

Configurazione e risoluzione dei problemi di SSO WebApp su CMS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Configurazione](#)

[Esempio di rete](#)

[Installazione e configurazione iniziale di ADFS](#)

[Mappa utenti CMS a provider di identità \(IdP\)](#)

[Crea XML metadati WebBridge per IdP](#)

[Importa metadati per Webbridge nel provider di identità \(IdP\)](#)

[Crea regole attestazione per il servizio Webbridge nel provider di identità](#)

[Crea file ZIP di archivio SSO per Webbridge:](#)

[Ottenerne e configurare idp_config.xml](#)

[Creare il file config.json con il relativo contenuto](#)

[Impostare sso_sign.key \(FACOLTATIVO\)](#)

[Impostare sso_encrypt.key \(FACOLTATIVO\)](#)

[Creazione del file ZIP SSO](#)

[Carica i file SSO Zip in Webbridge](#)

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

[Test dell'accesso SSO tramite WebApp](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi di base](#)

[Codici di errore di Microsoft ADFS](#)

[Impossibile ottenere authenticationID](#)

[Nessuna asserzione passata/associata nella convalida](#)

[Accesso non riuscito all'app Web:](#)

[Scenario 1:](#)

[Scenario 2:](#)

[Scenario 3:](#)

[Nome utente non riconosciuto](#)

[Scenario 1:](#)

[Scenario 2:](#)

[Esempio di log di Webbridge che mostra il log di lavoro. Esempio generato utilizzando ?trace=true nell'URL di join:](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi all'implementazione dell'app Web Cisco Meeting Server (CMS) Single Sign-On (SSO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CMS Callbridge versione 3.1 o successiva
- CMS Webbridge versione 3.1 o successiva
- Server Active Directory
- Identifica provider (IdP)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.


Introduzione

In CMS 3.1 e versioni successive è stata introdotta la possibilità per gli utenti di accedere utilizzando un SSO senza dover immettere la password ogni volta che l'utente accede, in quanto viene creata una singola sessione con il provider Identify.

Questa funzionalità utilizza il linguaggio SAML (Security Assertion Markup Language) versione 2.0 come meccanismo SSO.



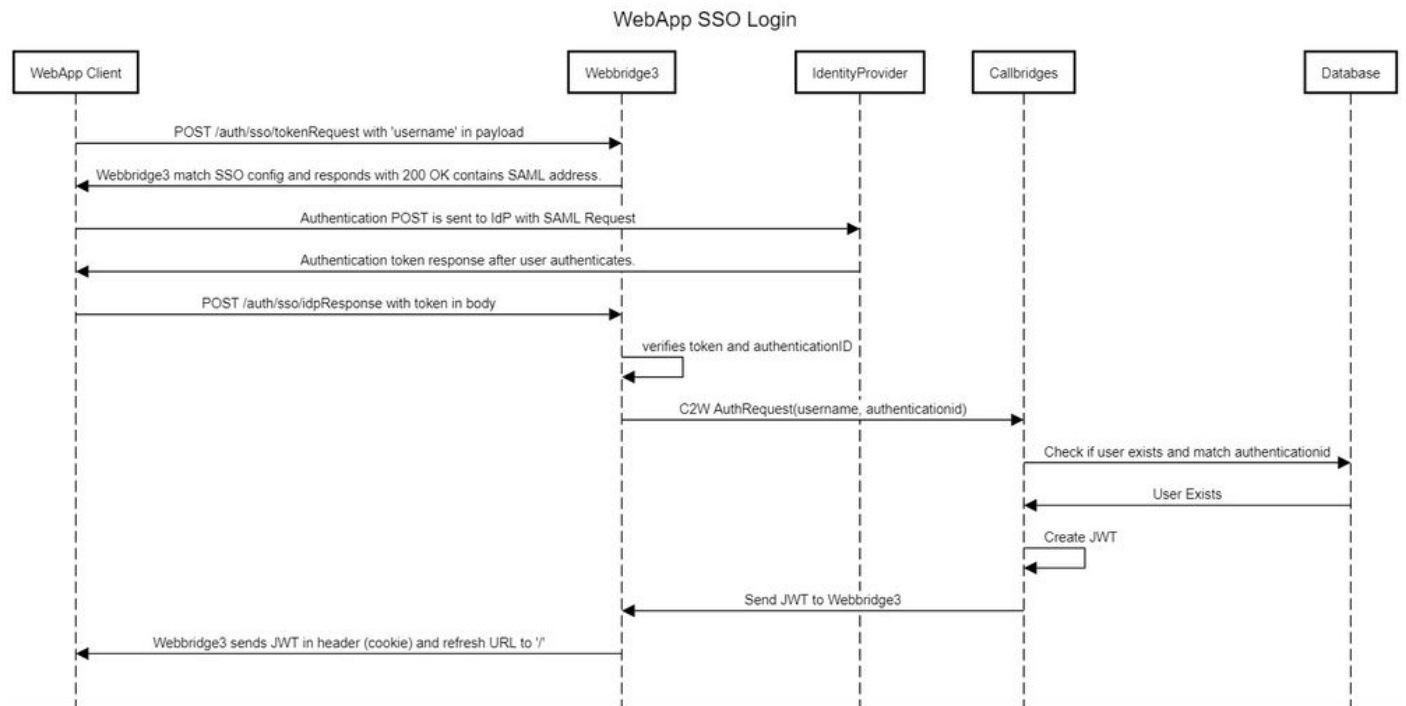
Nota: CMS supporta solo le associazioni HTTP-POST in SAML 2.0 e rifiuta qualsiasi

 associazione Identify Provider senza associazioni HTTP-POST disponibili.

 Nota: quando l'SSO è abilitato, l'autenticazione LDAP di base non è più possibile.

