

WebApp SSO auf CMS konfigurieren und Fehlerbehebung durchführen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ADFS-Installation und Ersteinrichtung](#)

[Zuordnen von CMS-Benutzern zum Identitätsanbieter \(IdP\)](#)

[Webbridge-Metadaten-XML für IdP erstellen](#)

[Metadaten für Webbridge in Identitätsanbieter \(IdP\) importieren](#)

[Erstellen von Anspruchsregeln für den Webbridge-Dienst auf dem IdP](#)

[SSO-Archiv-ZIP-Datei für Webbridge erstellen:](#)

[Rufen Sie die Datei idp_config.xml ab, und konfigurieren Sie sie.](#)

[Erstellen der config.json-Datei mit Inhalt](#)

[Legen Sie den Schlüssel sso_sign.key fest \(OPTIONAL\).](#)

[Legen Sie den Schlüssel sso_encrypt.key fest \(OPTIONAL\).](#)

[Erstellen der SSO-ZIP-Datei](#)

[SSO-Zip-Datei\(en\) auf Webbridge hochladen](#)

[Common Access Card \(CAC\)](#)

[Testen von SSO Anmeldung über WebApp](#)

[Fehlerbehebung](#)

[Grundlegende Fehlerbehebung](#)

[Microsoft ADFS-Fehlercodes](#)

[Fehler beim Abrufen der Authentifizierungs-ID.](#)

[Keine Assertion in Validierung übergeben/abgeglichen](#)

[Anmeldung fehlgeschlagen auf Web-App:](#)

[Szenario 1:](#)

[Szenario 2:](#)

[Szenario 3:](#)

[Benutzername wird nicht erkannt](#)

[Szenario 1:](#)

[Szenario 2:](#)

[Webbridge-Protokoll mit Arbeitsprotokoll als Beispiel. Beispiel generiert mit ?trace=true in der Join-URL:](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration und Fehlerbehebung der Cisco Meeting Server (CMS) Web App-Implementierung von Single Sign On (SSO) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- CMS Callbridge Version 3.1 oder höher
- CMS Webbridge Version 3.1 oder höher
- Active Directory-Server
- Identifizierungsanbieter (IdP)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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


Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

In CMS 3.1 und höher wurde die Möglichkeit eingeführt, dass sich Benutzer über eine SSO-Funktion anmelden können, ohne jedes Mal ihr Kennwort eingeben zu müssen, wenn sich der Benutzer anmeldet, da eine einzelne Sitzung mit dem Identifizierungsanbieter erstellt wird. Diese Funktion verwendet die Security Assertion Markup Language (SAML) Version 2.0 als SSO-Mechanismus.

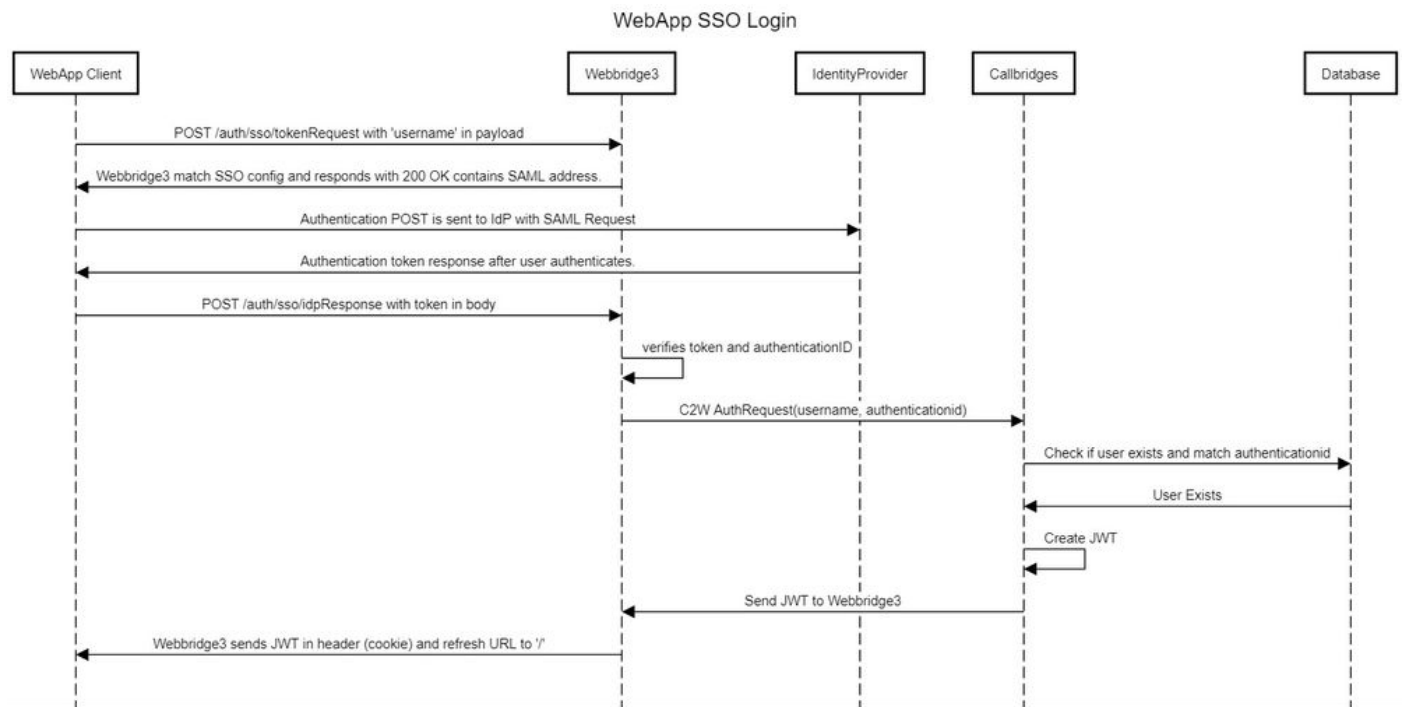
 Hinweis: CMS unterstützt nur HTTP-POST-Bindungen in SAML 2.0 und lehnt jeden Identify-

 Provider ab, für den keine HTTP-POST-Bindungen verfügbar sind.

 Hinweis: Wenn SSO aktiviert ist, ist die grundlegende LDAP-Authentifizierung nicht mehr möglich.

Konfigurieren

Netzwerkdiagramm



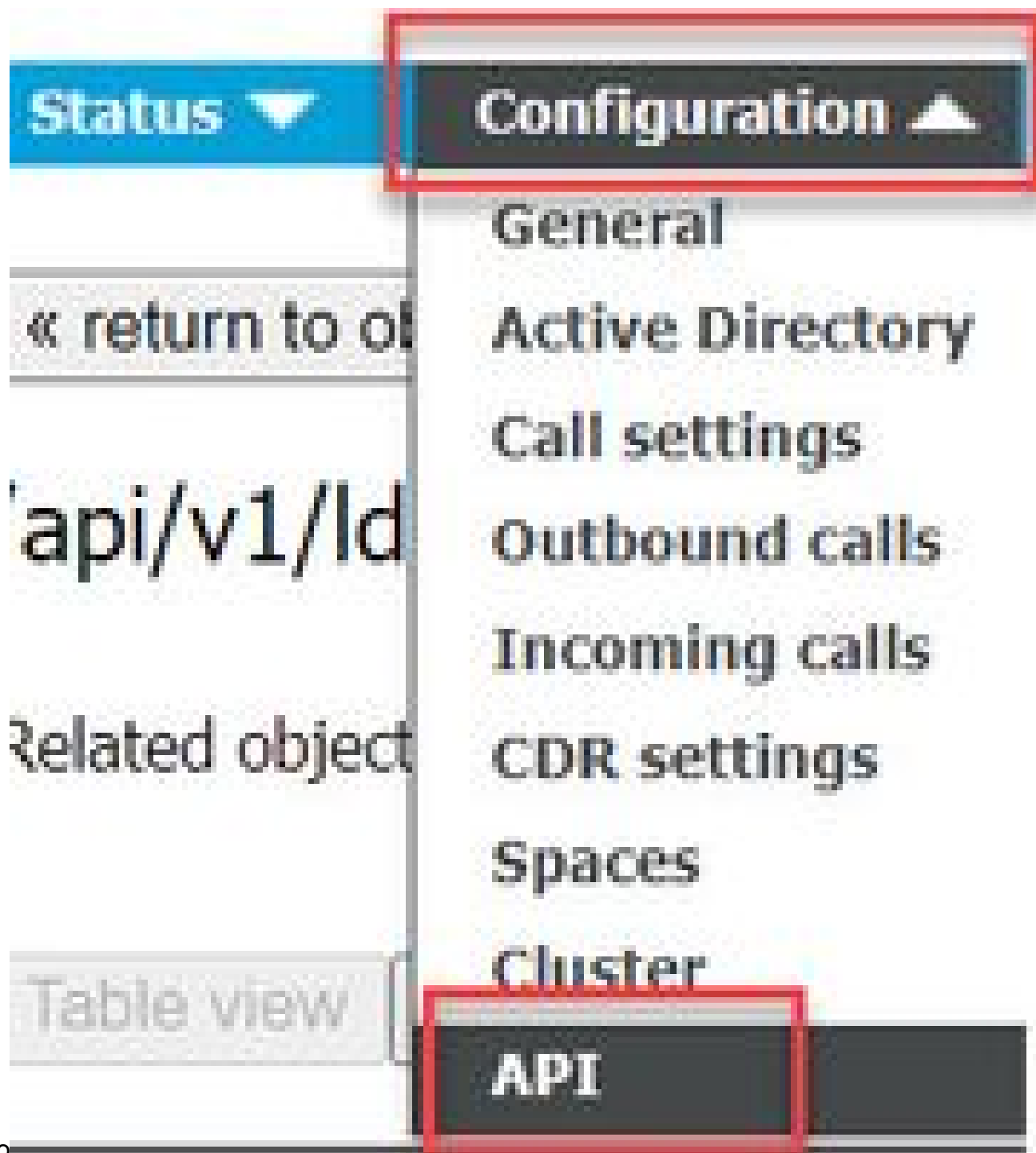
ADFS-Installation und Ersteinrichtung

In diesem Bereitstellungsszenario werden Microsoft Active Directory Federation Services (ADFS) als Identitätsanbieter (IdP) verwendet. Daher wird empfohlen, vor dieser Konfiguration ein ADFS (oder beabsichtigtes IdP) zu installieren und auszuführen.

Zuordnen von CMS-Benutzern zum Identitätsanbieter (IdP)

Damit Benutzer eine gültige Authentifizierung erhalten, müssen sie in der API (Application Programming Interface) für ein von IdP bereitgestelltes korrelierendes Feld zugeordnet werden. Die dafür verwendete Option ist `authenticationIdMapping` im `IdpMapping` der API.

1. Navigieren Sie in der CMS-Webadministrator-GUI zu Configuration > API.



2. Suchen Sie unter `api/v1/ldapMappings/<GUID-of-Ldap-Mapping>` nach einer vorhandenen LDAP-Zuordnung (oder erstellen Sie eine neue LDAP-Zuordnung).

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. Aktualisieren Sie im ausgewählten ldapMapping-Objekt das authenticationIdMapping auf das LDAP-Attribut, das von der IdP übergeben wird. Im Beispiel wird die Option \$sAMAccountName als LDAP-Attribut für die Zuordnung verwendet.

/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
cdtTagMapping	<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

 Hinweis: Das authenticationIdMapping wird von der Callbridge/Datenbank verwendet, um den Anspruch zu validieren, der von der IdP in der SAMLResponse gesendet wurde, und um dem Benutzer ein JSON Web Token (JWT) bereitzustellen.

4. Führen Sie eine LDAP-Synchronisierung für die ldapSource aus, die mit der kürzlich geänderten ldapMapping verknüpft ist:

Beispiele:

/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. Navigieren Sie nach Abschluss der LDAP-Synchronisierung in der CMS-API unter Konfiguration > api/v1/users, wählen Sie einen importierten Benutzer aus, und vergewissern Sie sich, dass die authenticationId korrekt ausgefüllt ist.

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

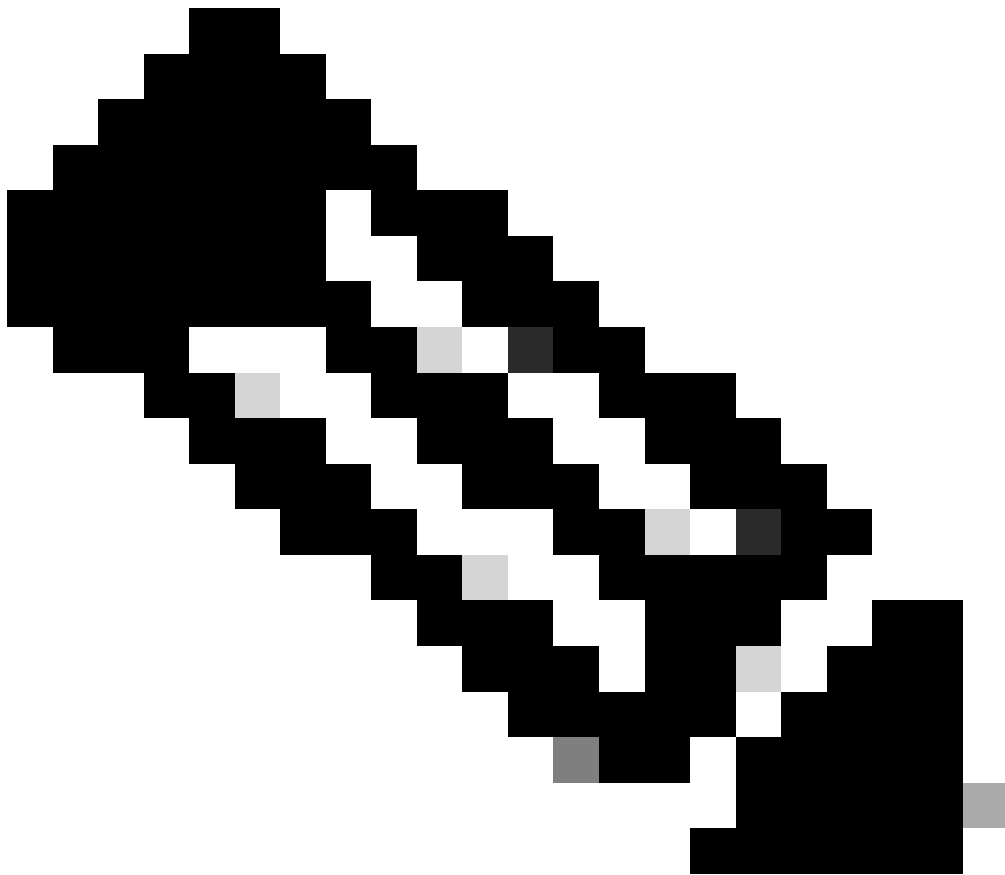
Webbridge-Metadaten-XML für IdP erstellen

Mit Microsoft ADFS kann eine XML-Metadaten-Datei als vertrauende Partei importiert werden, um den verwendeten Dienstanbieter zu identifizieren. Es gibt einige Möglichkeiten, die Metadaten-XML-Datei zu diesem Zweck zu erstellen. Es gibt jedoch einige Attribute, die in der Datei vorhanden sein müssen:

Beispiel für Webbridge-Metadaten mit erforderlichen Werten:

```
<?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 - Dies ist die Webbridge3-Serveradresse (FQDN/Hostname) und der zugehörige Port, die von Browsern für Benutzer erreichbar ist.



Hinweis: Wenn mehrere Webbridges mit einer URL vorhanden sind, muss es sich um eine Load Balancing-Adresse handeln.

2. Speicherort - Dies ist der Speicherort, an dem der HTTP-POST AssertionConsumerService für die Webbridge-Adresse ausgeführt wird. Dies teilt der IdP mit, wohin ein authentifizierter Benutzer nach der Anmeldung umgeleitet werden soll. Dies muss auf die idpResponse-URL festgelegt werden: <https://<WebBridgeFQDN>:<port>/api/auth/sso/idpResponse>. Beispiel: <https://join.example.com:443/api/auth/sso/idpResponse>.
3. OPTIONAL - Öffentlicher Schlüssel für Signierung - Dies ist der öffentliche Schlüssel (Zertifikat) für die Signierung, der von IdP verwendet wird, um AuthRequest von Webbridge zu verifizieren. Dies MUSS mit dem privaten Schlüssel "sso_sign.key" auf dem SSO-Paket übereinstimmen, das auf Webbridge hochgeladen wurde, damit die IdP die Signatur mithilfe des öffentlichen Schlüssels (Zertifikats) überprüfen kann. Sie können ein vorhandenes Zertifikat aus der Bereitstellung verwenden. Öffnen Sie das Zertifikat in einer Textdatei, und kopieren Sie den Inhalt in die Webbridge-Metadatendatei. Verwenden Sie den passenden Schlüssel für das in der Datei sso_xxxx.zip verwendete Zertifikat als Datei sso_sign.key.

4. OPTIONAL - Öffentlicher Schlüssel für die Verschlüsselung - Dies ist der öffentliche Schlüssel (Zertifikat), mit dem die IdP die an Webbridge zurückgesendeten SAML-Informationen verschlüsselt. Dies MUSS mit dem privaten Schlüssel 'sso_encrypt.key' auf dem SSO-Paket übereinstimmen, das auf Webbridge hochgeladen wurde, damit Webbridge entschlüsseln kann, was von IdP zurückgesendet wird. Sie können ein vorhandenes Zertifikat aus der Bereitstellung verwenden. Öffnen Sie das Zertifikat in einer Textdatei, und kopieren Sie den Inhalt in die Webbridge-Metadatendatei. Verwenden Sie den passenden Schlüssel für das in der Datei sso_xxxx.zip verwendete Zertifikat als Datei sso_encrypt.key.

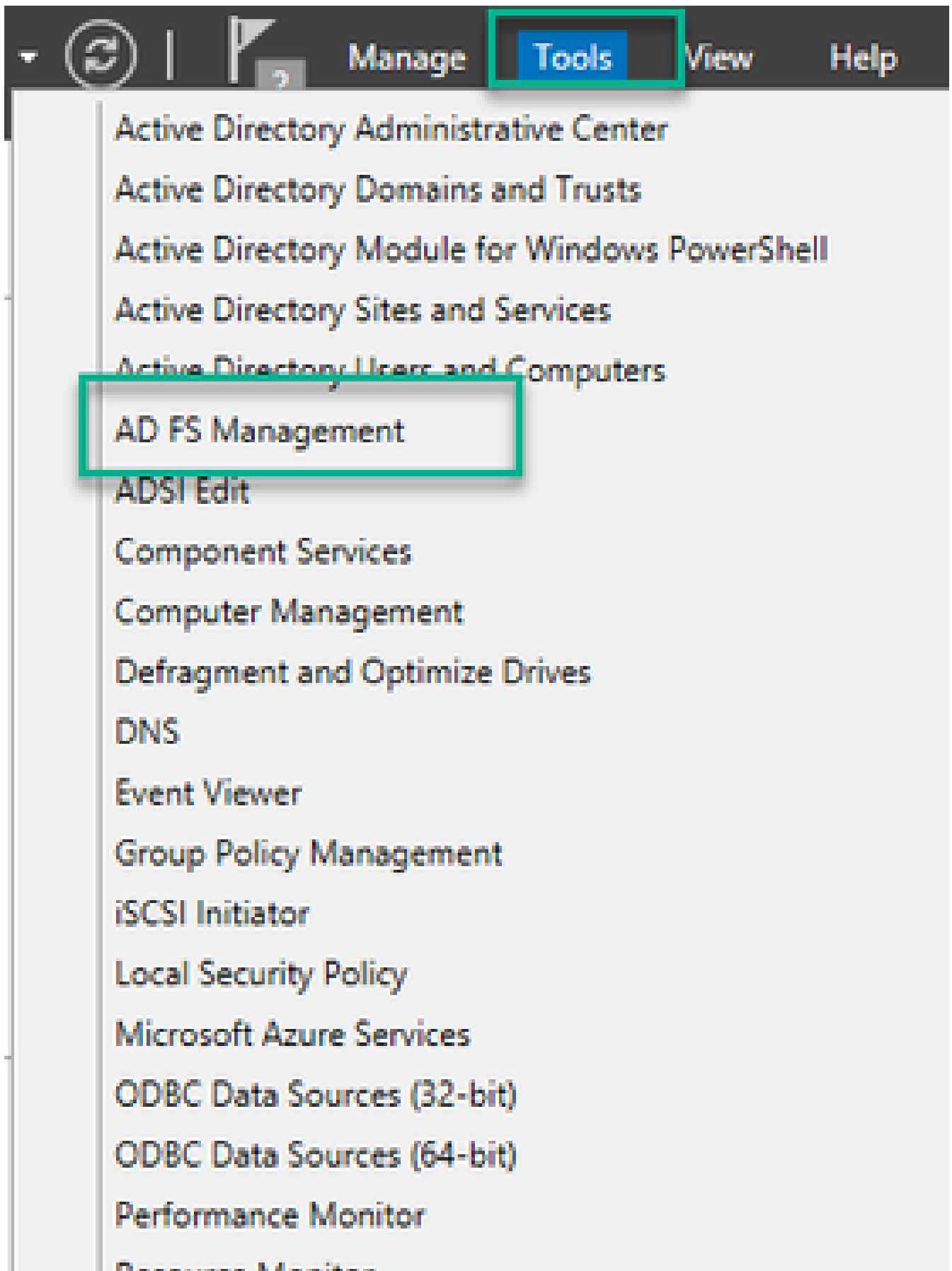
Beispiel für in IdP zu importierende Webbridge-Metadaten mit optionalen öffentlichen Schlüsseldaten (Zertifikatdaten):

