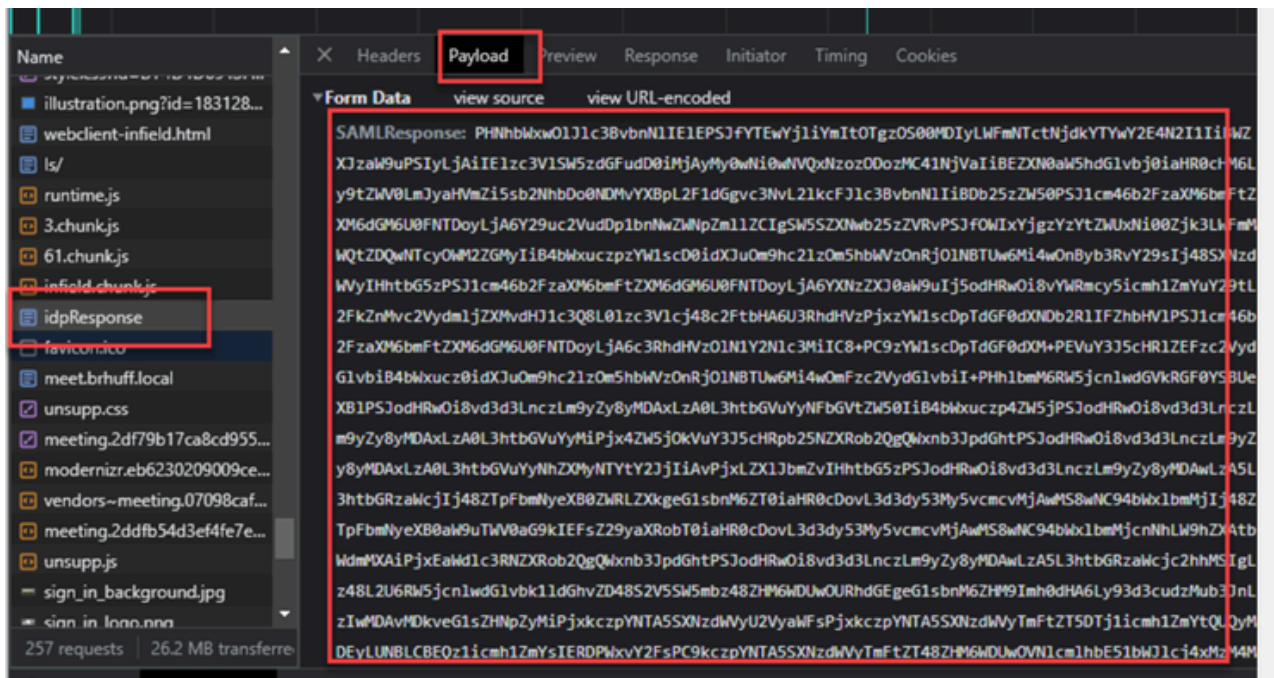
Er kunnen gevallen zijn waarin tijdens de uitwisseling van SAMLResponse terug van IDP, de Webbridge deze foutmelding in de logboeken kan weergeven met een fout in het inloggen via SSO:

```
client_backend: INFO: SamlManager: [57dff9e3-862e-4002-b4fa-683e4a6922c] Er is geen verificatie-ID verkregen
```

Wat dit betekent is dat bij het bekijken van de SAMLResponse gegevens die tijdens de authenticatieuitwisseling van de IdP zijn doorgegeven, de Webbridge3 geen geldig bijpassend attribuut in het antwoord heeft gevonden in vergelijking met zijn config.json voor de authenticatieveld.

Als de communicatie niet is versleuteld met het gebruik van de teken- en encryptie-privésleutels, kan de SAML Response via een webbrower worden geëxtraheerd uit de Developer Tools Network Logging en gedecodeerd met base64. Als de respons versleuteld is, kunt u de gedecrypteerde SAML-respons aanvragen bij de IDp-kant.