Configurazione

Esempio di rete



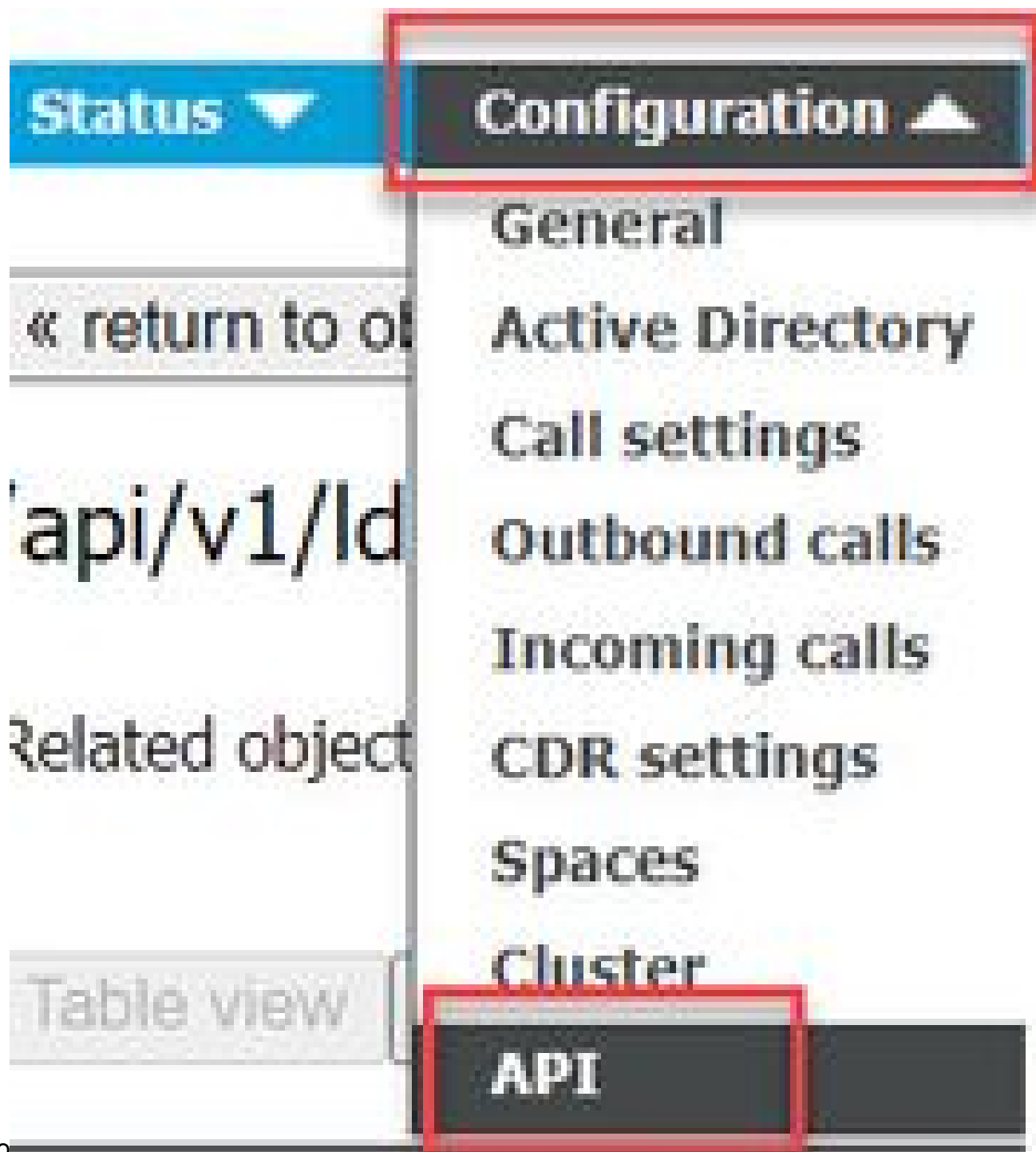
Installazione e configurazione iniziale di ADFS

In questo scenario di distribuzione viene utilizzato Microsoft Active Directory Federation Services (ADFS) come provider di identità (IdP). Si consiglia pertanto di installare ed eseguire ADFS (o IdP previsto) prima di questa configurazione.

Mappa utenti CMS a provider di identità (IdP)

Affinché gli utenti ottengano l'autenticazione valida, è necessario che siano mappati nell'API (Application Programming Interface) per un campo correlato fornito da IdP. L'opzione utilizzata per questa operazione è `authenticationIdMapping` in `IdapMapping` dell'API.

1. Passare a Configurazione > API sull'interfaccia GUI CMS Web Admin



2. Individuare il mapping LDAP esistente (o crearne uno nuovo) in `api/v1/ldapMappings/<GUID-of-Ldap-Mapping>`.

API objects

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

Filter (2 of 129 nodes)

/api/v1/ldapMappings ◀


◀ start ◀ prev 1 - 2 (of 2) next >

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

3. Nell'oggetto ldapMapping selezionato, aggiornare authenticationIdMapping all'attributo LDAP passato da IdP. Nell'esempio, l'opzione \$sAMAccountName viene utilizzata come attributo LDAP per la mappatura.

/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

 Nota: l'elemento authenticationIdMapping viene utilizzato dal callbridge/database per convalidare l'attestazione inviata dall'IdP in SAMLResponse e fornire all'utente un token Web JSON (JWT).

4. Eseguire una sincronizzazione LDAP sul ldapSource associato al ldapMapping modificato di recente:

Ad esempio:

/api/v1/ldapSyncs

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

5. Una volta completata la sincronizzazione LDAP, spostarsi nell'API CMS in Configurazione > api/v1/users e selezionare un utente importato e verificare che authenticationId sia compilato correttamente.