```
<?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: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>
```

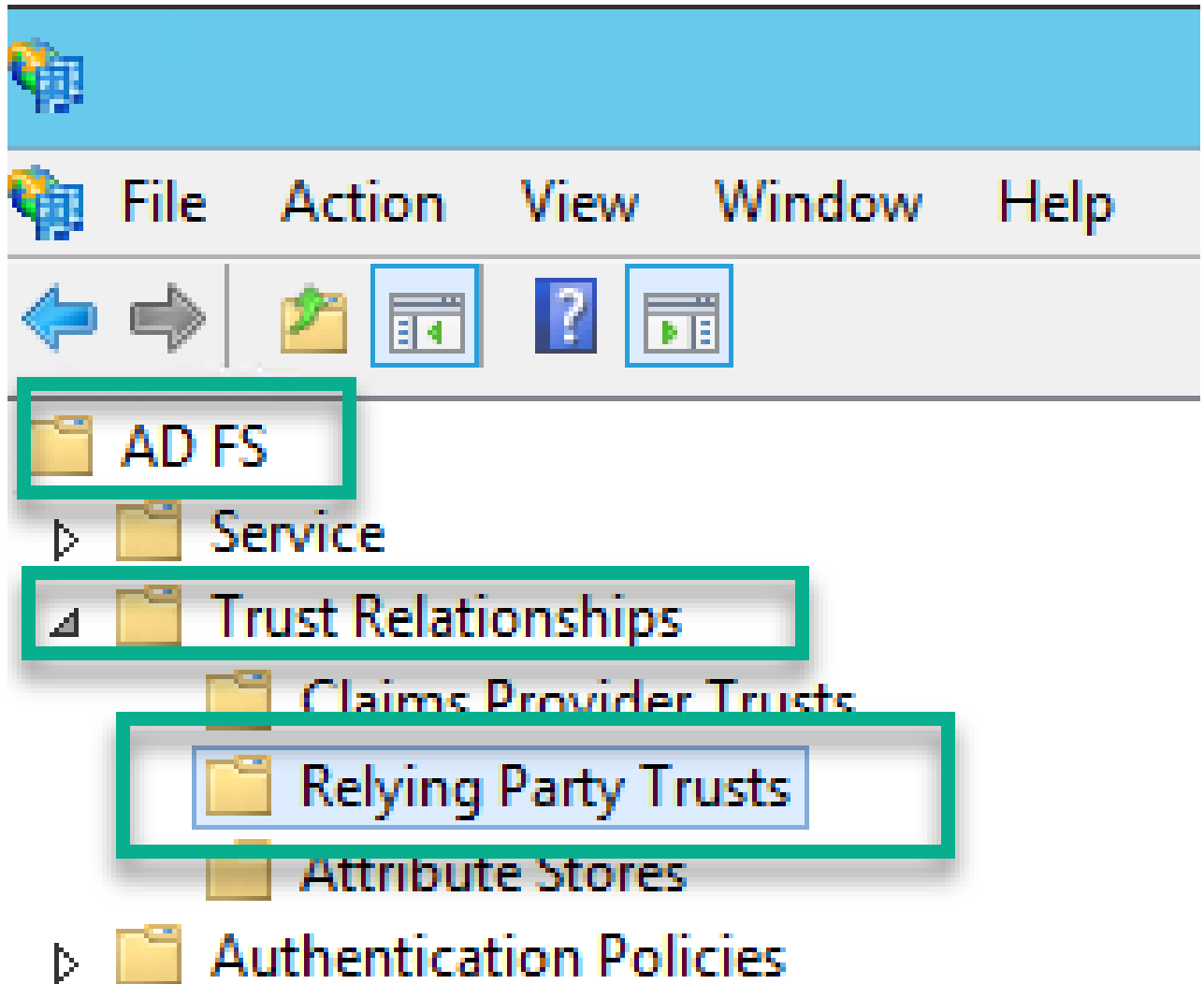
Metadaten für Webbridge in Identitätsanbieter (IdP) importieren

Nachdem die Metadaten-XML mit den richtigen Attributen erstellt wurde, kann die Datei in den Microsoft ADFS-Server importiert werden, um eine vertrauensvolle Partei zu erstellen.

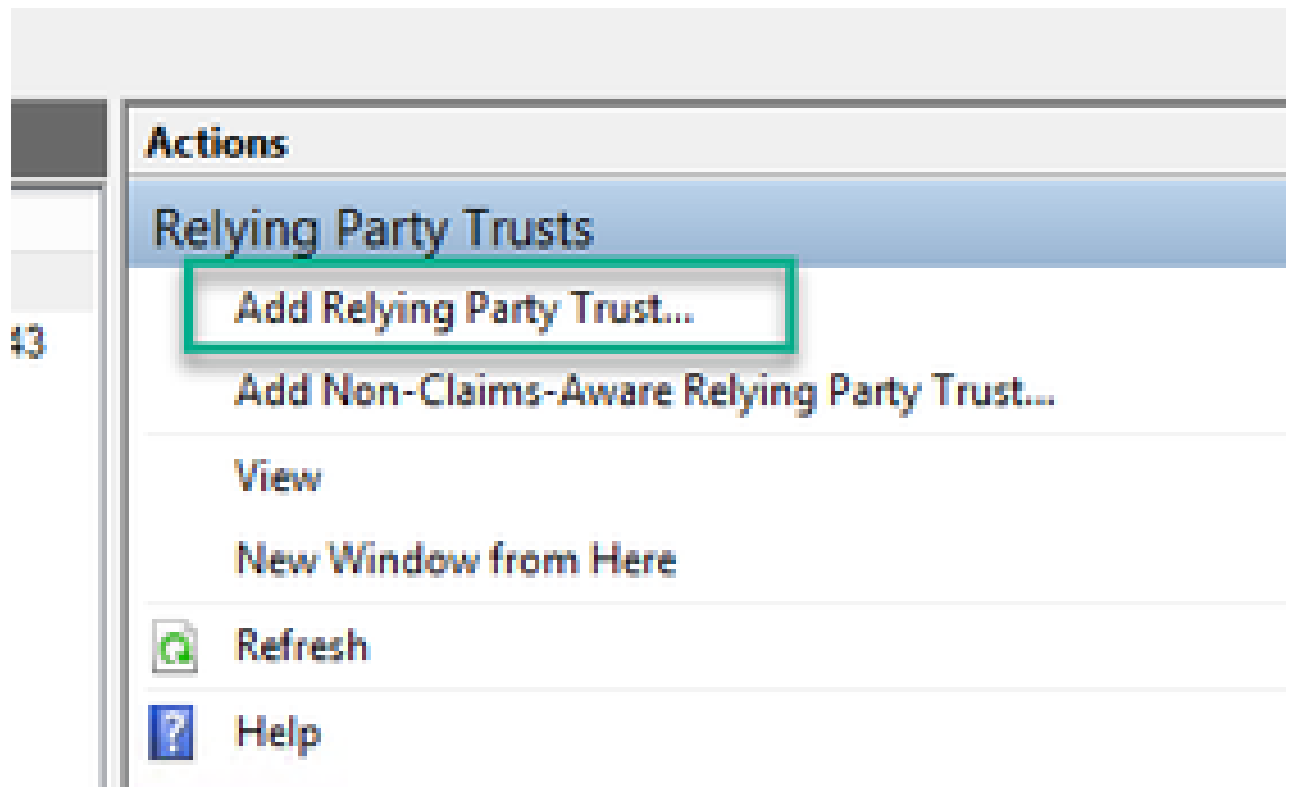
1. Remotedesktop in Windows Server, der die ADFS-Dienste hostet
2. Öffnen Sie die AD FS-Verwaltungskonsole, auf die normalerweise über den Server Manager zugegriffen werden kann.



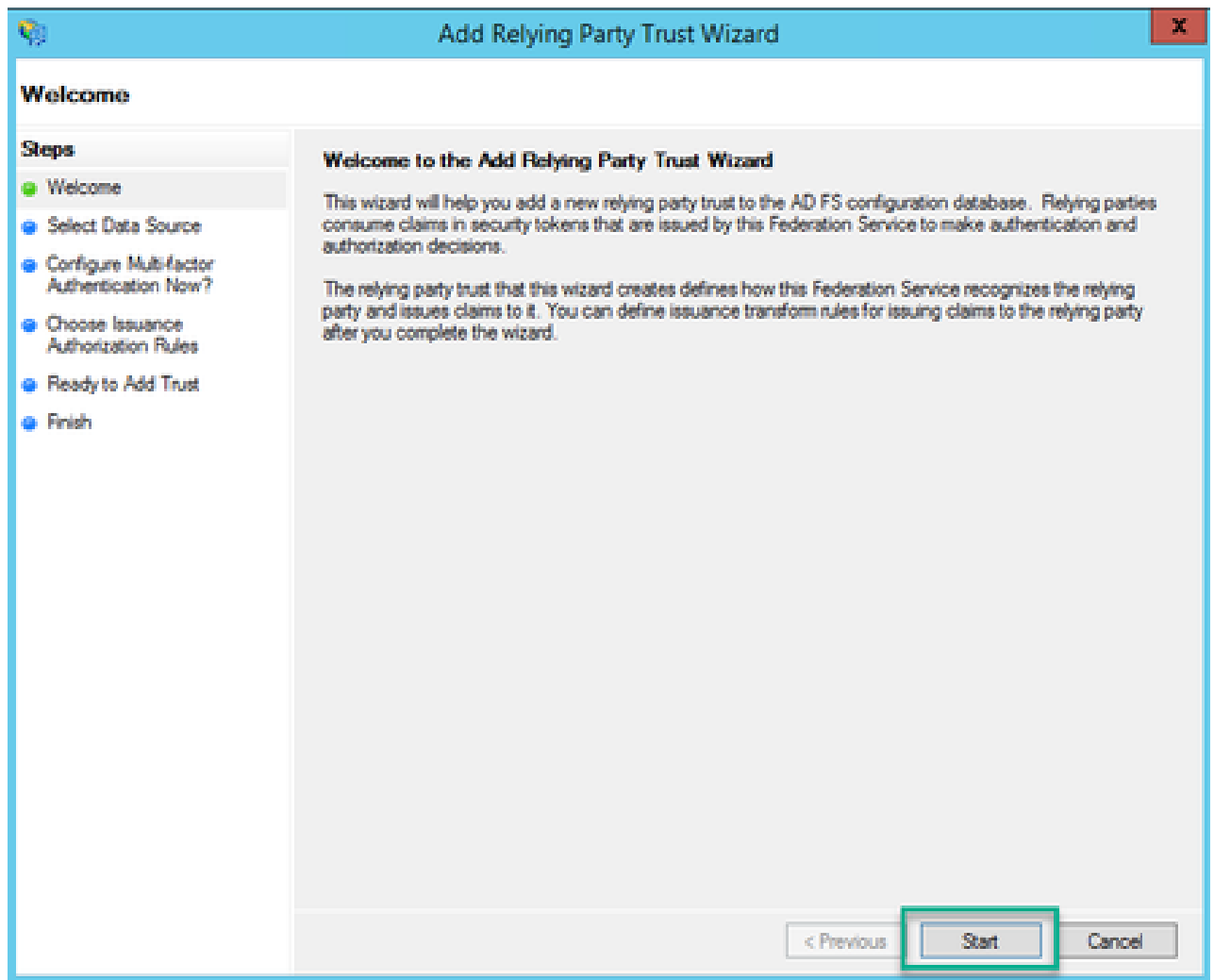
3. Navigieren Sie in der ADFS-Verwaltungskonsole im linken Bereich zu ADFS > Trust Relationships > Relying Party Trust.



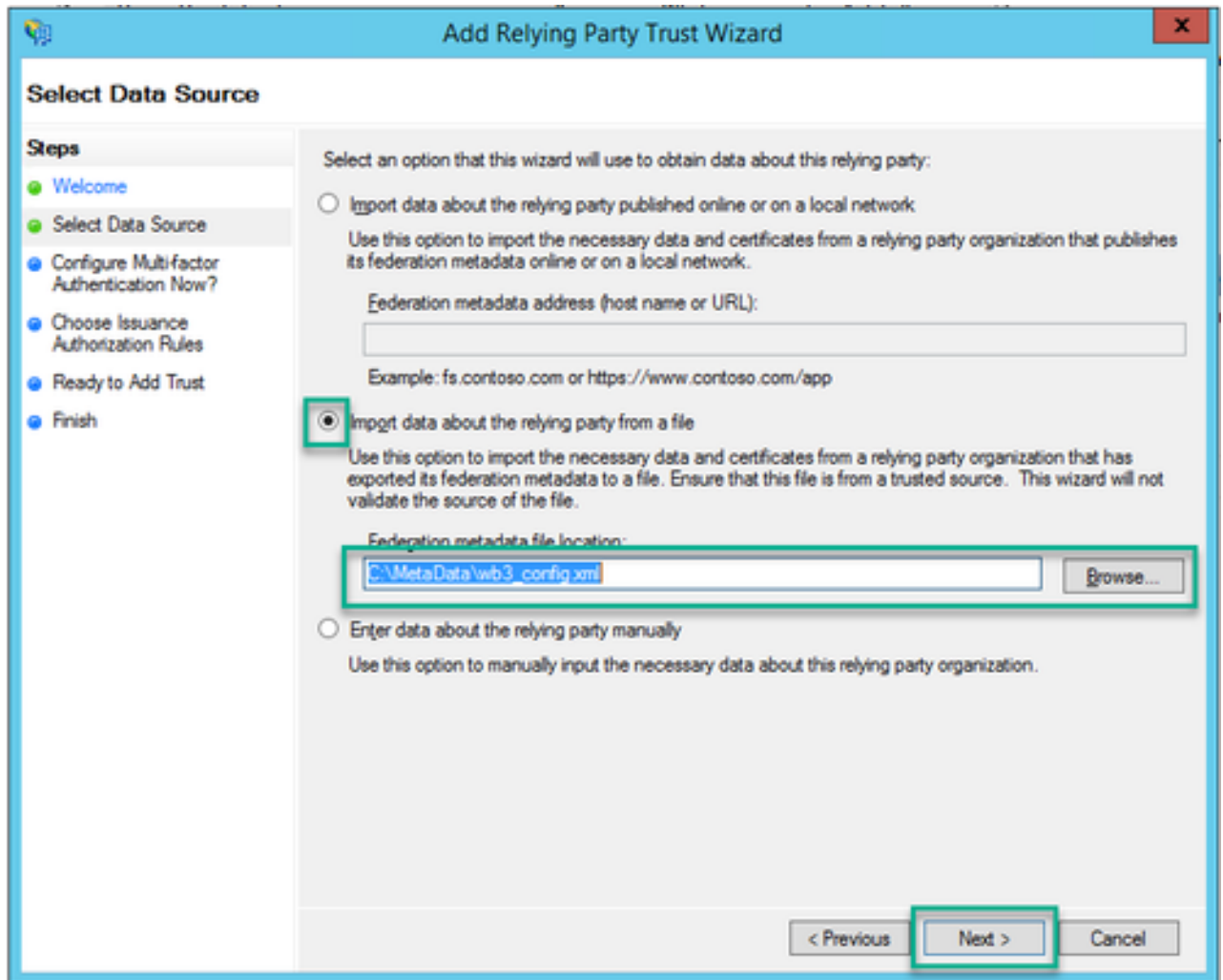
4. Wählen Sie im rechten Bereich der ADFS-Verwaltungskonsolle die Option Vertrauenswürdigkeit der vertrauenden Partei hinzufügen... aus.



5. Nachdem Sie diese Option ausgewählt haben, wird der Assistent zum Hinzufügen von Vertrauensstellungen für vertrauende Parteien geöffnet. Wählen Sie die Option Start.



6. Wählen Sie auf der Seite Datenquelle auswählen das Optionsfeld Daten über die vertrauende Partei aus einer Datei importieren aus, und wählen Sie Durchsuchen und navigieren Sie zum Speicherort der Webbridge-MetaData-Datei.



7. Geben Sie auf der Seite Anzeigenamen angeben einen Namen ein, der für die Entität in ADFS angezeigt werden soll (der Anzeigename dient nicht als Server für die ADFS-Kommunikation und ist rein informativ).

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 progression: Welcome, Select Data Source, Specify Display Name (current), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains a text box for "Display name:" with the text "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

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

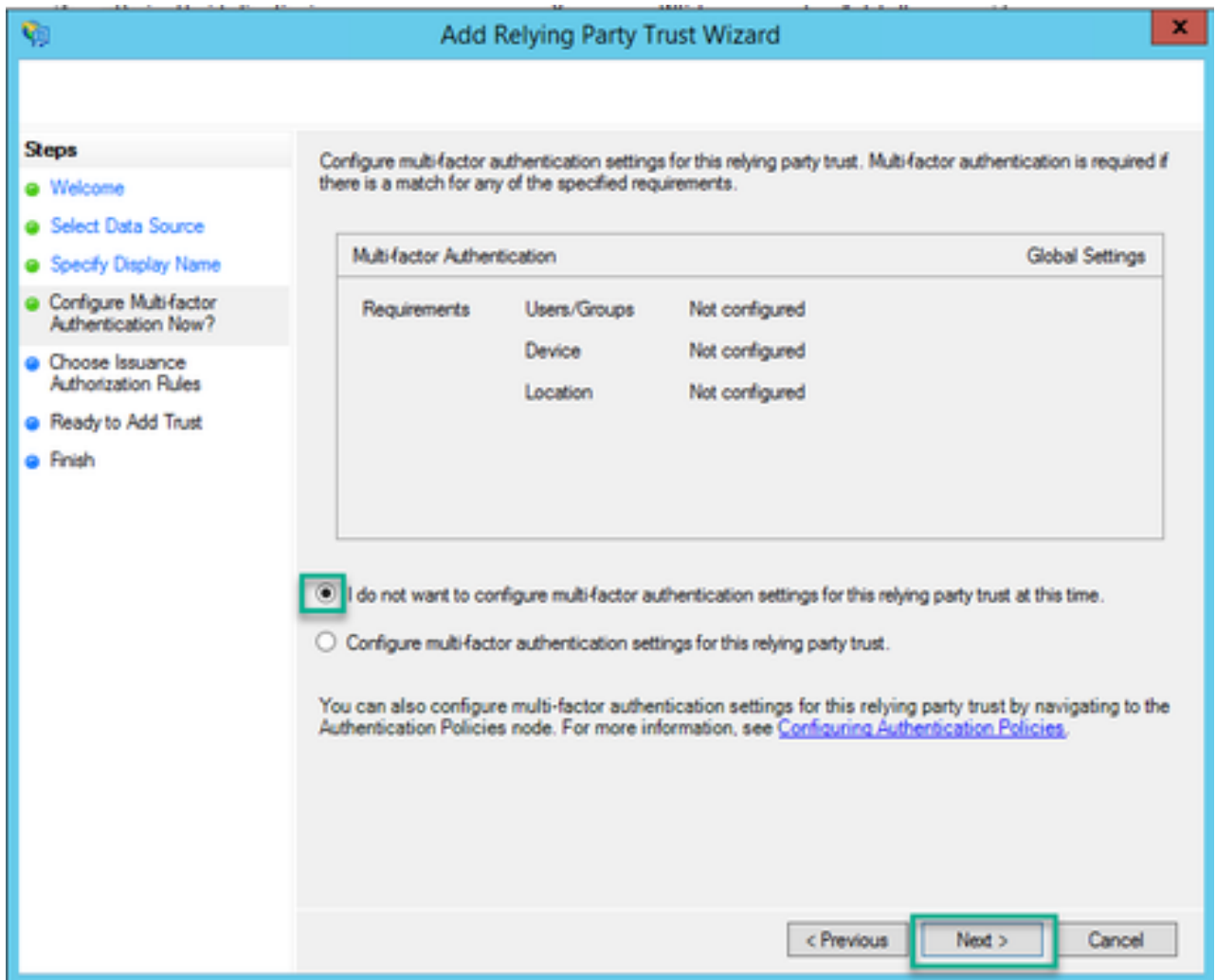
Enter the display name and any optional notes for this relying party.

Display name: Webbridge CMS SSO

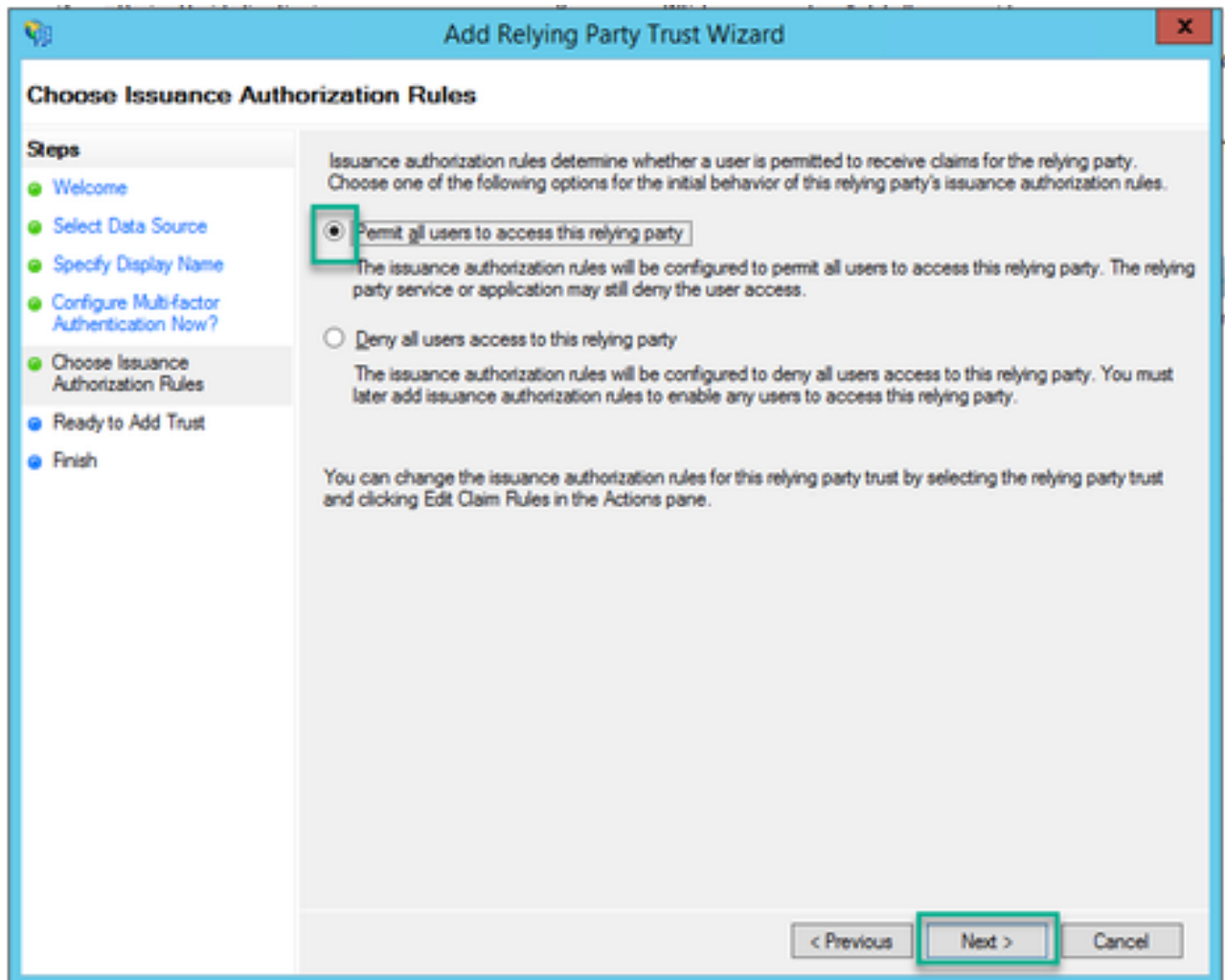
Notes: This is the relying trust part for CMS SSO with WebApp

< Previous Next > Cancel

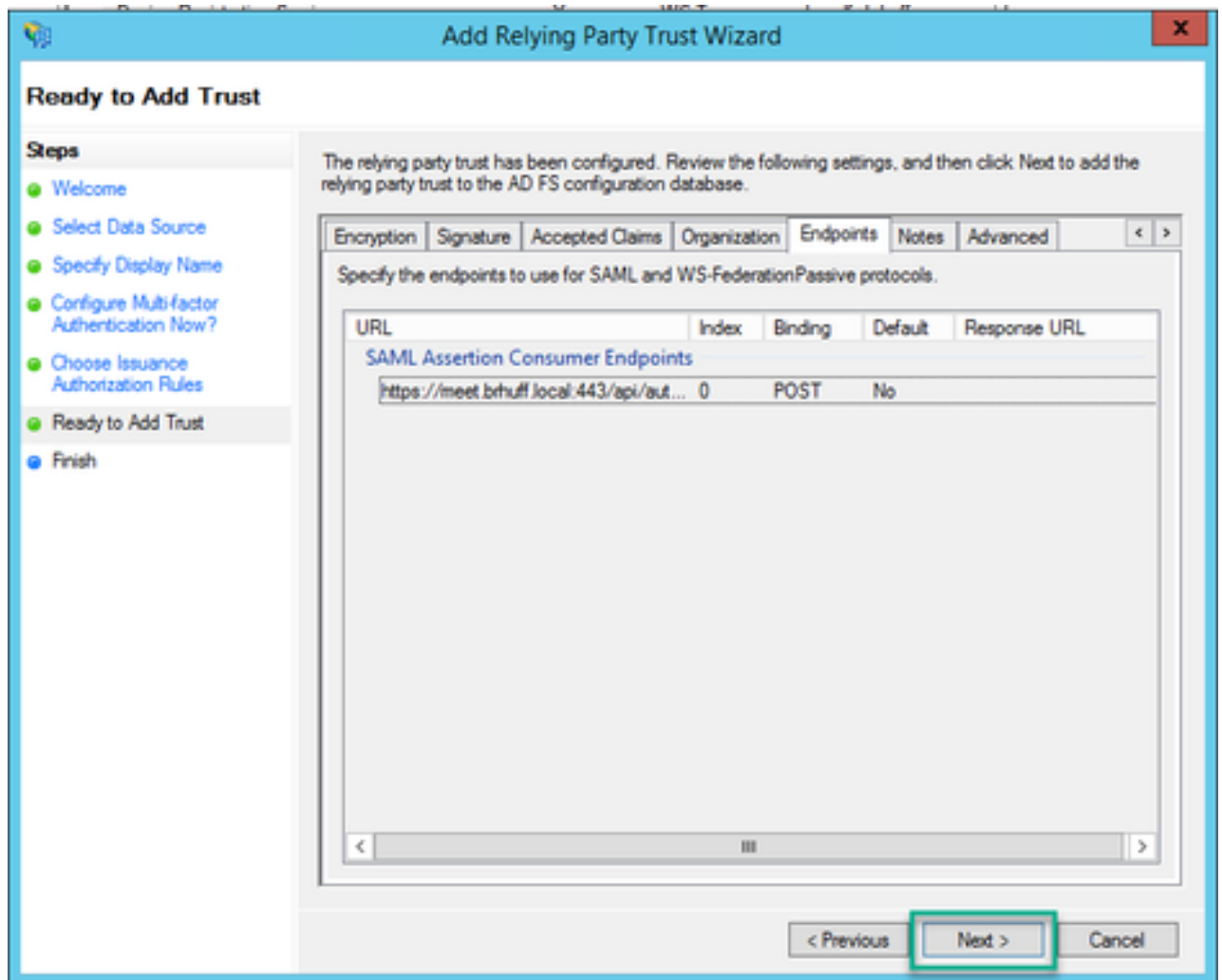
8. Wählen Sie auf der Seite Multi-Factor Authentication Now? (Multifaktor-Authentifizierung jetzt konfigurieren) die Option Next (Weiter).



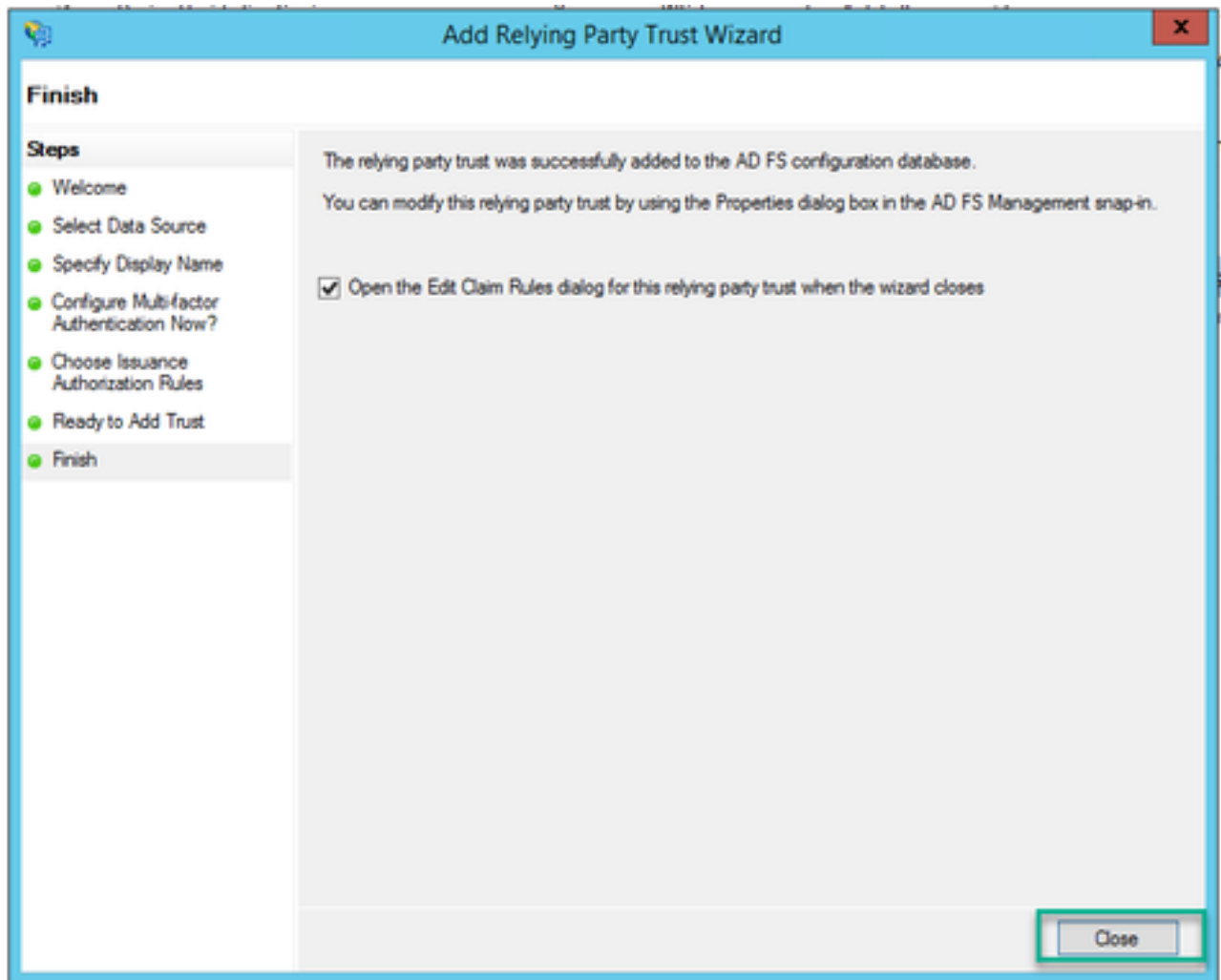
9. Belassen Sie auf der Seite Issuance-Autorisierungsregeln auswählen die Auswahl für Alle Benutzer den Zugriff auf diese vertrauende Seite erlauben unverändert.



10. Auf der Seite Ready to Add Trust (Bereit, Vertrauenswürdigkeit hinzuzufügen) können die importierten Details der Relying Trust Party für Webbridge über die Registerkarten überprüft werden. Überprüfen Sie die Bezeichner und Endpunkte auf die URL-Details für den Webbridge-Dienstanbieter.



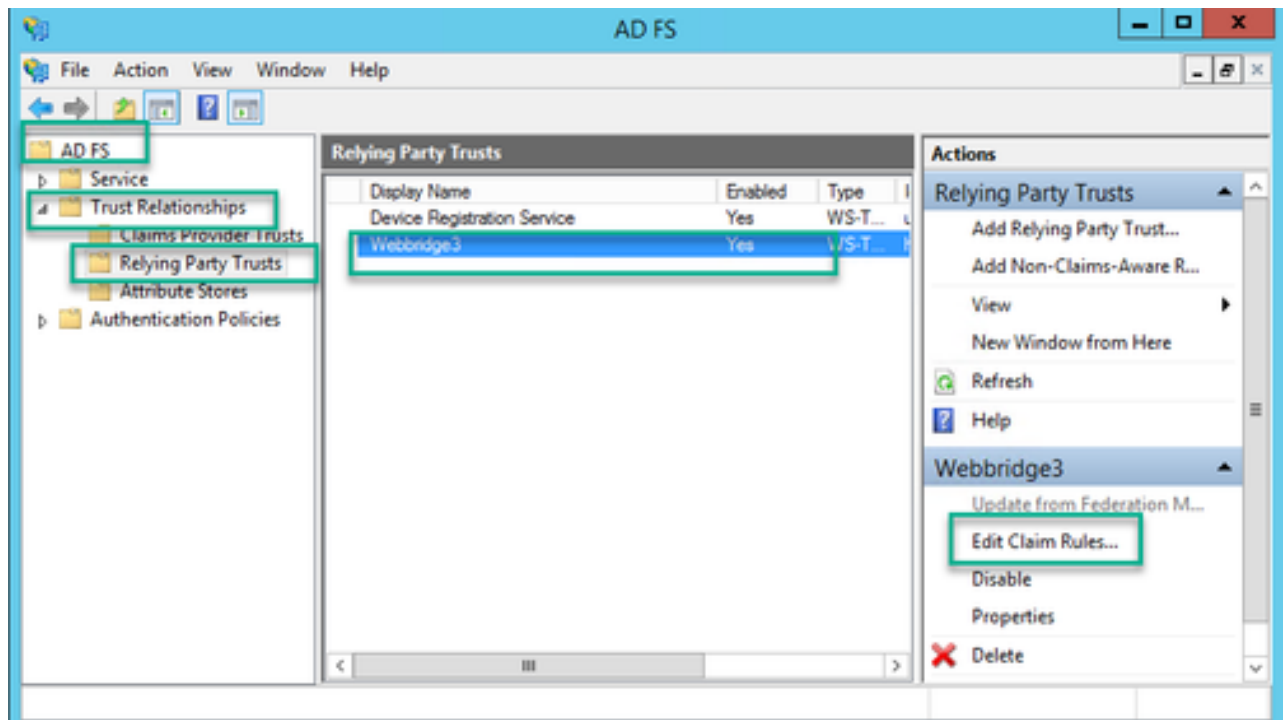
11. Wählen Sie auf der Seite Fertig stellen die Option Schließen, um den Assistenten zu schließen und mit der Bearbeitung der Anspruchsregeln fortzufahren.



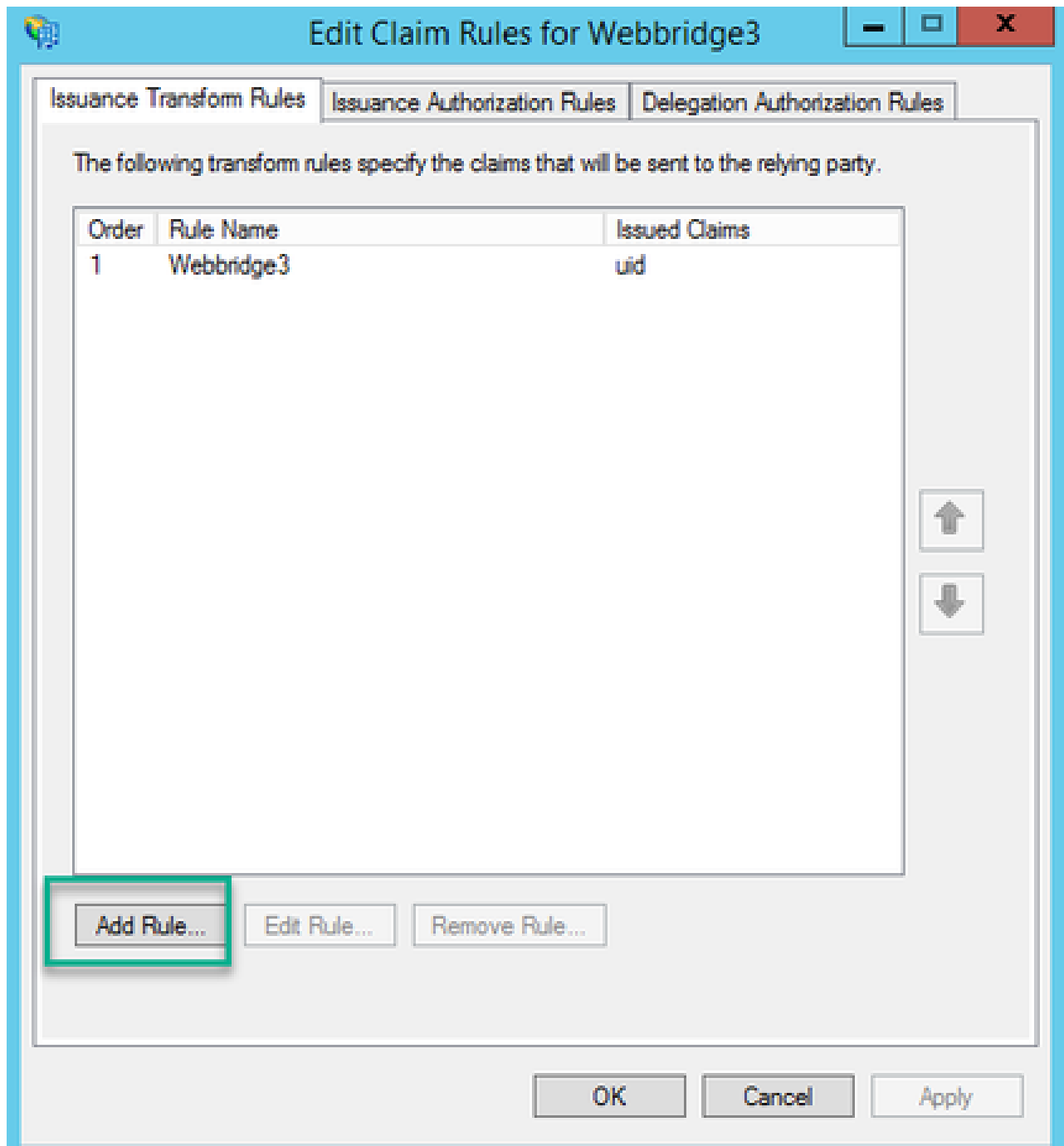
Erstellen von Anspruchsregeln für den Webbridge-Dienst auf dem IdP

Nachdem die Vertrauensstellung der vertrauenden Partei für die Webbridge erstellt wurde, können Anspruchsregeln erstellt werden, um bestimmte LDAP-Attribute an ausgehende Anspruchstypen anzupassen, die der Webbridge in der SAML-Antwort bereitgestellt werden.

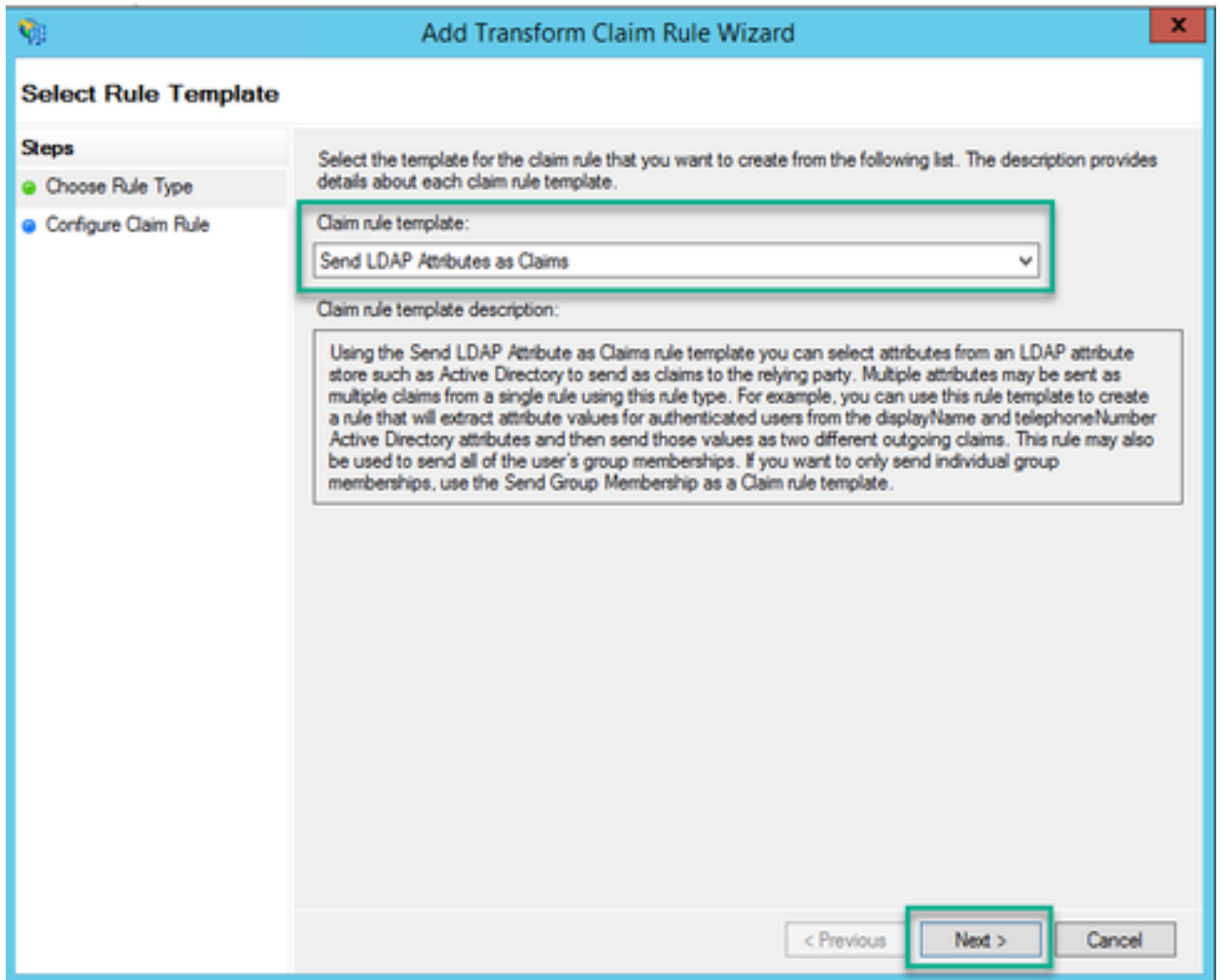
1. Markieren Sie in der ADFS-Verwaltungskonsole die Vertrauenswürdigkeit der vertrauenden Partei für die Webbridge, und wählen Sie im rechten Bereich Anspruchsregeln bearbeiten aus.



2. Wählen Sie auf der Seite Anspruchsregeln für <DisplayName> bearbeiten die Option Regel hinzufügen....



3. Wählen Sie auf der Seite Assistent zum Umwandeln von Anspruchsregeln hinzufügen die Option LDAP-Attribute als Ansprüche für die Anspruchsregelvorlage senden, und wählen Sie Weiter aus.



4. Konfigurieren Sie auf der Seite Anspruchsregel konfigurieren die Anspruchsregel für die Vertrauensstellung der vertrauenden Partei mit folgenden Werten:

1. Name der Anspruchsregel = dies muss ein Name sein, der der Regel in ADFS zugewiesen wurde (nur für Regelreferenz)
2. Attributspeicher = Active Directory
3. LDAP-Attribut = Diese Eigenschaft muss mit der authenticationIdMapping in der Callbridge-API übereinstimmen. (Beispiel: \$sAMAccountName\$.)
4. Ausgehender Anspruchstyp = Dieser muss mit der authenticationIdMapping-Eigenschaft in der Webbridge SSO-config.json übereinstimmen. (Beispiel: 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

SSO-Archiv-ZIP-Datei für Webbridge erstellen:

Auf diese Konfiguration verweist Webbridge, um die SSO-Konfiguration für unterstützte Domänen, die Authentifizierungszuordnung usw. zu validieren. Diese Regeln müssen für diesen Teil der Konfiguration berücksichtigt werden:

- Die ZIP-Datei MUSS mit dem Präfix sso_ auf den Dateinamen beginnen (z. B. sso_cmstest.zip).
- Wenn diese Datei hochgeladen wurde, deaktiviert Webbridge die grundlegende Authentifizierung, und für die Webbridge, auf die diese hochgeladen wurde, kann NUR SSO

verwendet werden.

- Wenn mehrere Identity Provider verwendet werden, muss eine separate ZIP-Datei mit einem anderen Namensschema hochgeladen werden (STILL mit dem Präfix sso_).