In de ontwikkelaargereedschappen netwerklogboekuitvoer, ook wel de HAR-gegevens genoemd, zoek naar idpResponse onder de naamkolom en selecteer payload om de SAML-respons te zien. Zoals eerder vermeld, kan dit worden gedecodeerd met behulp van base64-decoder.



Bij ontvangst van de SAMLResponse gegevens, controleer de sectie van <AttributeStatement> om de teruggezonden attributennamen te vinden en binnen deze sectie kunt u de claimtypen vinden die zijn geconfigureerd en verzonden vanuit de IDp. Voorbeeld:

```

<AttribuutStatement>
  <Attribute Name="<URL voor algemene naam">
  <AttributeValue>testuser1</AttributeValue>
  </Kenmerk>
  <Attribute Name="<URL voor NameID">
  <AttributeValue>testuser1</AttributeValue>
  </Kenmerk>
  <Attribute Name="uid">
  <AttributeValue>testuser1</AttributeValue>
  </Kenmerk>
</AttributeStatement>

```

Als u de vorige namen bekijkt, kunt u de <AttributeName>controleren onder de sectie Attribute Statement en elke waarde vergelijken met wat is ingesteld in de sectie AuthenticatielDmapping van de SSO config.json.

In het vorige voorbeeld kunt u zien dat de configuratie voor de authenticatielDMapping niet precies overeenkomt met wat er wordt doorgegeven en dus resulteert in het niet vinden van een overeenkomende authenticatielD:

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

Om deze kwestie op te lossen, zijn er twee mogelijke manieren om te proberen:

1. De IDp Uitgaande eisingsregel kan worden bijgewerkt om een passende eis te hebben die precies aansluit wat in authenticatielDMapping van config.json op Webbridge3 wordt



gevormd. (Claimregel toegevoegd op IDp voor <http://example.com/claims/NameID>)  
OF

2. Config.json kan worden bijgewerkt op de Webbridge3 om de 'authenticatielDMapping' exact te laten overeenkomen met wat is geconfigureerd als een van de uitgaande claimregels die op de IdP zijn geconfigureerd. (Dat is 'authenticatielDMapping' die moet worden bijgewerkt om een van de attributnamen te matchen, die "uid", "<URL>/NameID", of "<URL>/CommonName" zouden kunnen zijn. Zolang deze (exact) overeenkomt met de verwachte waarde die op CallBridge API is geconfigureerd wanneer deze wordt doorgegeven)

## Geen bewering doorgegeven/gematched in validatie

Soms, tijdens de uitwisseling van de SAMLResponse van IdP, geeft Webbridge deze fout weer die aangeeft dat er een fout is in het aanpassen van de bewering en slaat alle beweringen die niet overeenkomen met de serverconfiguratie over:

```
client_backend: FOUT: SamlManager: Geen beweringen geslaagd voor validatie  
client_backend: INFO: SamlManager: Skipping bewering zonder ons in het toegestane publiek
```

Wat deze fout aangeeft is dat bij het bekijken van de SAMLResponse van de IdP, de Webbridge geen overeenkomende beweringen kon vinden en dus niet-overeenkomende fouten oversloeg en uiteindelijk resulteerde in een mislukte SSO-aanmelding.

Om dit probleem te lokaliseren, is het ideaal om de SAMLResponse van de IDp te bekijken. Als de communicatie niet is versleuteld met het gebruik van de teken- en encryptie privésleutels, kan de SAML Response worden afgeleid uit de Developer Tools Network Logging via een webbrowser en gedecodeerd met base64. Als de respons versleuteld is, kunt u de gedecrypteerde SAML-respons aanvragen bij de IDp-kant.