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

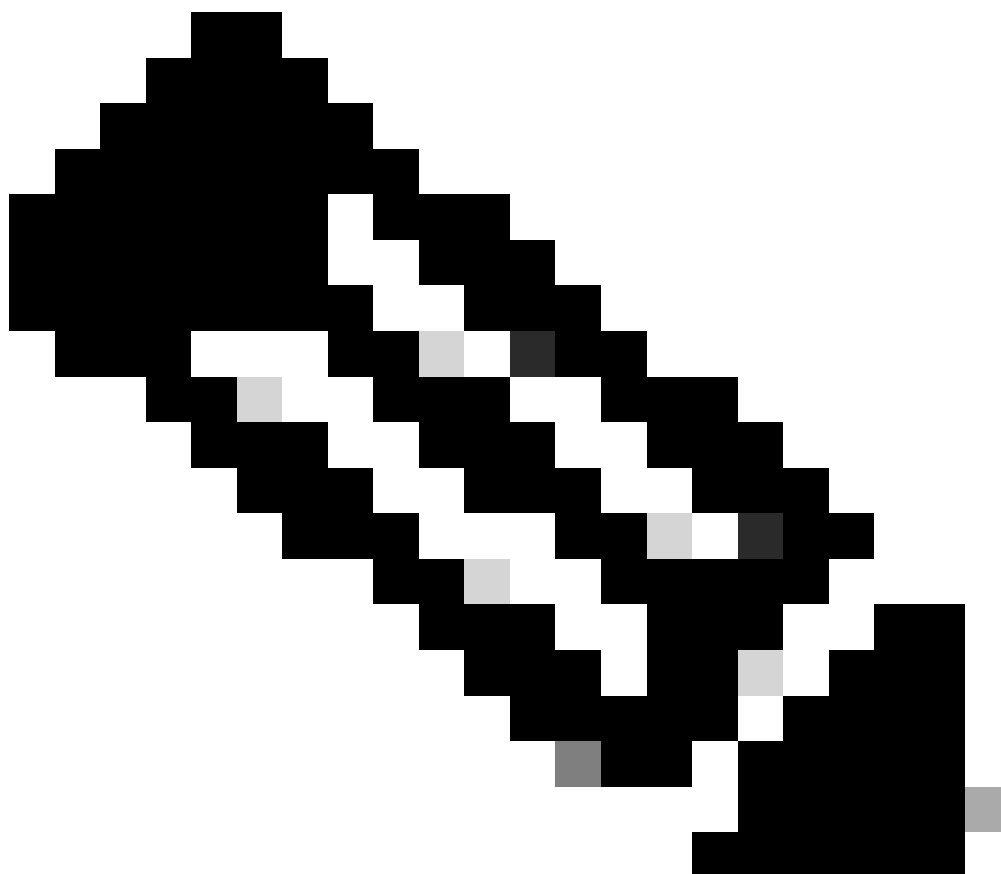
Crea XML metadati WebBridge per IdP

Microsoft ADFS consente di importare un file XML di metadati come componente attendibile per identificare il provider di servizi utilizzato. Esistono alcuni modi per creare il file XML dei metadati a tale scopo, tuttavia nel file devono essere presenti alcuni attributi:

Esempio di metadati di Webbridge con valori obbligatori:

```
<?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: indirizzo del server Webbridge3 (FQDN/Nome host) e porta associata raggiungibile dai browser per gli utenti.



Nota: se sono presenti più bridge Web che utilizzano un solo URL, questo deve essere un indirizzo di bilanciamento del carico.

2. Posizione: posizione in cui si trova il servizio HTTP-POST AssertionConsumerService per l'indirizzo di Webbridge. Questo è ciò che indica all'IdP dove reindirizzare un utente autenticato dopo l'accesso. Deve essere impostato sull'URL di idpResponse: <https://<FQDNbridge>:<porta>/api/auth/sso/idpResponse>. Ad esempio, <https://join.example.com:443/api/auth/sso/idpResponse>.
3. FACOLTATIVO - Chiave pubblica per la firma - Chiave pubblica (certificato) per la firma, utilizzata dall'IdP per verificare AuthRequest da Webbridge. DEVE corrispondere alla chiave privata 'sso_sign.key' nel bundle SSO caricato in Webbridge in modo che l'IdP possa utilizzare la chiave pubblica (certificato) per verificare la firma. È possibile utilizzare un certificato esistente della distribuzione. Aprire il certificato in un file di testo e copiare il contenuto nel file di metadati di Webbridge. Utilizzare la chiave corrispondente per il certificato utilizzato nel file sso_xxxx.zip come file sso_sign.key.

4. FACOLTATIVO - Chiave pubblica per la crittografia - Chiave pubblica (certificato) utilizzata dal provider di identità per crittografare le informazioni SAML inviate a Webbridge. DEVE corrispondere alla chiave privata 'sso_encrypt.key' nel bundle SSO caricato in Webbridge, in modo che Webbridge possa decrittografare i dati restituiti da IdP. È possibile utilizzare un certificato esistente della distribuzione. Aprire il certificato in un file di testo e copiare il contenuto nel file di metadati di Webbridge. Utilizzare la chiave corrispondente per il certificato utilizzato nel file sso_xxxx.zip come file sso_encrypt.key.

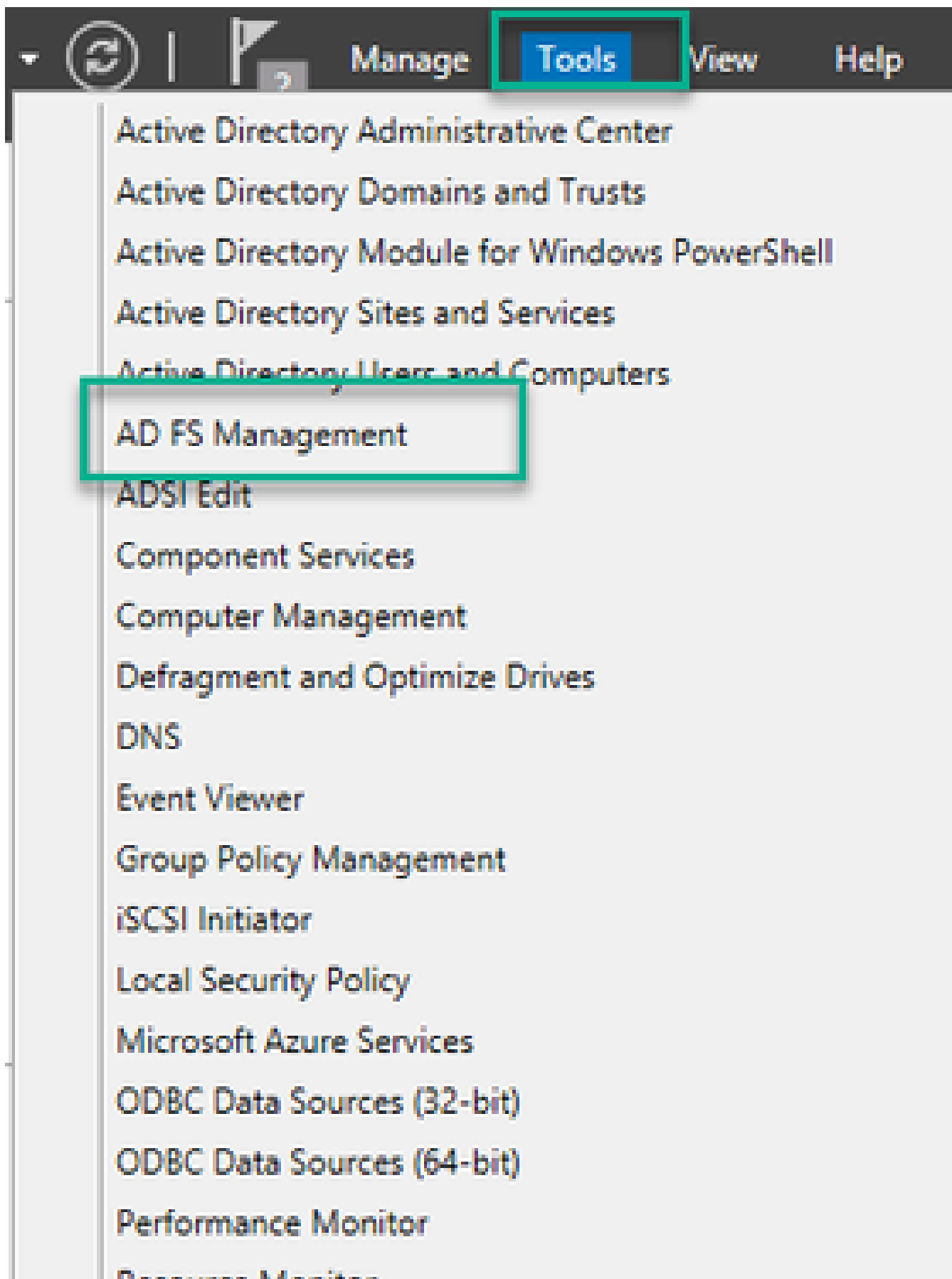
Esempio di metadati di Webbridge da importare in IdP con dati di chiave pubblica (certificato) facoltativi:

```
<?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...
- </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...
- </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>
```

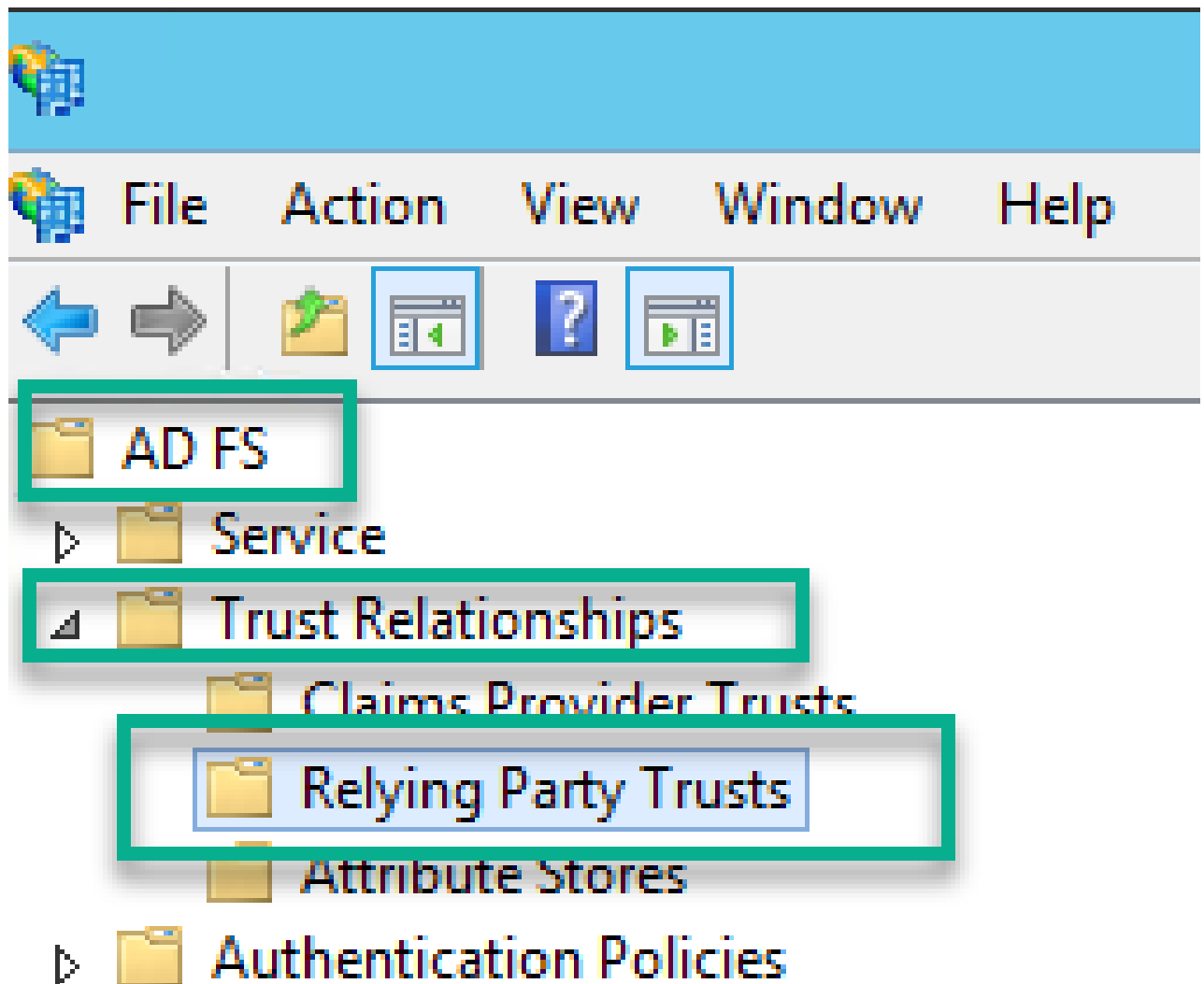
Importa metadati per Webbridge nel provider di identità (IdP)

Dopo aver creato il file XML dei metadati con gli attributi appropriati, è