- Wenn Sie die ZIP-Datei erstellen, markieren und zippen Sie den Dateiinhalte, und legen Sie die erforderlichen Dateien nicht in einen Ordner, in dem Sie die ZIP-Datei erstellen möchten.

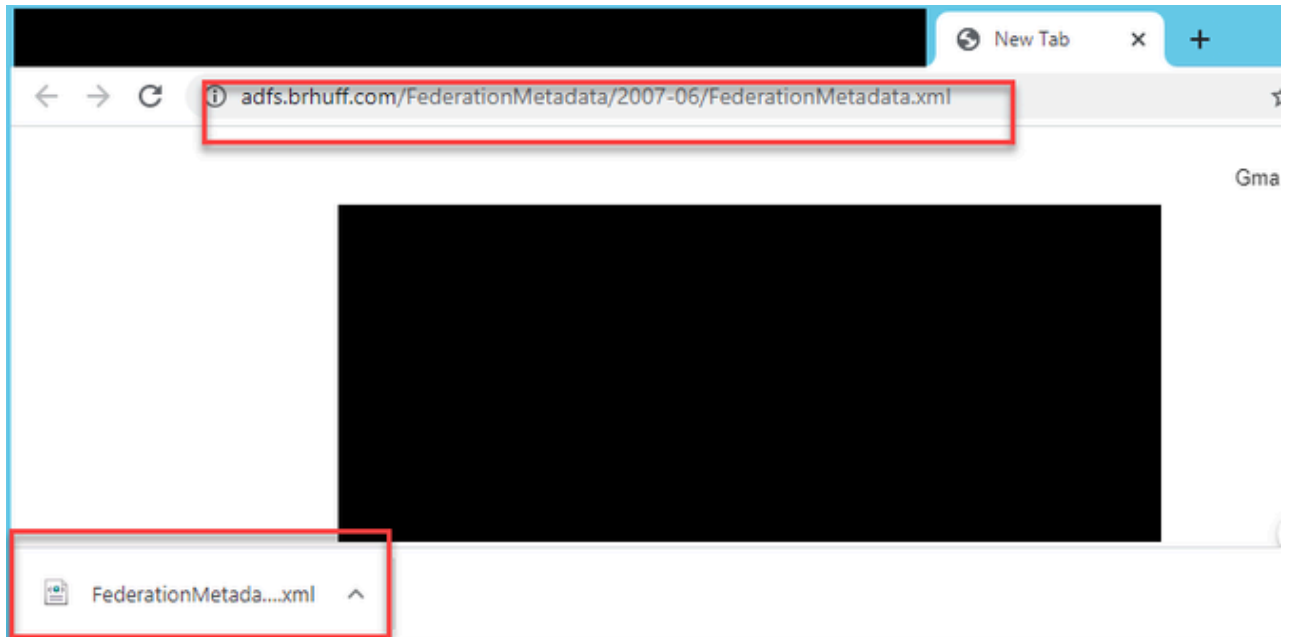
Der Inhalt der ZIP-Datei besteht aus 2 bis 4 Dateien, je nachdem, ob Verschlüsselung verwendet wird oder nicht.

Dateiname	Beschreibung	Erforderlich?
idp_config.xml	Dies ist die MetaData-Datei, die von idP gesammelt werden kann. In ADFS finden Sie diese Informationen unter <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml .	JA
config.json	Dies ist die JSON-Datei, mit der Webbridge die unterstützten Domänen validiert, d. h. die Authentifizierungszuordnung für SSO.	JA
sso_sign.key	Dies ist der private Schlüssel für den öffentlichen Signaturschlüssel, der auf dem Identitätsanbieter konfiguriert wurde. Wird nur zum Sichern der signierten Daten benötigt	NEIN
sso_encrypt.key	Dies ist der private Schlüssel für den öffentlichen Verschlüsselungsschlüssel, der auf dem Identitätsanbieter konfiguriert wurde. Wird nur zur Sicherung der verschlüsselten Daten benötigt	NEIN

Rufen Sie die Datei idp_config.xml ab, und konfigurieren Sie sie.

1. Öffnen Sie auf dem ADFS-Server (oder einem Speicherort, der Zugriff auf das ADFS hat) einen Webbrowser.

2. Geben Sie im Webbrowser die URL <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml> ein (Sie können auch localhost anstelle des FQDN verwenden, wenn Sie sich lokal auf dem ADFS-Server befinden). Dadurch wird die Datei FederationMetadata.xml heruntergeladen.



3. Kopieren Sie die heruntergeladene Datei an einen Speicherort, an dem die ZIP-Datei erstellt wird, und benennen Sie sie in idp_config.xml um.

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

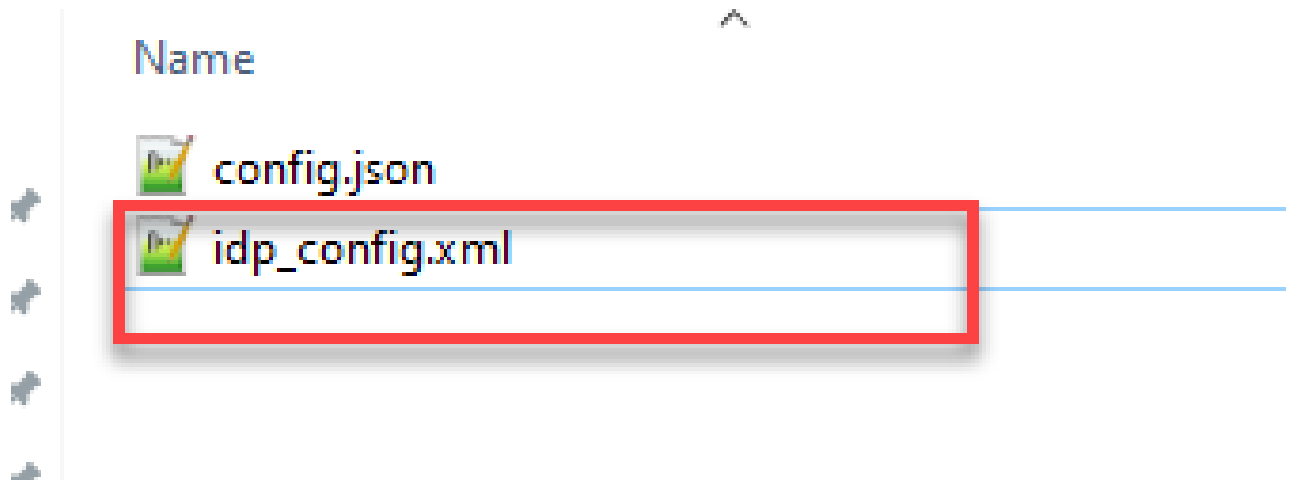
Create shortcut

Delete

Rename

Properties

Local Disk (D:) > brentssoconfig > SSOconfig



Erstellen Sie die Datei config.json mit dem Inhalt.

Die config.json enthält die folgenden drei Attribute und muss in Klammern enthalten sein, { }:

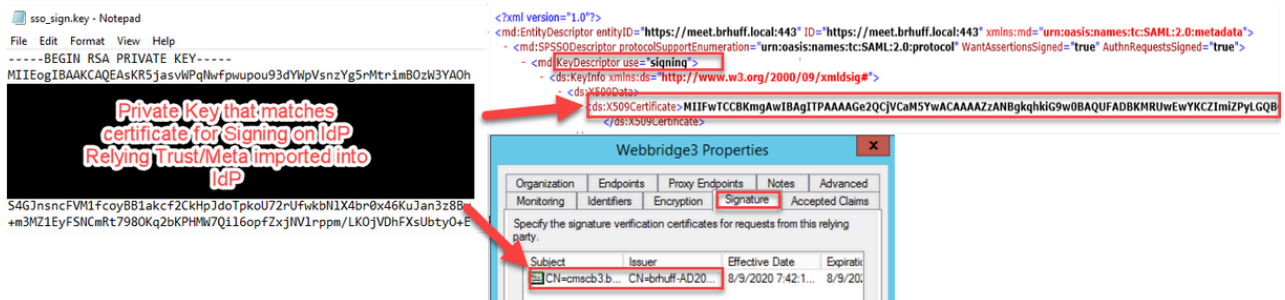
1. supportedDomains (Unterstützte Domänen) - Dies ist eine Liste von Domänen, die für die SSO-Authentifizierung anhand der IdP überprüft werden. Mehrere Domänen können durch ein Komma getrennt werden.
2. authenticationIdMapping: Dies ist der Parameter, der als Teil der ausgehenden Anspruchsregel von ADFS/IdP zurückgegeben wird. Dies muss mit dem Namenswert des ausgehenden Anspruchstyps für die IdP übereinstimmen. Anspruchsregel.
3. ssoServiceProviderAddress: Dies ist die FQDN-URL, an die der Identifizierungsanbieter die SAML-Antworten sendet. Hierbei muss es sich um den Webbridge-FQDN handeln.

Legen Sie den Schlüssel sso_sign.key fest (OPTIONAL).

Diese Datei muss den privaten Schlüssel des Zertifikats enthalten, das zum Signieren in den Webbridge-Metadaten verwendet wird, die in den IdP importiert wurden. Das zum Signieren verwendete Zertifikat kann während des Imports der Webbridge-Metadaten im ADFS festgelegt werden, indem das X509Certificate mit den Zertifikatinformationen im Abschnitt <KeyDescriptor use=signing> gefüllt wird. Sie kann auch auf ADFS in der Webbridge Relying Trust Party unter Eigenschaften > Signatur angezeigt (und importiert) werden.

Im nächsten Beispiel sehen Sie das Callbridge-Zertifikat (CN=cmscb3.brhuff.local), das den Webbridge-Metadaten hinzugefügt wurde, bevor es in ADFS importiert wurde. Der in sso_sign.key eingefügte private Schlüssel entspricht dem cmscb3.brhuff.local-Zertifikat.

Dies ist eine optionale Konfiguration, die nur bei der Verschlüsselung der SAML-Antworten erforderlich ist.

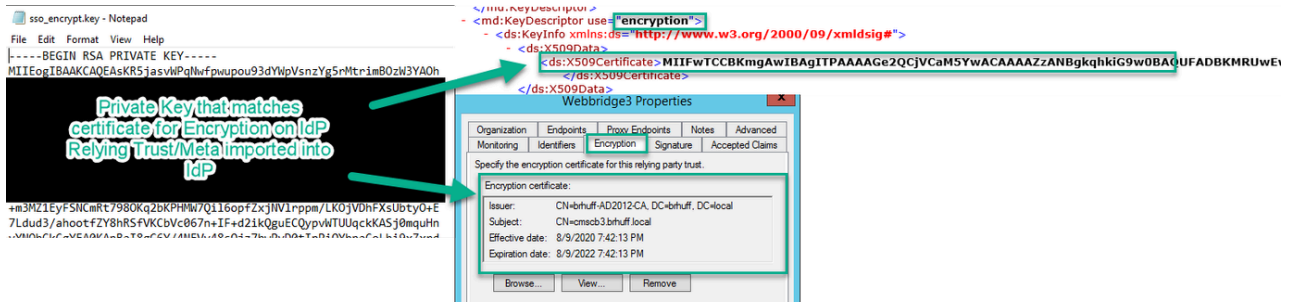


Legen Sie den Schlüssel sso_encrypt.key fest (OPTIONAL).

Diese Datei muss den privaten Schlüssel des Zertifikats enthalten, das für die Verschlüsselung in den Webbridge-Metadaten verwendet wird, die in den IdP importiert wurden. Das für die Verschlüsselung verwendete Zertifikat kann während des Imports der Webbridge-Metadaten im ADFS festgelegt werden, indem das X509Certificate mit den Zertifikatinformationen im Abschnitt <KeyDescriptor use=encryption> gefüllt wird. Sie kann auch auf ADFS in der Webbridge Relying Trust Party unter Eigenschaften > Verschlüsselung angezeigt (und importiert) werden.

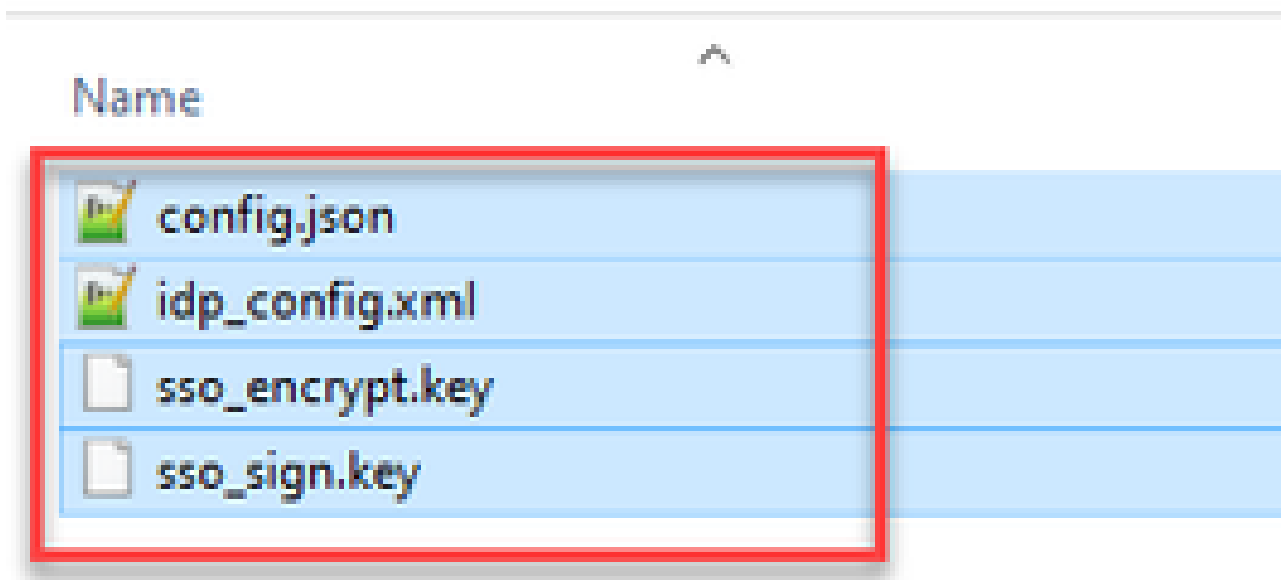
Im nächsten Beispiel sehen Sie das Callbridge-Zertifikat (CN=cmscb3.brhuff.local), das den Webbridge-Metadaten vor dem Importieren in ADFS hinzugefügt wurde. Der in 'sso_encrypt.key' eingefügte private Schlüssel entspricht dem Zertifikat cmscb3.brhuff.local.

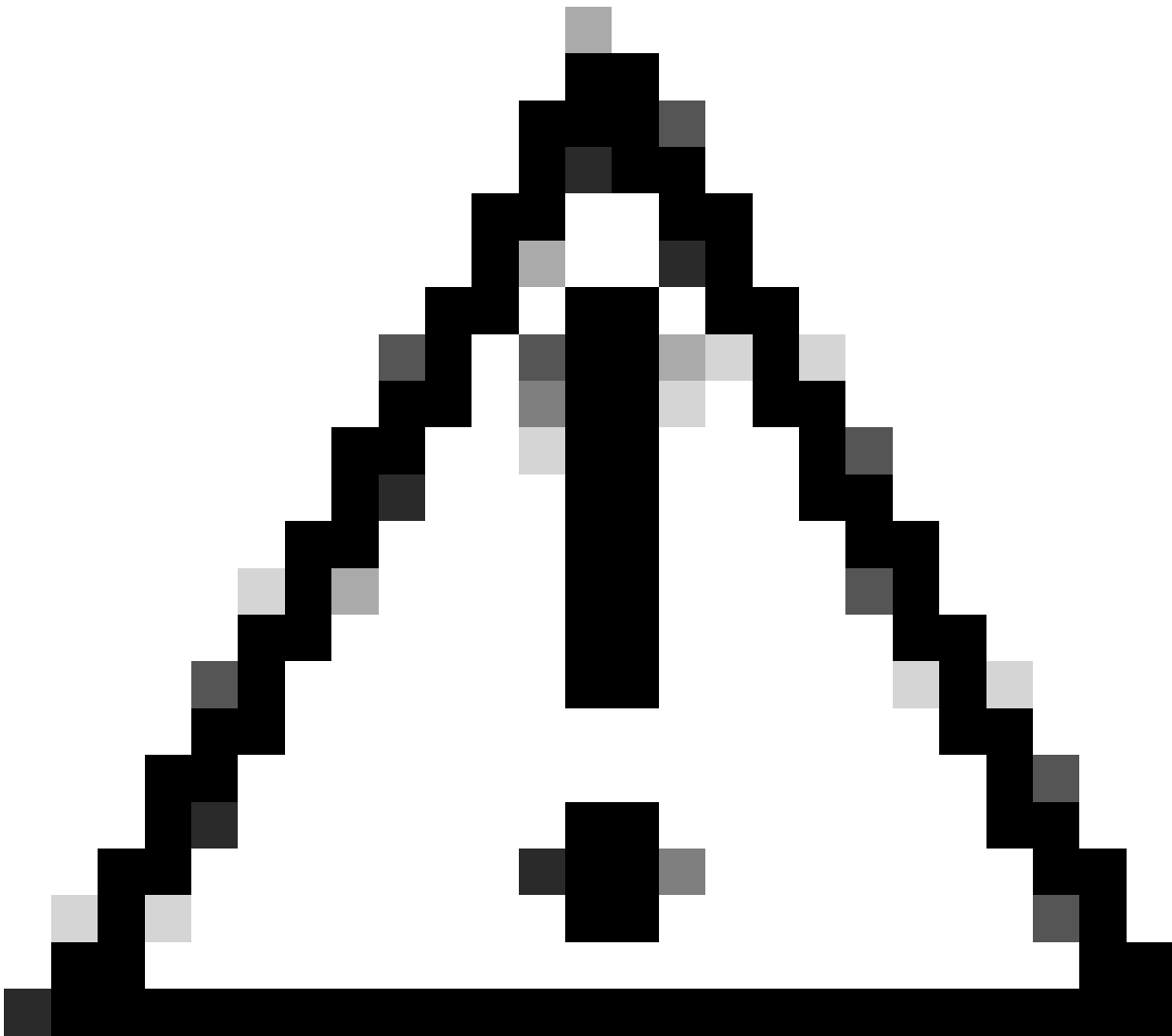
Dies ist eine optionale Konfiguration und wird nur benötigt, wenn Sie die SAML-Antworten verschlüsseln möchten.



Erstellen der SSO-ZIP-Datei

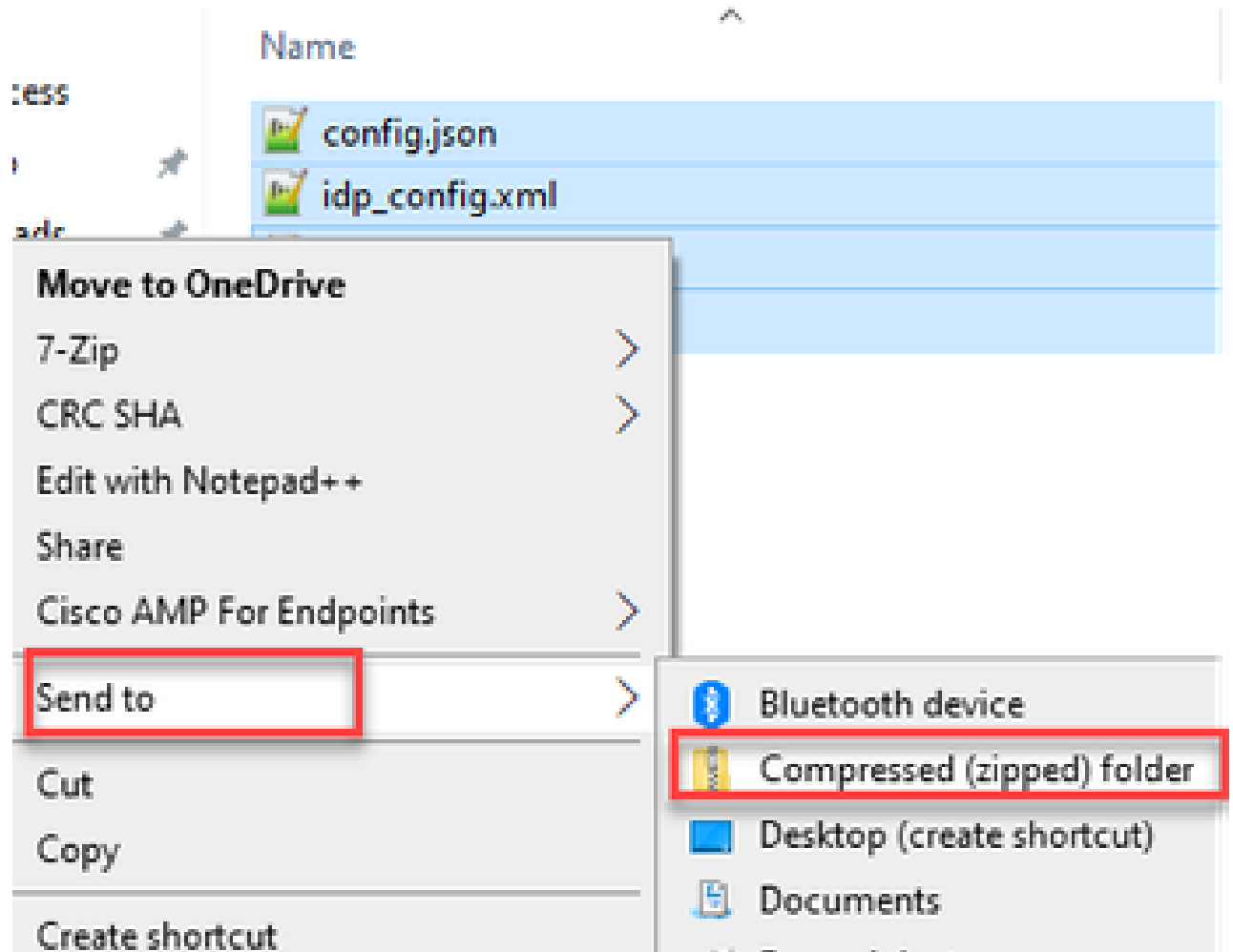
1. Markieren Sie alle Dateien, die für die SSO-Konfigurationsdatei verwendet werden sollen.



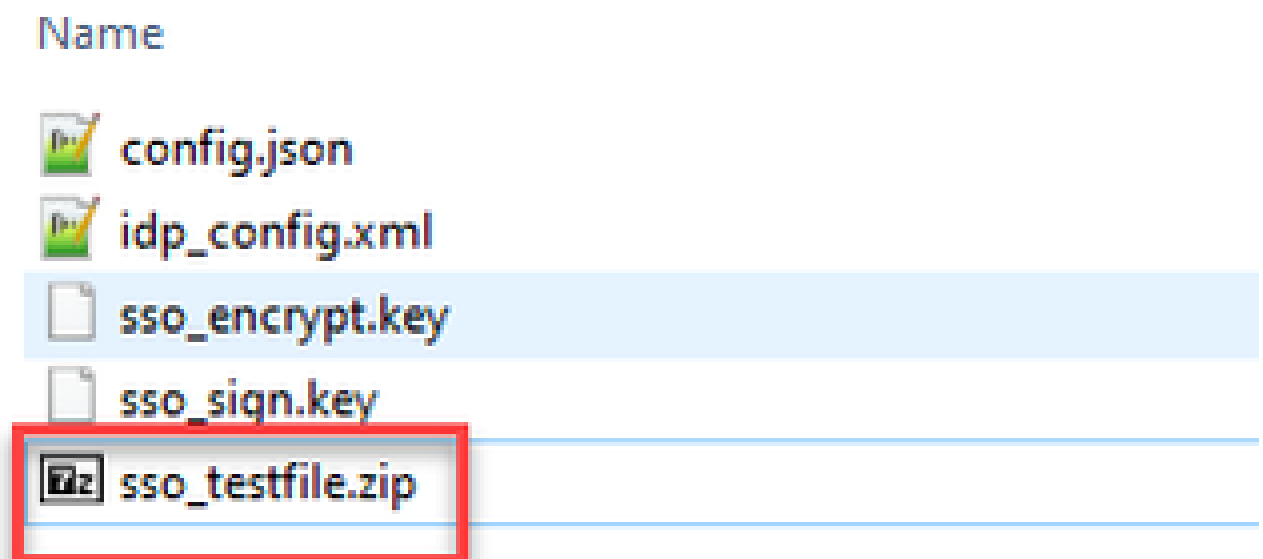


Achtung: ZIP-Datei nicht in den Ordner, der die Dateien enthält, da dies dazu führt, dass die SSO nicht funktioniert.

2. Klicken Sie mit der rechten Maustaste auf die hervorgehobenen Dateien und wählen Sie Senden an > ZIP-komprimierten Ordner.



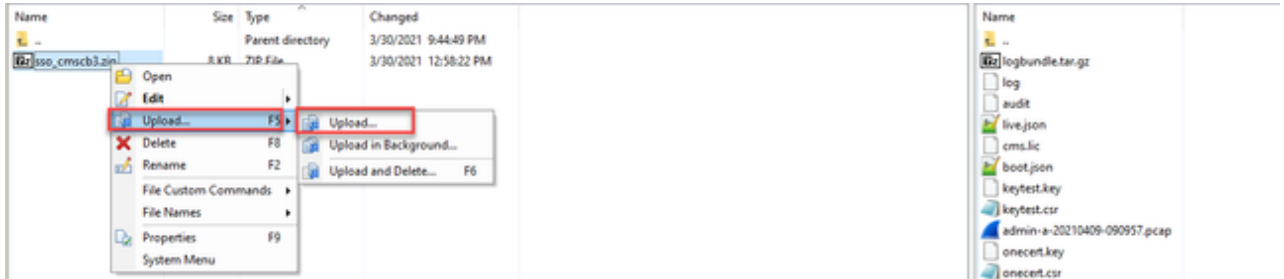
3. Nachdem die Dateien komprimiert wurden, benennen Sie sie mit dem Präfix sso_in den gewünschten Namen um:



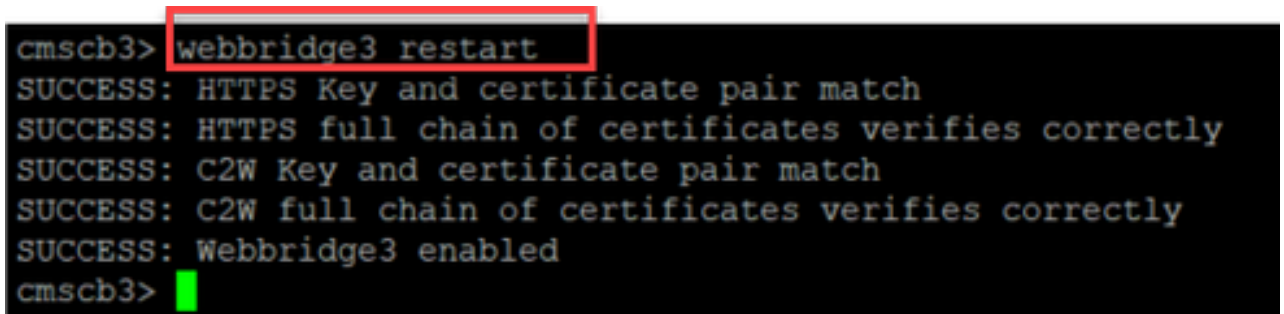