Bij het bekijken van de SAMLResponse data, kijkend naar het <AudienceRestriction> gedeelte van de respons, kunt u alle doelgroepen vinden dat deze reactie beperkt is voor:

```
<Voorwaarden NotBefore=2021-03-30T19:35:37.071Z NietOpOfAfter=2021-03-30T19:36:37.071Z>  
<Beperking publiek>  
<Publiek>https://cisco.example.com</Publiek>  
</PubliekRestrictie>  
</Voorwaarden>
```

Met behulp van de waarde in de sectie <Publiek> (<https://cisco.example.com>) kunt u deze vergelijken met het ssoServiceProviderAddress in de configuratie config.json van Webbridge en controleren of deze exact overeenkomt. Bij dit voorbeeld, kunt u zien dat de reden voor de mislukking het Publiek niet het adres van de Dienstverlener in de configuratie aanpast, omdat het het volgende heeft toegevoegd :443:

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

Dit vereist een exacte overeenkomst tussen deze om niet te resulteren in een mislukking als deze. Dit voorbeeld. de oplossing zou aan een van deze twee methoden zijn:

1. De :443 kan worden verwijderd van het adres in het gedeelte SsoServiceProviderAddress van config.json, zodat het overeenkomt met het veld Publiek dat in de SAMLResponse van de IdP wordt verstrekt.

OF

2. De metagegevens OF vertrouwenspartij voor Webbridge3 in de IDp kan worden bijgewerkt om het :443 aan de URL toe te voegen. (Als de metagegevens worden bijgewerkt, moet het opnieuw als Relying Trust Party op ADFS worden ingevoerd. Als u de Relying Trust Party echter rechtstreeks vanuit de IDP-wizard wijzigt, hoeft deze niet opnieuw te worden geïmporteerd.)

Aanmelden mislukt in webapp:



# Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

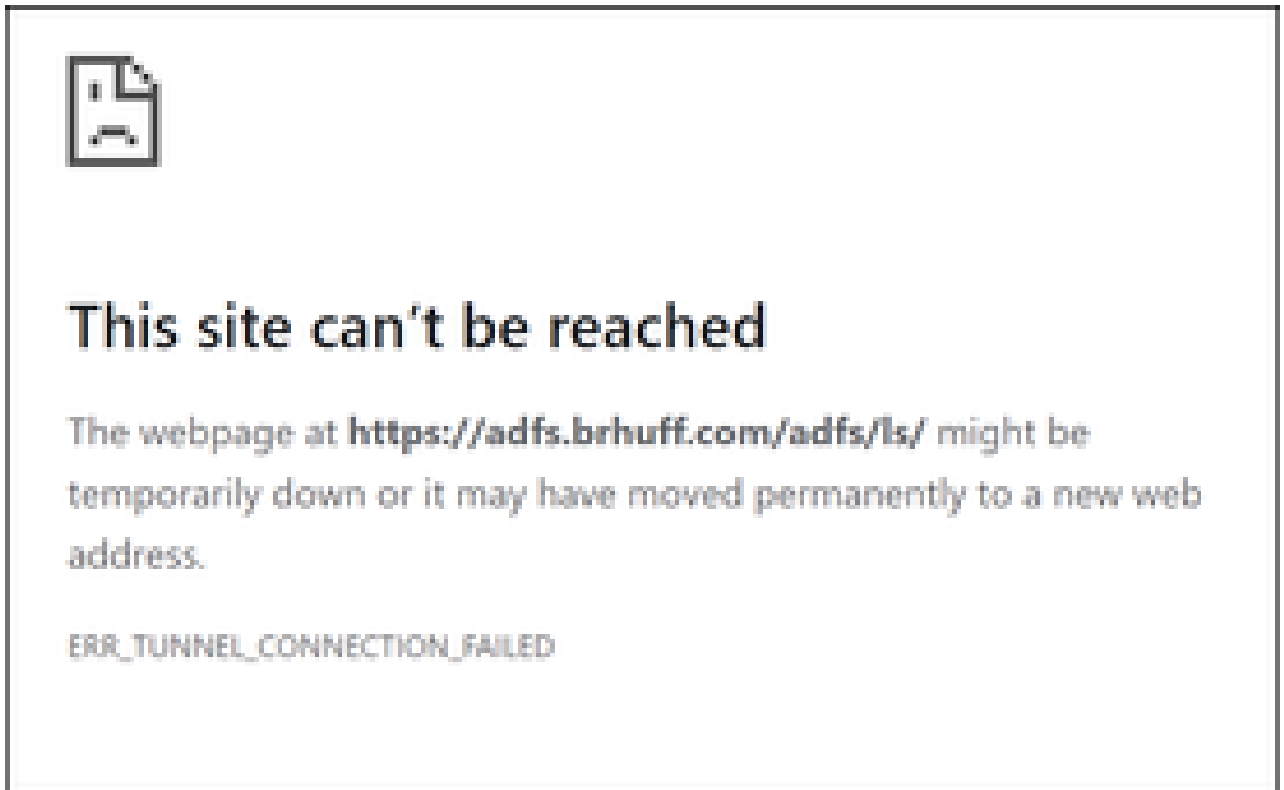
Sign in

 Sign in failed

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



), controleert webbridge of het gebruikte domein overeenkomt met een van de domeinnamen in het configuratie.json-bestand. Vervolgens wordt de SAML-informatie naar de client verzonden en wordt de client verteld waar de verbinding moet worden gemaakt voor verificatie. De client zal proberen verbinding te maken met de IDp in het SAML-token. In het onderstaande voorbeeld toont de browser deze pagina, omdat deze niet op de ADFS-server kan komen.



Fout in clientbrowser

CMS Webbridge overtrekken (terwijl ?trace=true wordt gebruikt)

Mar 19 10:47:07.927 user.info cmscb3-1 client\_backend: INFO: SamIManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Overeenkomende SSO\_2024.zip in SAML Token Verzoek

Mar 19 10:47:07.927 user.info cmscb3-1 client\_backend: INFO: SamIManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Pogingen om SSO te vinden in SAML Token Verzoek

Mar 19 10:47:07.930 user.info cmscb3-1 client\_backend: INFO: SamIManager: [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAML Token met succes gegenereerd

Scenario 2:

Gebruiker heeft geprobeerd in te loggen met behulp van een domein dat niet in het zip-bestand SSO staat op de webpagina. De client stuurt een tokenAanvraag met een payload van de gebruikersnaam die de gebruiker heeft ingevoerd. Webbridge stopt de inlogpoging onmiddellijk.

CMS Webbridge overtrekken (terwijl ?trace=true wordt gebruikt)

Mar 18 14:54:52.698 user.err cmscb3-1 client\_backend: FOUT: SamIManager: Ongeldige SSO login poging

Mar 18 14:54:52.698 user.info cmscb3-1 client\_backend: INFO: SamIManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Er is geen SSO gevonden in SAML Token Verzoek

Mar 18 14:54:52.698 user.info cmscb3-1 client\_backend: INFO: SamIManager: [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Poging tot het vinden van SSO in SAML Token Verzoek

### Scenario 3:

De gebruiker heeft de juiste gebruikersnaam ingevoerd en krijgt het SSO-teken in pagina te zien. De gebruiker voert hier ook de juiste gebruikersnaam en wachtwoord in, maar krijgt nog steeds Inloggen mislukt

CMS Webbridge overtrekken (terwijl ?trace=true wordt gebruikt)