possibile importarlo nel server Microsoft ADFS per creare un componente attendibile.

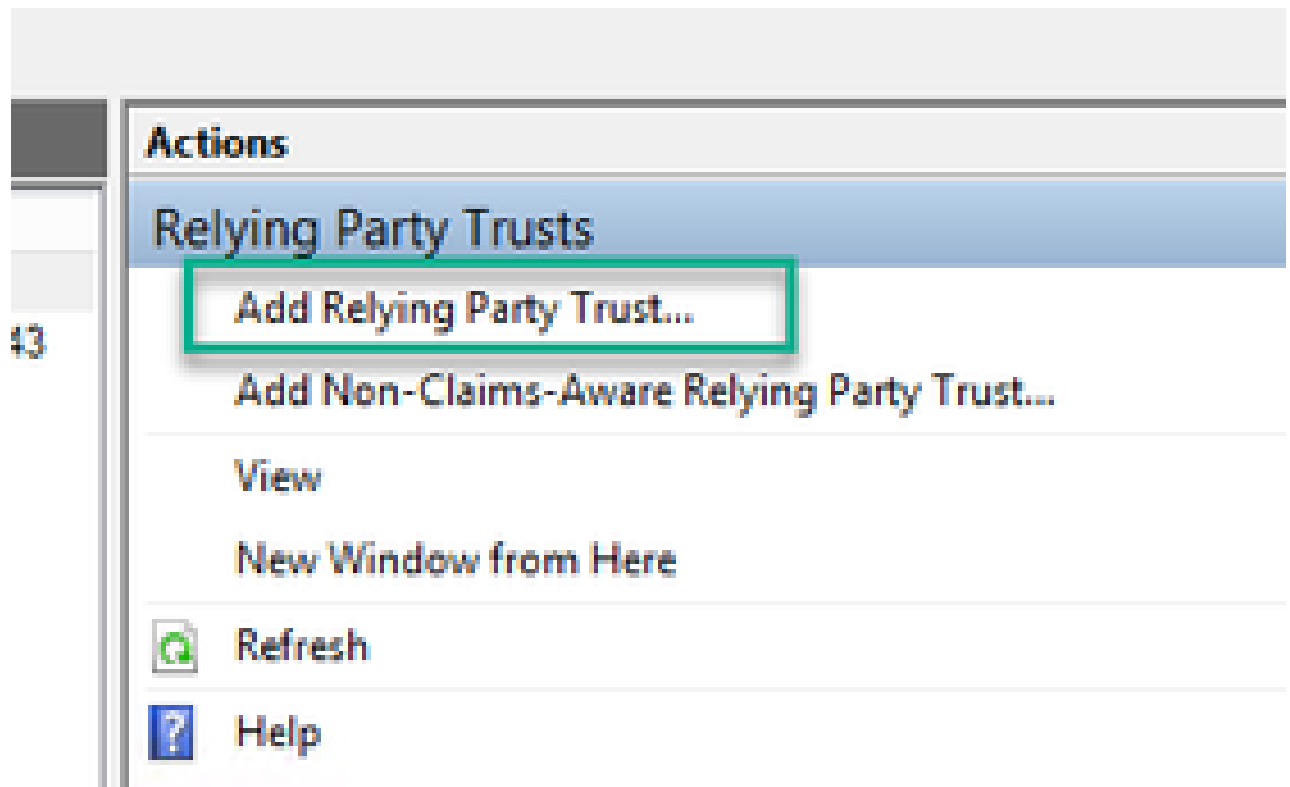
1. Desktop remoto nel server Windows che ospita i servizi ADFS
2. Aprire la console di gestione di AD FS, a cui è in genere possibile accedere tramite Server Manager.



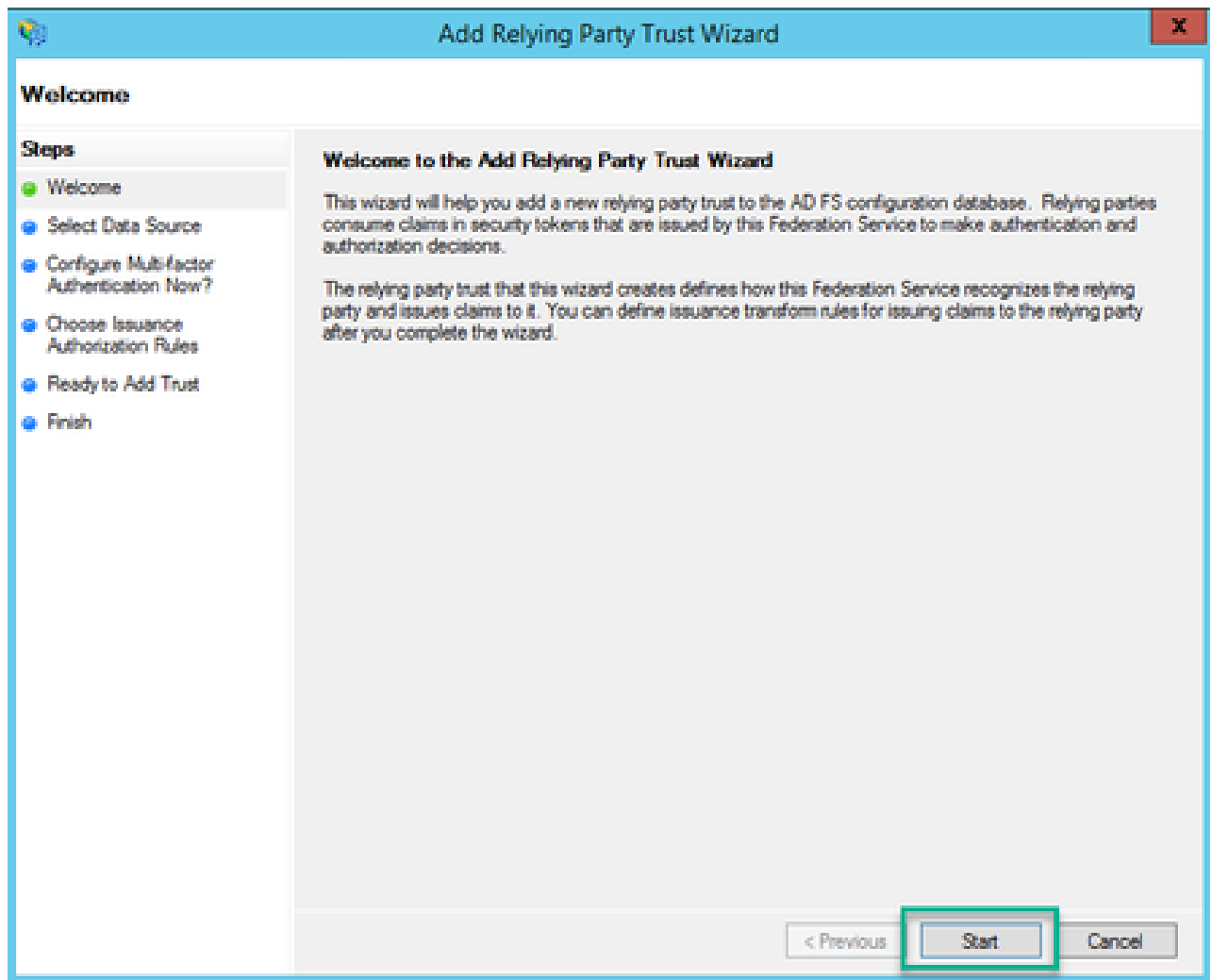