SSO-Zip-Datei(en) auf Webbridge hochladen

Öffnen Sie einen SFTP/SCP-Client, in diesem Beispiel wird WinSCP verwendet, und stellen Sie eine Verbindung mit dem Server her, der Webbridge3 hostet.

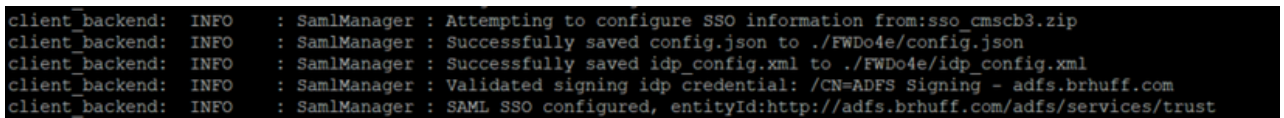
1. Navigieren Sie im linken Bereich zum Speicherort der SSO-Zip-Datei, und klicken Sie mit der rechten Maustaste auf "Hochladen", oder ziehen Sie die Datei per Drag & Drop.



2. Wenn die Datei vollständig auf den Webbridge3-Server hochgeladen wurde, öffnen Sie eine SSH-Sitzung, und führen Sie den Befehl `webbridge3 restart` aus.



3. Im Syslog geben diese Meldungen an, dass die SSO-Aktivierung erfolgreich war:



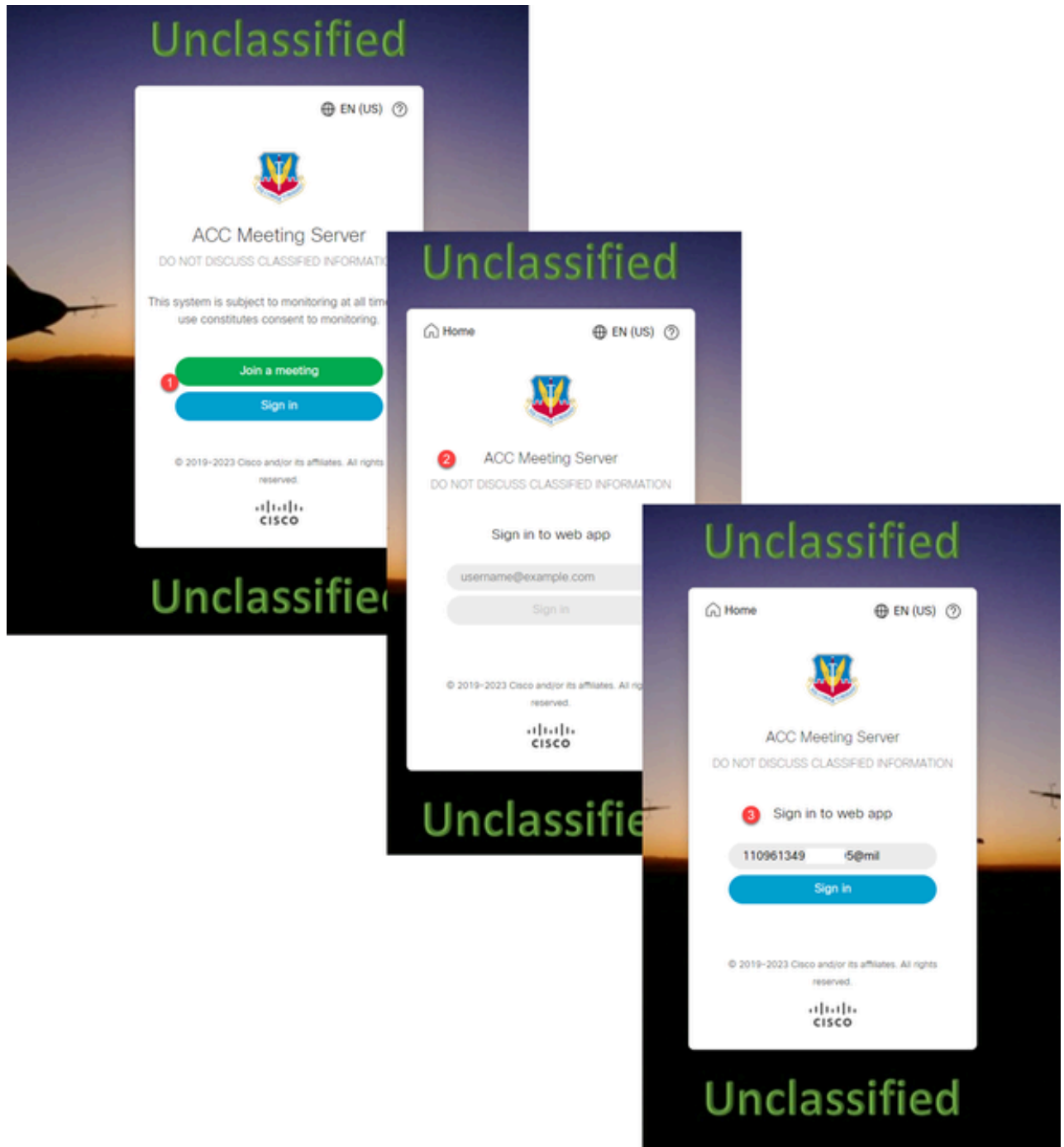
Common Access Card (CAC)

Eine Common Access Card (CAC) ist eine Smartcard, die als Standardkennung für aktives militärisches Personal, zivile DoD-Mitarbeiter und teilnahmeberechtigtes Auftragnehmerpersonal dient.

Hier sehen Sie den gesamten Anmeldevorgang für Benutzer, die CAC-Karten verwenden:

1. PC einschalten und CAC-Karte einstecken
2. Melden Sie sich an (wählen Sie manchmal ein Zertifikat aus), und geben Sie "Pin" ein.

3. Browser öffnen
4. Navigieren Sie zur Join-URL, und zeigen Sie die Optionen An einem Meeting teilnehmen oder Anmelden an.
5. Sign in: Geben Sie den Benutzernamen ein, der als jidMapping konfiguriert ist und Active Directory von einem CAC-Login erwartet
6. Hit-Anmeldung
7. Die ADFS-Seite wird kurz angezeigt und automatisch ausgefüllt
8. Der Benutzer wird an diesem Punkt angemeldet.

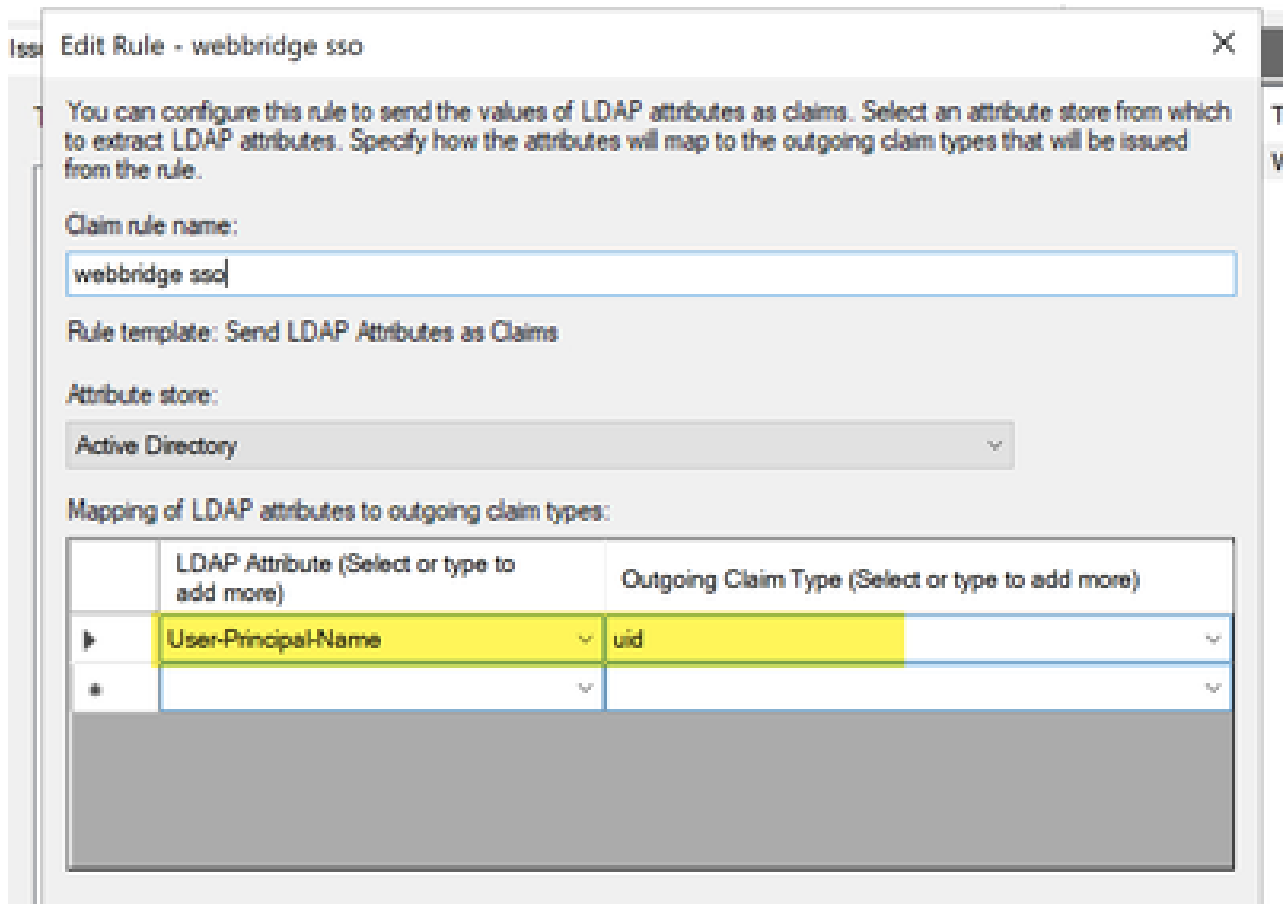


Konfigurieren Sie jidMapping (dies ist der Benutzername) in Ldapmapping genauso wie das, was ADFS für die CAC-Karte verwendet. \$userPrincipalName\$ (Groß- und Kleinschreibung beachten)

Legen Sie außerdem das gleiche LDAP-Attribut für authenticationIdMapping fest, damit es mit

dem Attribut übereinstimmt, das in der Anspruchsregel in ADFS verwendet wird.

In diesem Fall sendet die Anspruchsregel \$userPrincipalName\$ als UID zurück an das CMS.



Testen von SSO Anmeldung über WebApp

Nachdem SSO konfiguriert wurde, können Sie den Server testen:

1. Navigieren Sie zur Webbridge-URL für die Web-App, und wählen Sie die Schaltfläche Anmelden aus.



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

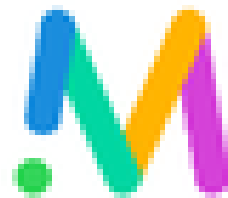
Join a meeting

Sign in

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



2. Dem Benutzer wird die Möglichkeit zur Eingabe seines Benutzernamens angezeigt (Option "Hinweis: kein Kennwort" auf dieser Seite).



Cisco Meeting Server

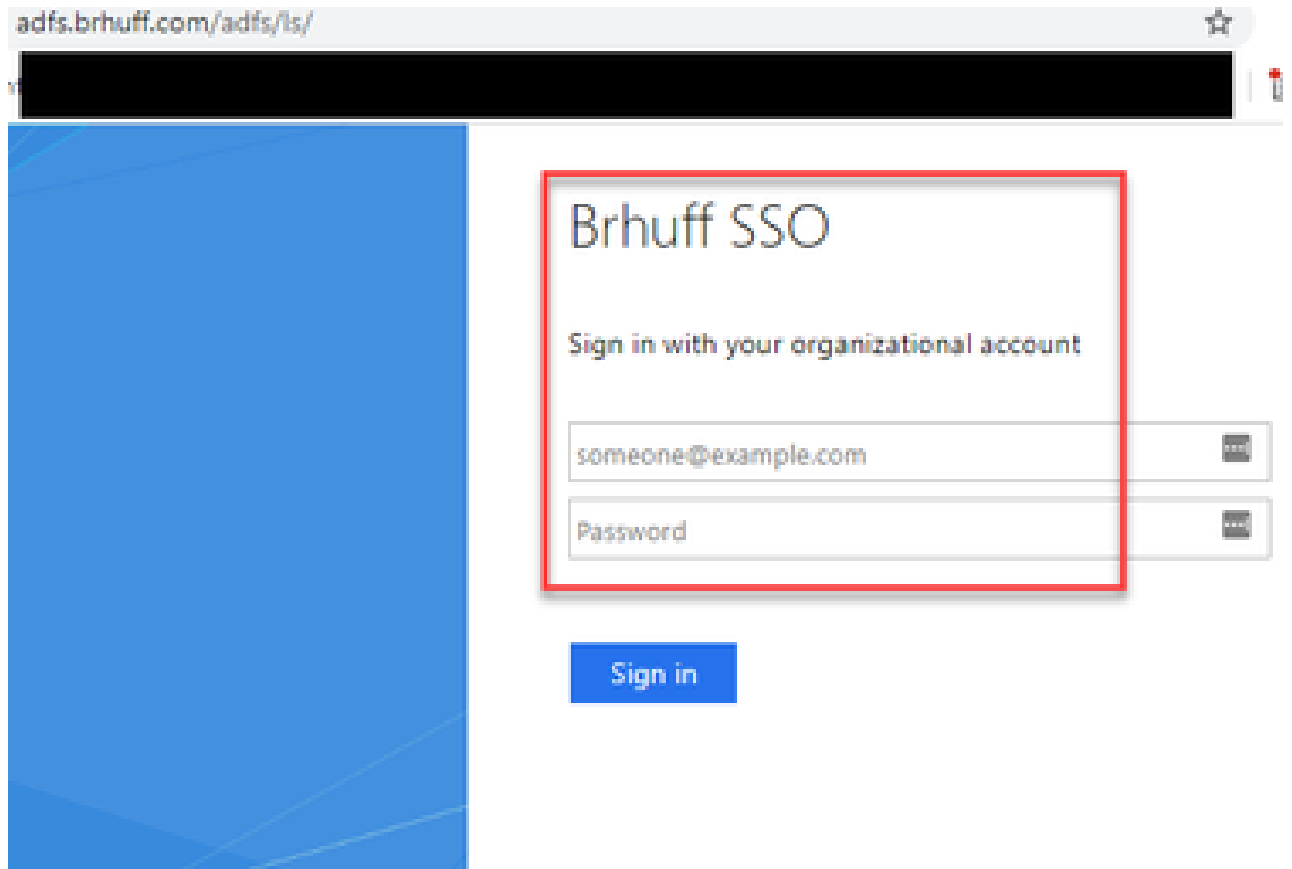
web app

Sign in to web app

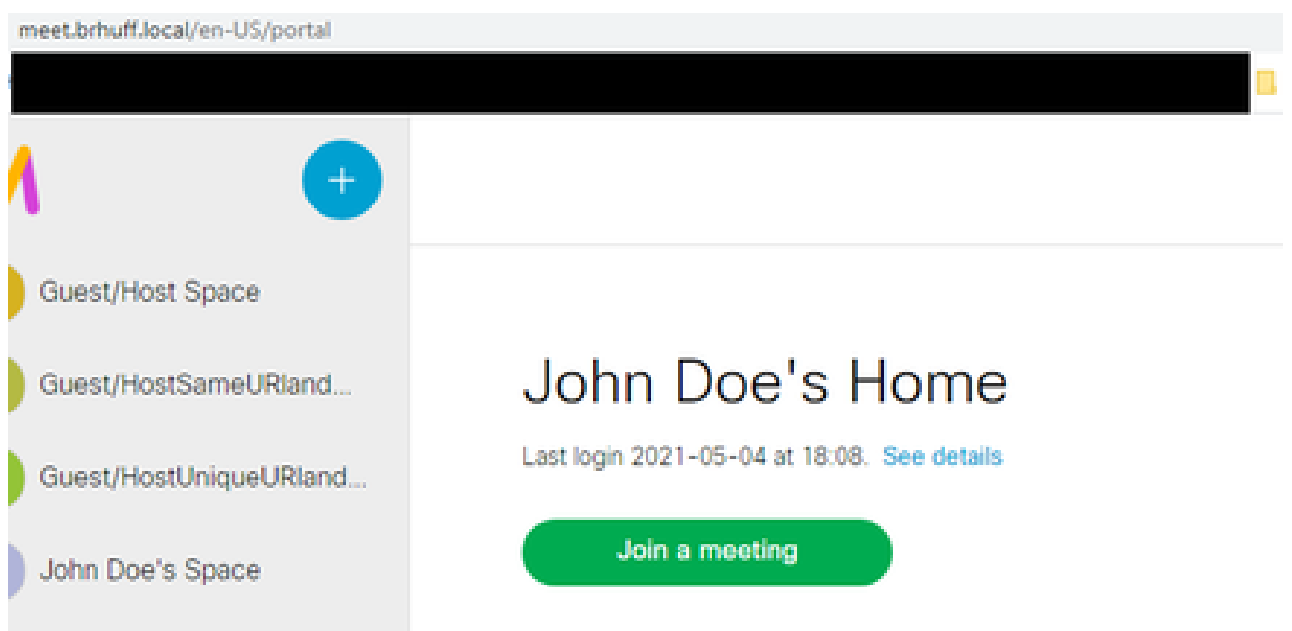
© 2020 Cisco and/or its affiliates. All rights reserved.



3. Der Benutzer wird dann (nach Eingabe der Benutzerdetails) auf die ADFS-Seite weitergeleitet, auf der er seine Anmeldeinformationen eingeben muss, um sich bei IdP zu authentifizieren.



4. Der Benutzer wird nach Eingabe und Validierung der Anmeldeinformationen mit der IdP mit dem Token umgeleitet, um auf die Web App-Startseite zuzugreifen:



Fehlerbehebung

Grundlegende Fehlerbehebung

Grundlegende Fehlerbehebung bei SSO-Problemen:

1. Stellen Sie sicher, dass die erstellten Metadaten für Webbridge3, die als Relying Trust in IdP importiert werden, richtig konfiguriert sind und die konfigurierte URL genau der `ssoServiceProviderAddress` in der `config.json` entspricht.
2. Stellen Sie sicher, dass die von IdP bereitgestellten und in die Webbridge3-Konfigurationsdatei gezippten Metadaten die aktuellsten von IdP sind. Wenn sich beispielsweise der Hostname, die Zertifikate usw. des Servers ändern, muss die Datei erneut exportiert und in die Konfigurationsdatei gezippt werden.
3. Wenn Sie private Schlüssel zur Verschlüsselung von Daten verwenden, stellen Sie sicher, dass die richtigen übereinstimmenden Schlüssel Teil der Datei `sso_xxxx.zip` sind, die Sie auf `webbridge` hochgeladen haben. Versuchen Sie nach Möglichkeit, ohne die optionalen privaten Schlüssel zu testen, ob SSO ohne diese verschlüsselte Option funktioniert.
4. Stellen Sie sicher, dass die Datei `config.json` mit den richtigen Details für SSO-Domänen, Webbridge3-URL UND die erwartete Authentifizierungszuordnung konfiguriert ist, die aus der SAMLResponse übereinstimmen.

Es empfiehlt sich auch, die Fehlerbehebung aus der Protokollsicht zu versuchen:

1. Wenn Sie zur Webbridge-URL navigieren, setzen Sie `?trace=true` an das Ende der URL, um eine ausführliche Protokollierung im CMS-Syslog zu aktivieren. (Bsp.: <https://join.example.com/en-US/home?trace=true>).
2. Führen Sie das Syslog follow-Protokoll auf dem Webbridge3-Server aus, um während des Tests Live-Daten zu erfassen, oder führen Sie den Test mit der Trace-Option aus, die an die URL angefügt ist, und erfassen Sie die Datei "logbundle.tar.gz" von den Webbridge3- und CMS Callbridge-Servern. Wenn `webbridge` und `callbridge` sich auf demselben Server befinden, ist hierfür nur die Datei `logbundle.tar.gz` erforderlich.

Microsoft ADFS-Fehlercodes

Manchmal tritt ein Fehler für den SSO-Prozess auf, der zu einem Fehler für die IdP-Konfiguration oder deren Kommunikation mit dem IdP führen kann. Bei Verwendung von ADFS wäre es ideal, den nächsten Link zu überprüfen, um den erkannten Fehler zu bestätigen und entsprechende

Korrekturmaßnahmen zu ergreifen:

[Microsoft-Statuscodes](#)

Ein Beispiel hierfür ist:

```
client_backend: FEHLER : SamlManager : SAML Authentifizierungsanfrage _e135ca12-4b87-4443-abe1-30d396590d58 fehlgeschlagen mit Grund:  
urn:oasis:names:tc:SAML:2.0:status:Responder
```

Dieser Fehler weist darauf hin, dass der Fehler gemäß der vorherigen Dokumentation auf den IdP oder ADFS zurückzuführen ist und daher vom ADFS-Administrator behandelt werden muss, um behoben zu werden.

Fehler beim Abrufen der Authentifizierungs-ID.

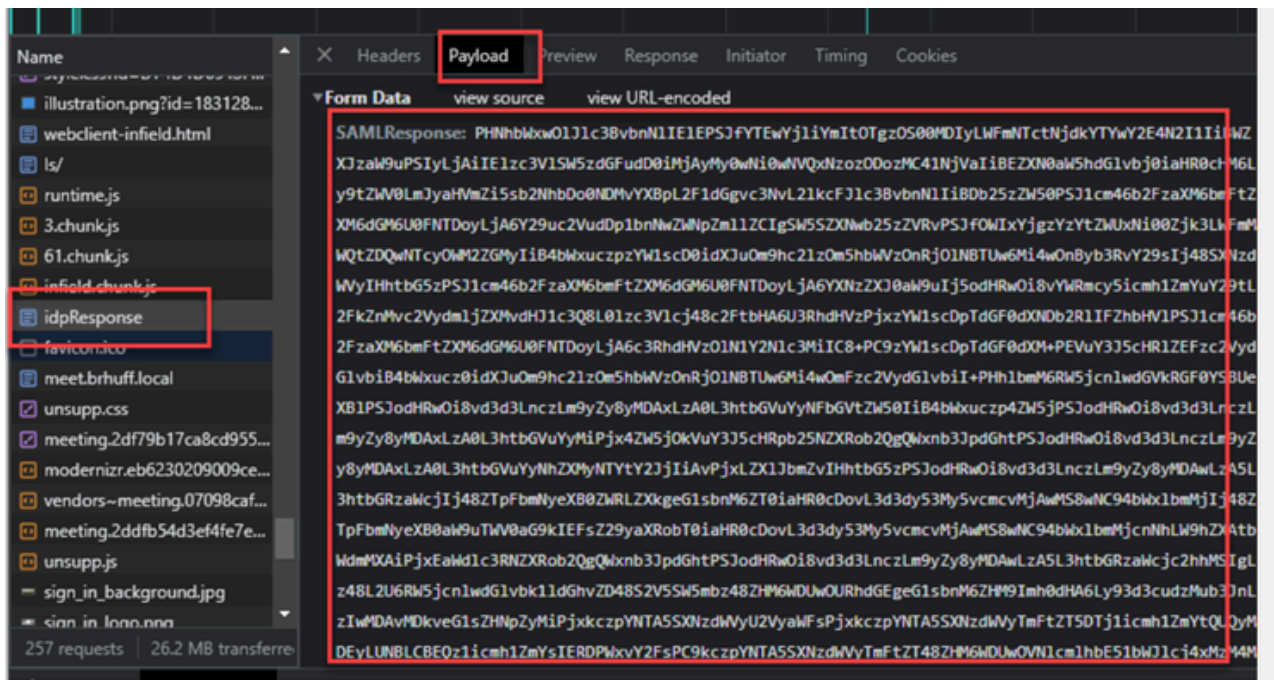
Es kann Fälle geben, in denen die Webbridge beim Austausch der SAMLResponse von der IdP diese Fehlermeldung in den Protokollen anzeigen kann, wobei die Anmeldung über SSO fehlgeschlagen ist:

```
client_backend: INFO : SamlManager : [57dff9e3-862e-4002-b4fa-683e4aa6922c] Fehler  
beim Abrufen einer authenticationId.
```

Dies weist darauf hin, dass Webbridge3 beim Überprüfen der SAMLResponse-Daten, die während des Authentifizierungsaustauschs von IdP zurückgegeben wurden, in der Antwort kein gültiges übereinstimmendes Attribut im Vergleich zu seiner config.json für authenticationId gefunden hat.

Wenn die Kommunikation nicht mit dem Vorzeichen und den privaten Schlüsseln verschlüsselt wird, kann die SAML-Antwort aus dem Developer Tools Network Logging über einen Webbrowser extrahiert und mit base64 decodiert werden. Wenn die Antwort verschlüsselt ist, können Sie die entschlüsselte SAML-Antwort von der IdP-Seite anfordern.

Suchen Sie in der Netzwerkprotokollierungsausgabe der Entwicklungstools, die auch als HAR-Daten bezeichnet wird, in der Namensspalte nach idpResponse, und wählen Sie Payload aus, um die SAML-Antwort anzuzeigen. Wie bereits erwähnt, kann dies mit dem Base64-Decoder decodiert werden.



Wenn Sie die SAMLResponse-Daten empfangen, überprüfen Sie den Abschnitt von `<AttributeStatement>`, um die zurückgesendeten Attributnamen zu finden. In diesem Abschnitt finden Sie die Anspruchsstypen, die konfiguriert und von der IdP gesendet wurden. Beispiele:

```

<AttributeStatement>
  <Attribute name="<URL für CommonName">
    <AttributeValue>testuser1</AttributeValue>
  </Attribute>
  <Attribute name="<URL für NameID">
    <AttributeValue>testuser1</AttributeValue>
  </Attribute>
  <Attribute name="uid">
    <AttributeValue>testuser1</AttributeValue>
  </Attribute>
</AttributeStatement>

```

Wenn Sie die vorherigen Namen überprüfen, können Sie den `<AttributeName>` unter dem Abschnitt `Attribute-Anweisung` überprüfen und jeden Wert mit dem vergleichen, der im `authenticationIdmapping`-Abschnitt der `SSO-config.json` festgelegt ist.

Im vorherigen Beispiel können Sie sehen, dass die Konfiguration für `authenticationIdMapping` NICHT exakt mit der übergebenen Adresse übereinstimmt und daher zum Fehlschlagen der Suche nach einer übereinstimmenden `authenticationId` führt:

```
authenticationIdMapping: http://example.com/claims/NameID
```

Zur Behebung dieses Problems gibt es zwei Möglichkeiten:

1. Die IdP-Anspruchsregel für `"Ausgehend"` kann aktualisiert werden, um einen übereinstimmenden Anspruch zu erhalten, der genau dem entspricht, was in

authenticationIdMapping der Datei config.json auf der Webbridge3 konfiguriert ist. (Anspruchsregel für IdP für <http://example.com/claims/NameID> hinzugefügt)
ODER

2. Die Datei "config.json" kann auf Webbridge3 aktualisiert werden, damit die 'authenticationIdMapping' genau mit der Konfiguration einer der auf der IDp konfigurierten Regeln für ausgehende Ansprüche übereinstimmt. (Dies ist 'authenticationIdMapping', die aktualisiert werden muss, damit sie mit einem der Attributnamen übereinstimmt, z. B. "uid", "<URL>/NameID" oder "<URL>/CommonName". Solange er (genau) mit dem erwarteten Wert übereinstimmt, der bei Übergabe auf der Callbridge-API konfiguriert wurde.

Keine Assertion in Validierung übergeben/abgeglichen

Manchmal zeigt die Webbridge beim Austausch der SAMLResponse von der IdP diesen Fehler an, der auf einen Fehler beim Abgleich der Assertion hinweist, und überspringt alle Assertionen, die nicht mit der Serverkonfiguration übereinstimmen:

```
client_backend: FEHLER : SamlManager : Keine Assertionen wurden validiert  
client_backend: INFO : SamlManager : Überspringen der Aussage ohne uns im erlaubten  
Publikum
```

Dieser Fehler weist darauf hin, dass die Webbridge beim Überprüfen der SAMLResponse aus dem IdP keine übereinstimmenden Assertionen gefunden und somit nicht übereinstimmende Fehler übersprungen hat, was letztendlich zu einer fehlerhaften SSO-Anmeldung geführt hat.

Um dieses Problem zu lokalisieren, ist es ideal, die SAMLResponse aus dem IdP zu überprüfen. Wenn die Kommunikation nicht mit dem Vorzeichen und den privaten Schlüsseln verschlüsselt wird, kann die SAML Response über einen Webbrowser aus der Developer Tools Network Logging extrahiert und mit base64 decodiert werden. Wenn die Antwort verschlüsselt ist, können Sie die entschlüsselte SAML-Antwort von der IdP-Seite anfordern.

Wenn Sie die SAMLResponse-Daten im Abschnitt <AudienceRestriction> der Antwort überprüfen, finden Sie alle Zielgruppen, für die diese Antwort eingeschränkt ist:

```
<Bedingungen nicht vor=2021-03-30t19:35:37.071z NotOnOrAfter=2021-03-  
30t19:36:37.071z>  
<Zielgruppeneinschränkung>  
<Zielgruppe>https://cisco.example.com</Zielgruppe>  
</AudienceRestriction>  
</Bedingungen>
```

Verwenden Sie den Wert im Abschnitt <Audience> (<https://cisco.example.com>), um ihn mit der ssoServiceProviderAddress in der config.json der Webbridge-Konfiguration zu vergleichen und zu überprüfen, ob er exakt übereinstimmt. In diesem Beispiel sehen Sie, dass der Grund für den Fehler darin besteht, dass die Zielgruppe NICHT mit der Adresse des Service Providers in der

Konfiguration übereinstimmt, da Folgendes angehängt ist:443:

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

Dies erfordert eine genaue Übereinstimmung zwischen diesen beiden, um einen solchen Fehler nicht zu verursachen. Für dieses Beispiel wäre die Korrektur auf eine der beiden folgenden Methoden:

1. Das :443 könnte aus der Adresse im ssoServiceProviderAddress-Abschnitt der config.json entfernt werden, sodass es mit dem Zielgruppenfeld übereinstimmt, das in der SAMLResponse von der IdP bereitgestellt wird.

ODER

2. Die Metadaten ODER vertrauende Vertrauenspartei für Webbridge3 in der IdP kann aktualisiert werden, um :443 an die URL anzuhängen. (Wenn die Metadaten aktualisiert werden, muss sie erneut als vertrauende Vertrauenspartei in das ADFS importiert werden. Wenn Sie die vertrauende Partei jedoch direkt vom IdP-Assistenten ändern, muss sie nicht erneut importiert werden.)

Anmeldung fehlgeschlagen auf Web-App:



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

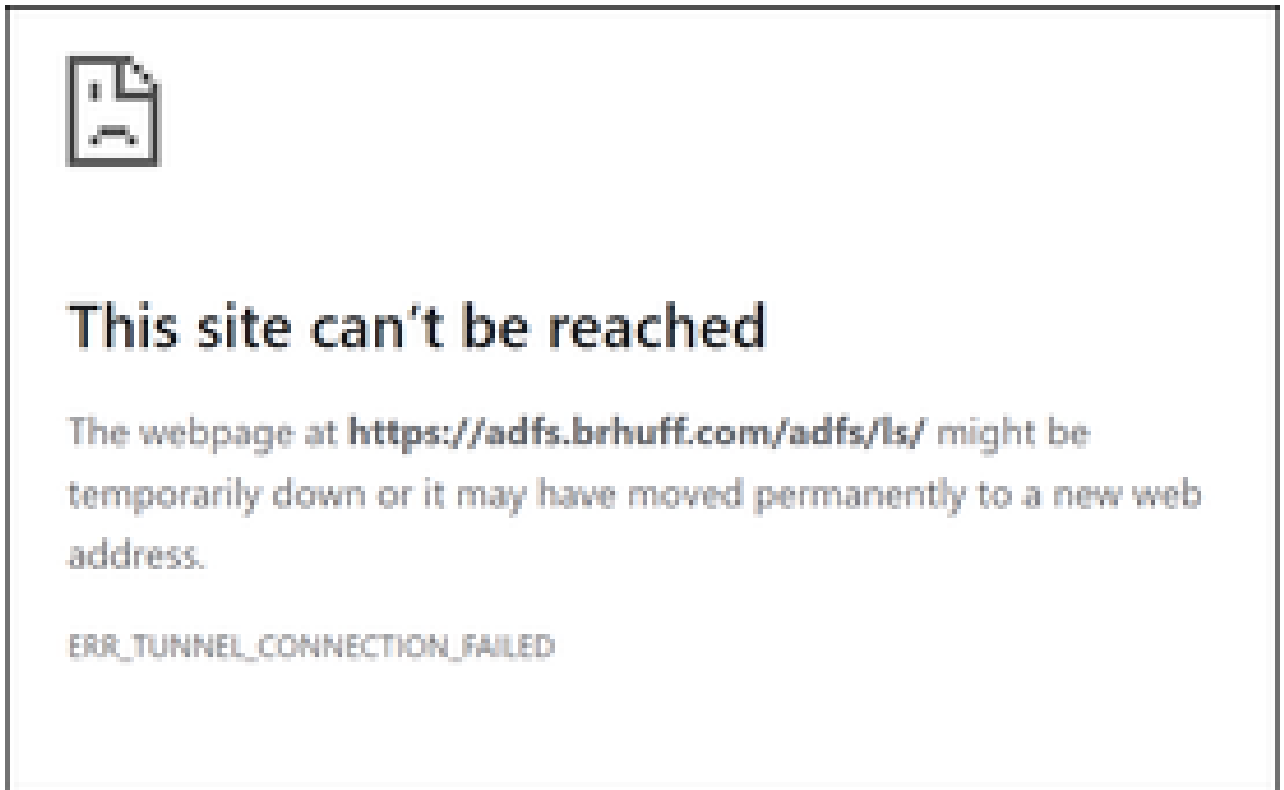
Sign in

 Sign in failed

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



, überprüft webbridge, ob die verwendete Domäne mit einer Domäne in der Datei config.json übereinstimmt, sendet dann die SAML-Informationen an den Client und teilt dem Client mit, wo er sich zur Authentifizierung anmelden muss. Der Client versucht, eine Verbindung mit dem IdP herzustellen, der sich im SAML-Token befindet. Im Beispiel unten zeigt der Browser diese Seite, da er den ADFS-Server nicht erreichen kann.



Fehler im Client-Browser

CMS Webbridge-Ablaufverfolgungen (wobei ?trace=true verwendet wird)

19. März 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamIManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Übereinstimmendes SSO sso_202 4.zip in SAML-Tokenanforderung

19. März 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamIManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Suche nach SSO in SAML Token de Anforderung

19. März 10:47:07.930 user.info cmscb3-1 client_backend: INFO : SamIManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAML-Token erfolgreich generiert

Szenario 2:

Der Benutzer hat versucht, sich über eine Domäne anzumelden, die sich nicht in der SSO-ZIP-Datei auf der Webbridge-Anmeldeseite befindet. Der Client sendet eine tokenRequest mit einer Nutzlast des vom Benutzer eingegebenen Benutzernamens. Webbridge stoppt den Anmeldeversuch sofort.

CMS Webbridge-Ablaufverfolgungen (wobei ?trace=true verwendet wird)

18. März 14:54:52.698 user.err cmscb3-1 client_backend: FEHLER : SamlManager : Ungültiger SSO-Anmeldeversuch

18.03.14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SSO in SAML-Tokenanforderung nicht gefunden

18. März 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Suche nach SSO in SAML-Tokenanforderung

Szenario 3:

Der Benutzer hat den richtigen Benutzernamen eingegeben und erhält die Anmeldeseite für SSO. Der Benutzer gibt auch hier den korrekten Benutzernamen und das korrekte Kennwort ein, erhält jedoch weiterhin die Anmeldung fehlgeschlagen

CMS Webbridge-Ablaufverfolgungen (wobei ?trace=true verwendet wird)

19. März 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Übereinstimmende SSO sso_2024.zip in SAML-Token-Anfrage

19. März 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Suche nach SSO in SAML IDP Response

19.03.16 16:39:17.720 user.err cmscb3-1 client_backend: ERROR : SamlManager : No authenticationId mapped element found in signed SAML Assertions

19. März 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Fehler beim Abrufen einer authenticationID

Ursache für Szenario 3 war die Anspruchsregel in der IdP, die einen Anspruchstyp verwendete, der nicht mit der authenticationIdMapping in der config.json-Datei übereinstimmt, die in der SSO-ZIP-Datei verwendet wurde, die auf webbridge hochgeladen wurde. Webbridge prüft die SAML-Antwort und erwartet, dass der Attributname mit der Konfiguration in der Datei config.json übereinstimmt.

Edit Rule - Webbridge3

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)
▶	E-Mail-Addresses	E-Mail Address
•		

Anspruchsregel in ADFS

```

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

```

config.json-Beispiel

Benutzername wird nicht erkannt

Szenario 1:

Der Benutzer hat sich mit einem falschen Benutzernamen angemeldet (die Domäne stimmt mit der ZIP-Datei für die SSO-Funktion überein, die auf webbridge3 hochgeladen wurde, aber der Benutzer ist nicht vorhanden).



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 stimmt nicht mit dem konfigurierten LDAP-Attribut überein, das für die Anspruchsregel in ADFS verwendet wird. Die Zeile unter "Successfully received authenticationID:darmckin@brhuff.com" besagt, dass ADFS eine Anspruchsregel mit einem Attribut konfiguriert hat, das darmckin@brhuff.com aus Active Directory abrufen. Die AuthenticationID in CMS-API > Users zeigt jedoch an, dass Darmckin erwartet wird. Im CMS ldapMappings ist die AuthenticationID als \$sAMAccountName\$ konfiguriert, aber die Anspruchsregel in ADFS ist so konfiguriert, dass die E-Mail-Adressen gesendet werden, sodass dies nicht übereinstimmt.

So beheben Sie dieses Problem:

Führen Sie einen der folgenden Schritte aus:

1. Ändern Sie die Authentifizierungs-ID in der CMS-Ldapmapping, um sie mit der in der Claim-Regel für ADFS verwendeten ID in Einklang zu bringen, und führen Sie einen neuen Abgleich durch.
2. Ändern Sie das in der ADFS-Anspruchsregel verwendete LDAP-Attribut in das in der CMS-Ldapmapping konfigurierte Attribut.

Related objects: </api/v1/ldapMappings>

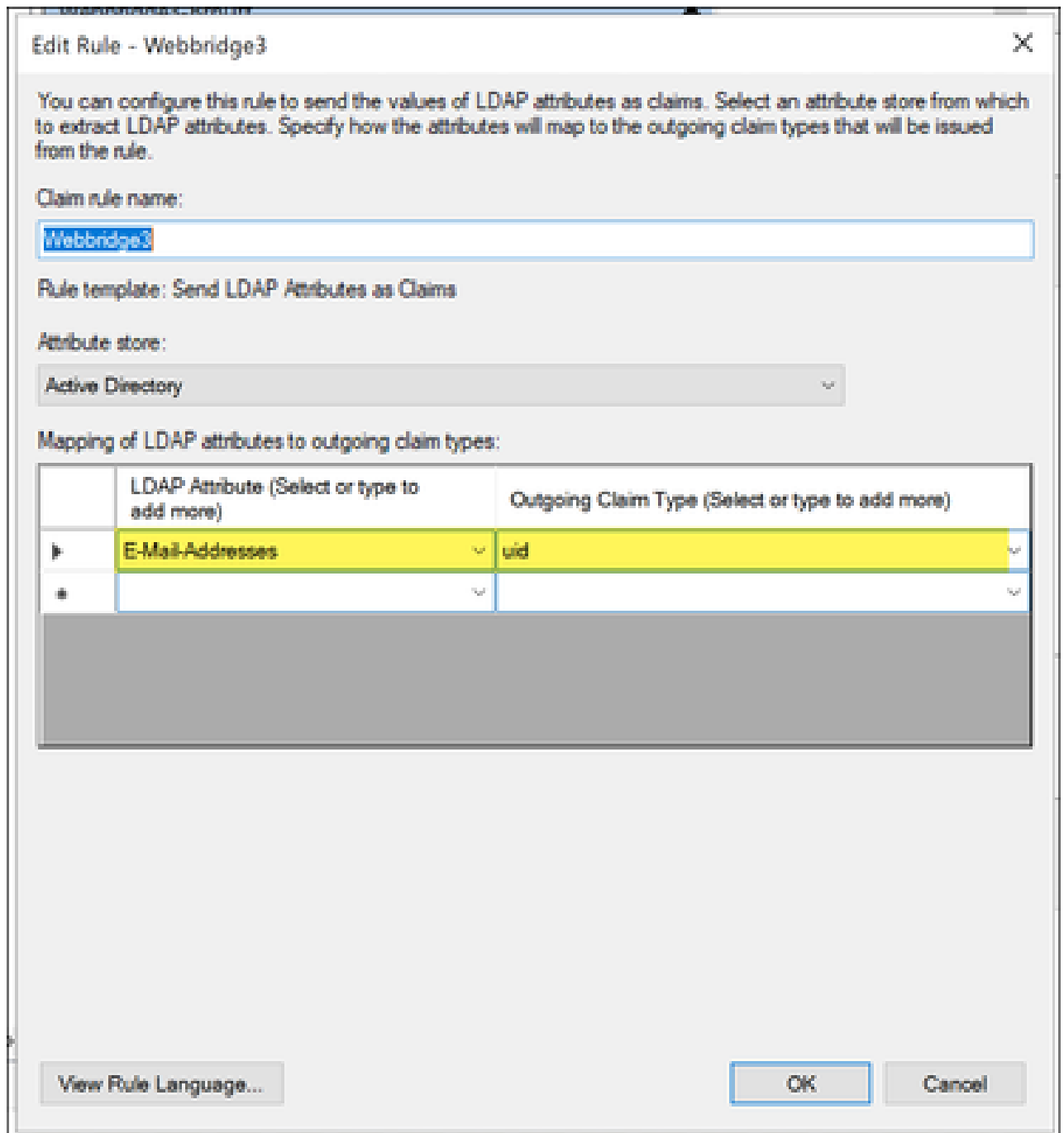
Table view XML view

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

API-Benutzerbeispiel



Anspruchsregel von ADFS

Webbridge-Protokoll mit Arbeitsprotokoll als Beispiel. Beispiel generiert mit ?trace=true in der Join-URL:

18. März 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Übereinstimmender SSO sso_2024.zip in SAML-Tokenanforderung

18. März 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Suche nach SSO in SAML IDP-Antwort

18. März 14:24:01.101 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Erfolgreich erhaltene

AuthentifizierungID:darmckin@brhuff.com

18. März 14:24:01.102 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequestReceived for connection id=64004556-fak ea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5 (user=darmckin@brhuff.com)

18. März 14:24:01.130 user.info cmscb3-1 host:server: INFO : successful login request from darmckin@brhuff.com

18. März 14:24:01.130 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba], JWT-ID e2a860b ef-f4ef-4391-b5d5-9abdfa89ba0f

18. März 14:24:01.132 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] Authentifizierungsantwort senden (jwt length=106 4, connection=64004556-faea-479f-aabe-691e17783aa5)

18. März 14:24:01.13 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25 10.247 - - [18/Mar/2024:18:24:01 +0000] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "<https://ads.brhuff.com/>" http_user_agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, wie Gecko) Chrome/122.0.0.0 Safari/537.36" zu Upstream 192.0.2.2:9000: Upstream_response_time 0,038 request_time 0,039 msec 1710786241,133 Upstream_Response_Length 24 200

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.