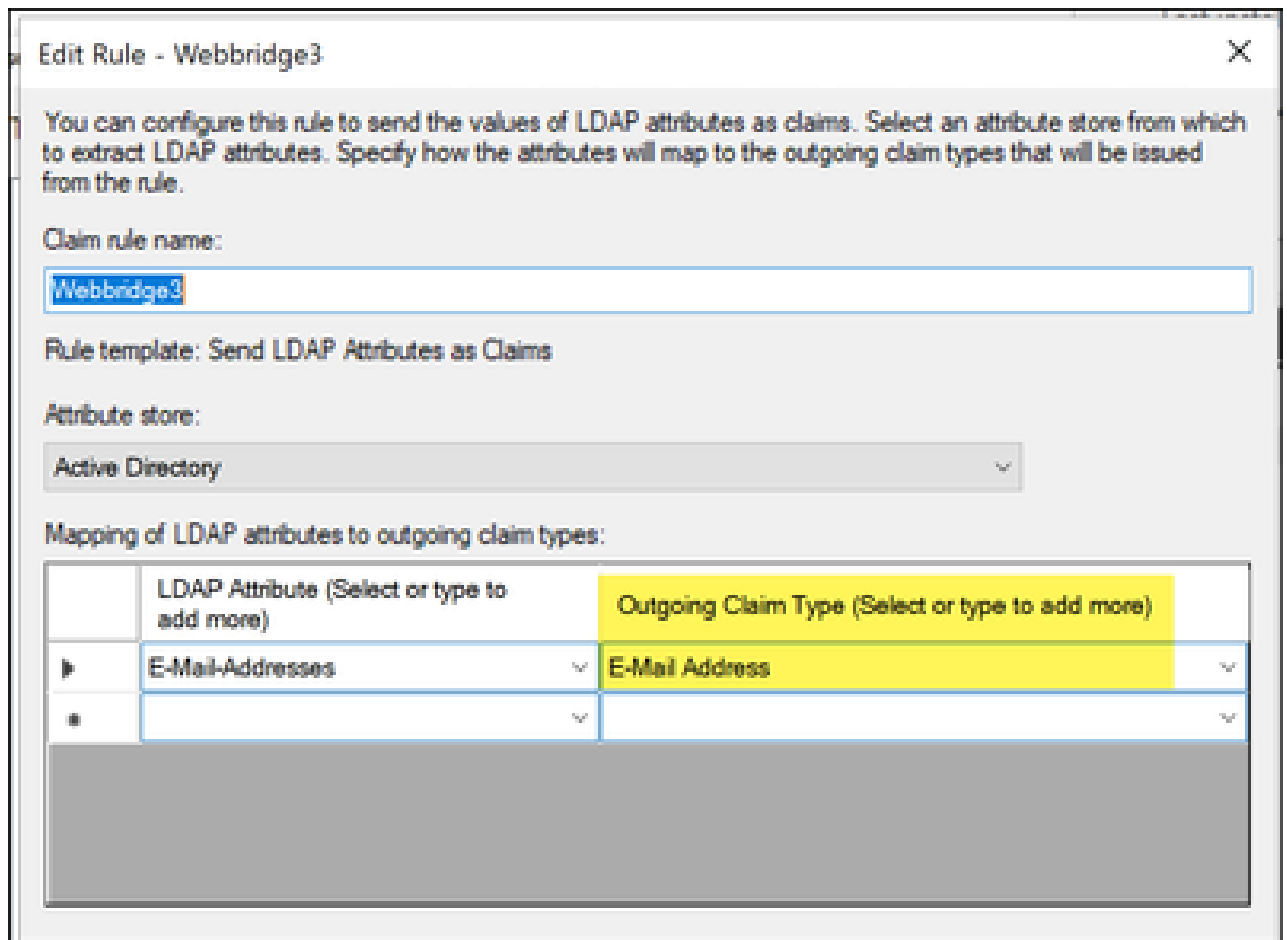
Mar 19 16:39:17.714 user.info cmscb3-1 client\_backend: INFO: SamIManager: [ef8fe67f-685c-4a81-9240-f76239379806] Gekoppeld SSO\_2024.zip in SAML Token Verzoek

Mar 19 16:39:17.714 user.info cmscb3-1 client\_backend: INFO: SamIManager: [ef8fe67f-685c-4a81-9240-f76239379806] Poging om SSO te vinden in SAML IDP Response

Mar 19 16:39:17.720 user.err cmscb3-1 client\_backend: FOUT: SamIManager: Geen authenticatielD in kaart gebracht element gevonden in ondertekende SAML Assertions

Mar 19 16:39:17.720 user.info cmscb3-1 client\_backend: INFO: SamIManager: [ef8fe67f-685c-4a81-9240-f76239379806] Kan geen verificatie-ID verkrijgen

De oorzaak voor scenario 3 was de claimregel in de IdP met behulp van een claimtype dat niet overeenkwam met de authenticatielDMapping in het config.json bestand gebruikt in het SSO zip bestand dat was geüpload naar webbridge. Webbridge kijkt naar de SAML-respons en verwacht dat de attributennaam overeenkomt met wat is geconfigureerd in config.json.