3. Nella console Gestione ADFS, passare ad ADFS > Relazioni di trust > Attendibilità componente nel riquadro di sinistra.



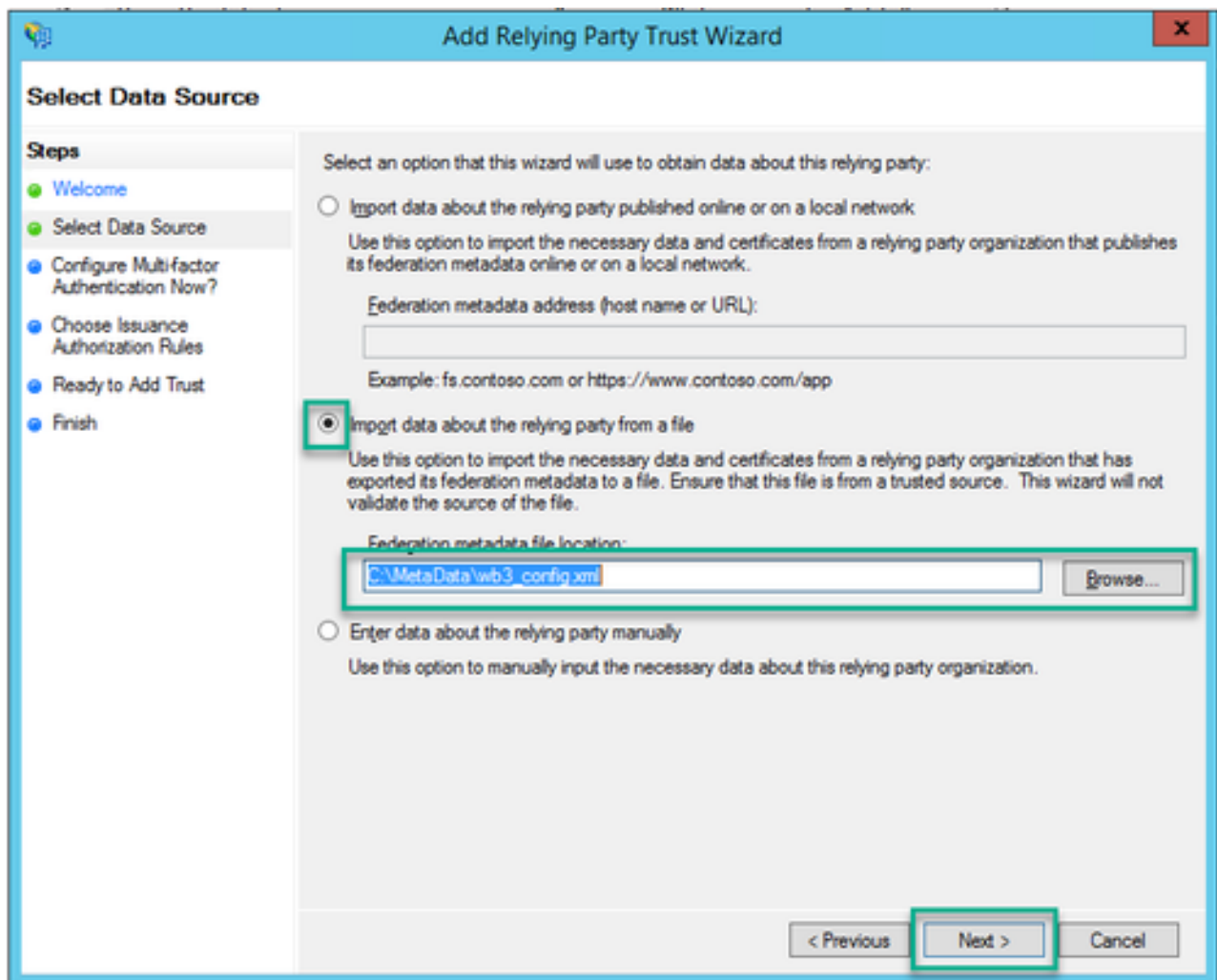
4. Nel riquadro di destra della console di gestione di ADFS, selezionare l'opzione Aggiungi attendibilità componente...



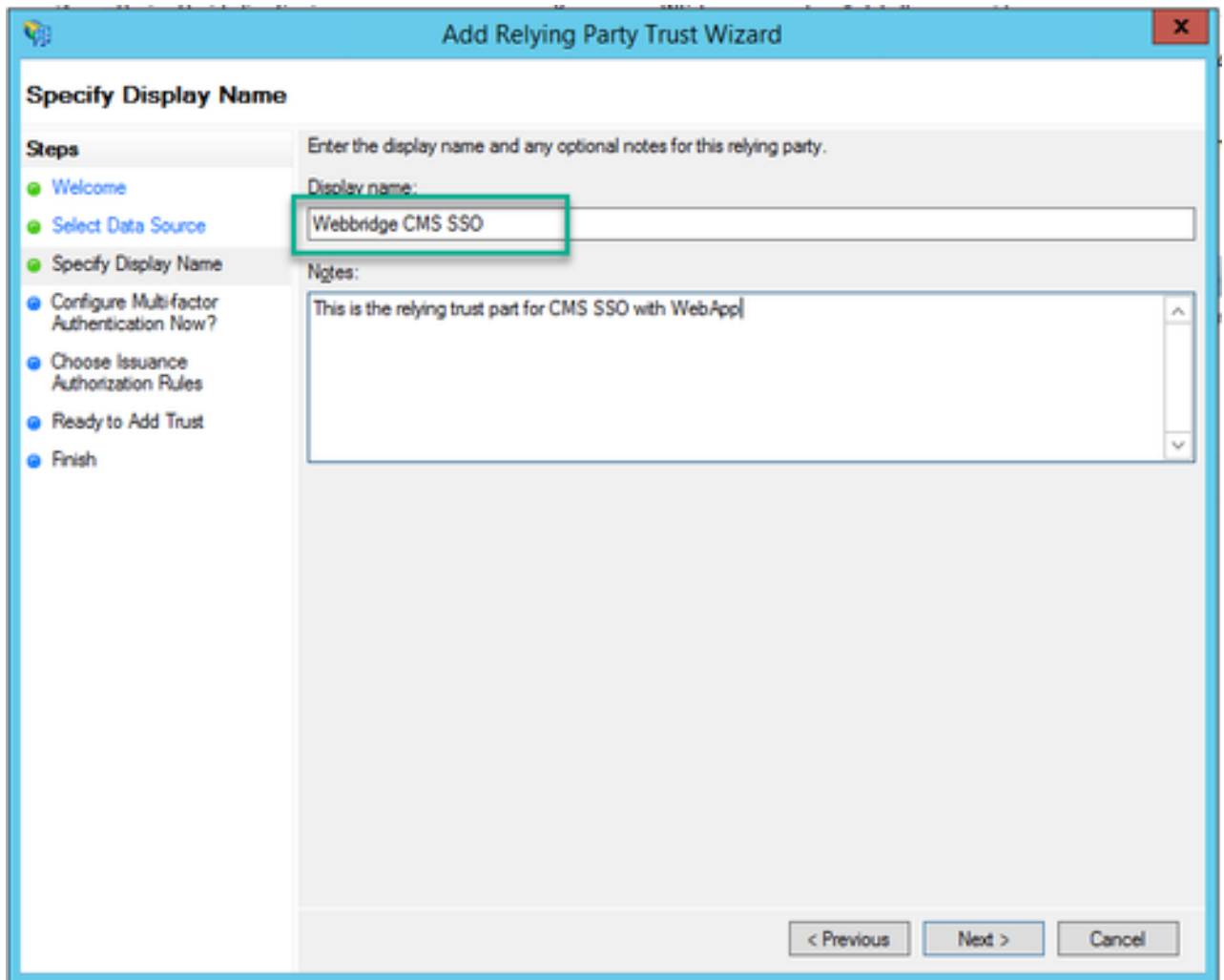
5. Dopo aver effettuato questa selezione, verrà aperta l'Aggiunta guidata attendibilità componente. Selezionare l'opzione Start.



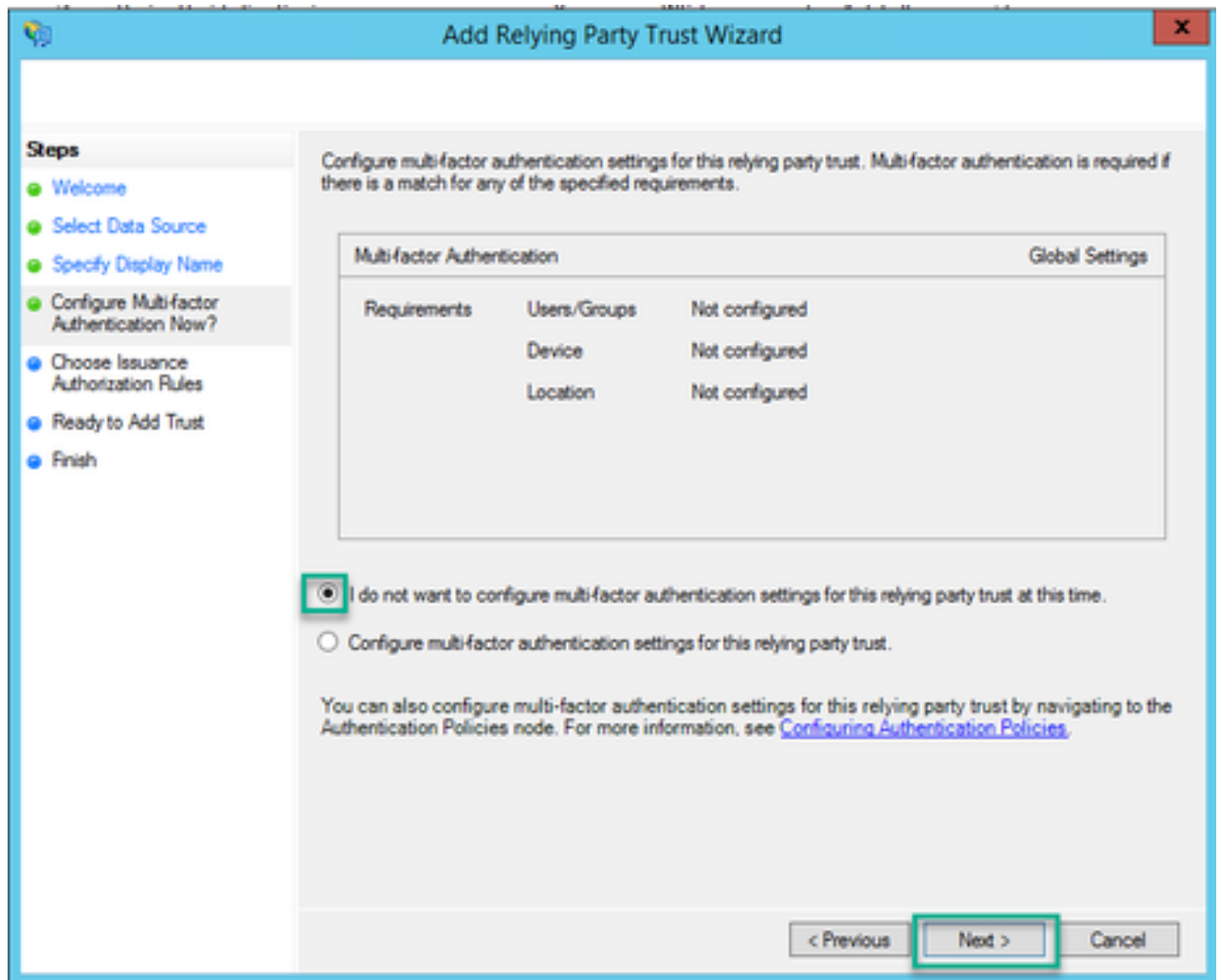
6. Nella pagina Seleziona origine dati, selezionare il pulsante di scelta per Importare i dati sul componente da un file e selezionare Sfogliare e passare alla posizione del file metadati di Webbridge.



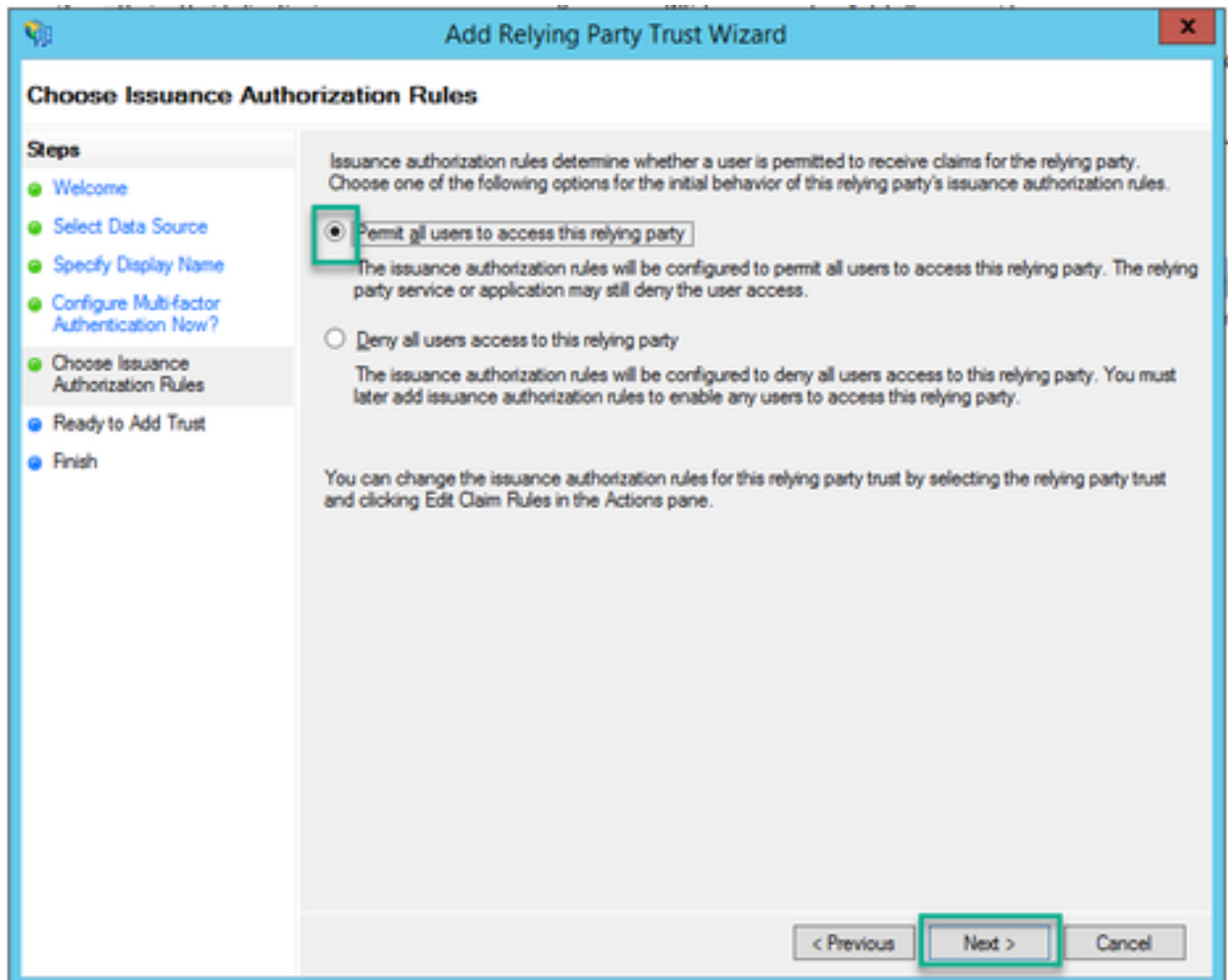