Claimregel in ADFS

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

config.json voorbeeld

## Gebruikersnaam wordt niet herkend

Scenario 1:

Gebruiker ingelogd met verkeerde gebruikersnaam (Domein komt overeen met wat in het zip-bestand SSO staat dat naar webbridge3 is geüpload, maar gebruiker bestaat niet)



## 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.



in CMS ldapmapping komt niet overeen met het gevormde LDAP attribuut dat voor de claimregel in ADFS wordt gebruikt. De regel hieronder die "met succes verkregen authenticatieID:darmckin@brhuff.com" zegt dat ADFS claimregel is geconfigureerd met attribuut dat darmckin@brhuff.com krijgt uit actieve directory, maar de AuthenticatieID in CMS API > Gebruikers laat zien dat het darmckin verwacht. In de CMS lapMappings, wordt de AuthenticatieID geconfigureerd als \$sAMAaccountName\$, maar de claimregel in ADFS is ingesteld om de e-mail-adressen te verzenden, dus dit komt niet overeen.

Hoe dit op te lossen:

Voer een van de volgende handelingen uit:

1. Wijzig de verificatie-ID in de CMS ldapmapping zodat deze overeenkomt met wat in de claimregel op ADFS wordt gebruikt en voer een nieuwe sync uit
2. Wijzig het LDAP-kenmerk dat in de ADFS-claimregel wordt gebruikt, zodat het overeenkomt met wat in CMS ldapmapping is geconfigureerd

Related objects: </api/v1/ldapMappings>

Table view XML view

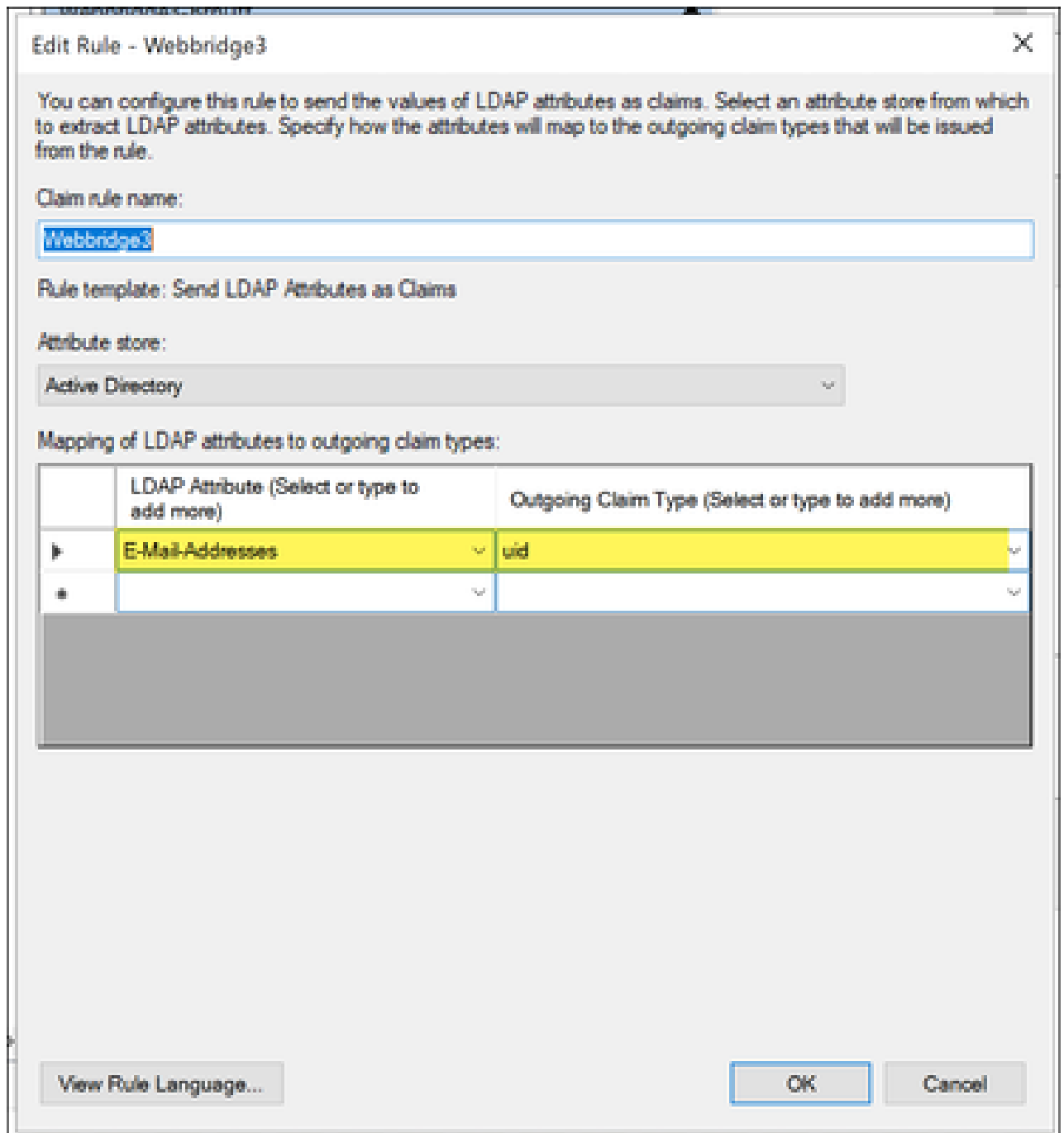
Object configuration	
jidMapping	\$sAMAaccountName\$@brhuff.com
nameMapping	\$cn\$
cdrTagMapping	
coSpaceNameMapping	\$cn\$'s Space
coSpaceUriMapping	\$sAMAaccountName\$.space
coSpaceSecondaryUriMapping	\$extensionAttribute12\$
coSpaceCallIdMapping	
authenticationIdMapping	\$sAMAaccountName\$

API-LDAPM-toepassing

Object configuration	
userId	darmckin@brhuff.com
name	Darren McKinnon
email	darmckin@brhuff.com
authenticationId	darmckin
userProfile	<a href="#">d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3</a>

API-gebruikersvoorbeeld





Claimregel van ADFS

Webbridge log toont werklog in voorbeeld. Geproduceerd voorbeeld met ?trace=true in de samengevoegde URL:

Mar 18 14:24:01.096 user.info cmscb3-1 client\_backend: INFO: SamIManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Gekoppelde SSO\_2024.zip in SAML Token Verzoek

Mar 18 14:24:01.096 user.info cmscb3-1 client\_backend: INFO: SamIManager: [7979f13c-d490-4f8b-899c-0c82853369ba] Poging om SSO te vinden in SAML IDP Response

Mar 18 14:24:01.101 user.info cmscb3-1 client\_backend: INFO: SamIManager: [7979f13c-d490-4f8b-899c-0c82853369ba] Met succes verkregen

authenticatieID:darmckin@brhuff.com

Mar 18 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-0272-4a5 B125-136fdf5612a5 (user=darmckin@brhuff.com)

Mar 18 14:24:01.130 user.info cmscb3-1 host:server: INFO: succesvol inlogverzoek van darmckin@brhuff.com

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

18 mrt 14:24:01.132 user.info cmscb3-1 host:server: INFO: WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] verzenden van auditieve reactie (jwt length=1064, connection=64004556-faea-479f-aabe-691e17783aa5)

18 mrt. 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] status 20 "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, zoals Gecko) Chrome/122.0.0.0 Safari/537.36" naar upstream 192.0.2.900 tijd: upstream\_response 0,038 request\_time 0,039 msec 1710786241.133 upstream\_response\_length 24 200

## Gerelateerde informatie

- [Cisco Technical Support en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.