7. Nella pagina Specifica nome visualizzato, inserire un nome da visualizzare per l'entità in ADFS (il nome visualizzato non è uno scopo server per la comunicazione ADFS ed è puramente informativo).



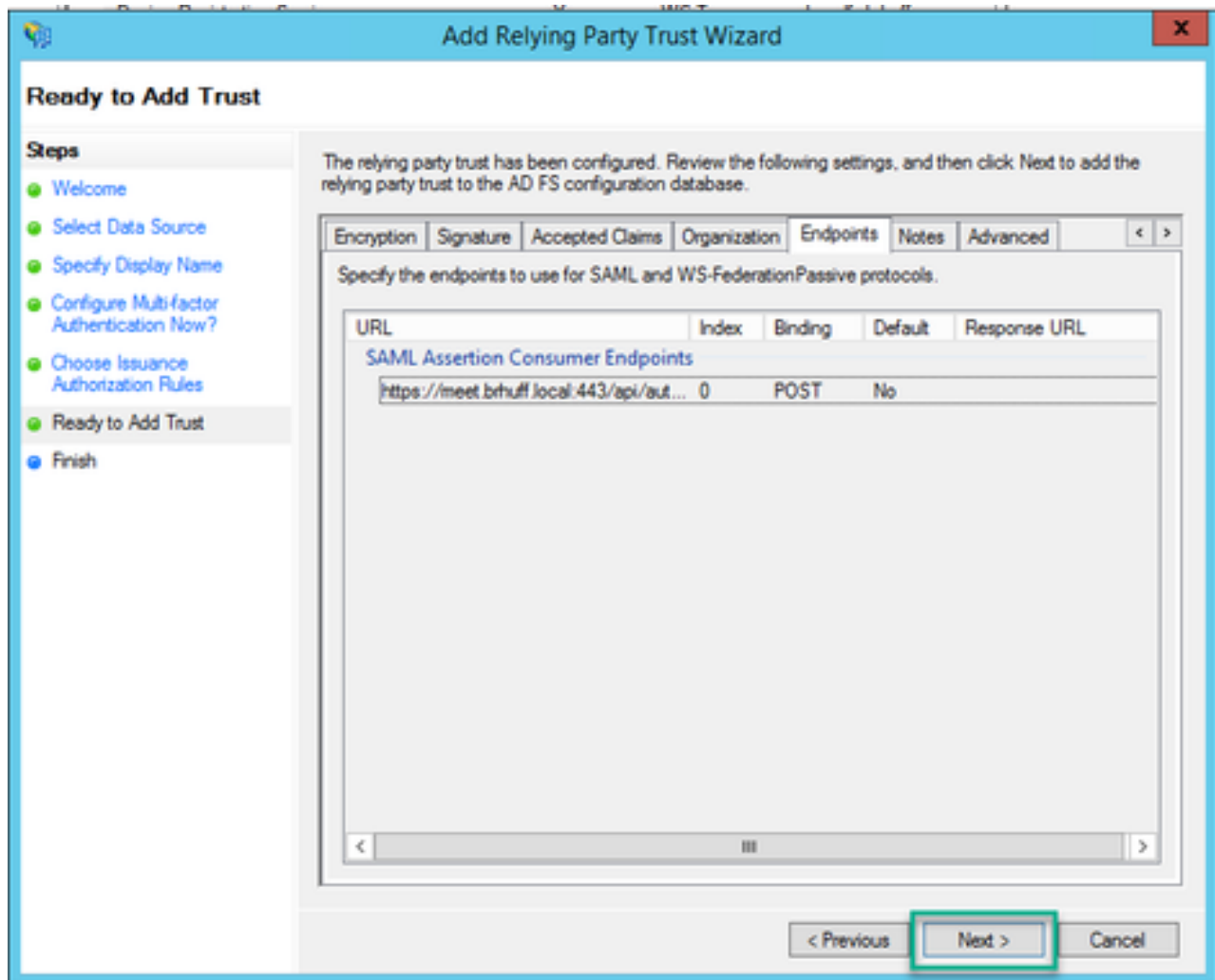
8. Nella pagina Configura Multi-Factor Authentication Now?, lasciare l'impostazione predefinita e selezionare Avanti.



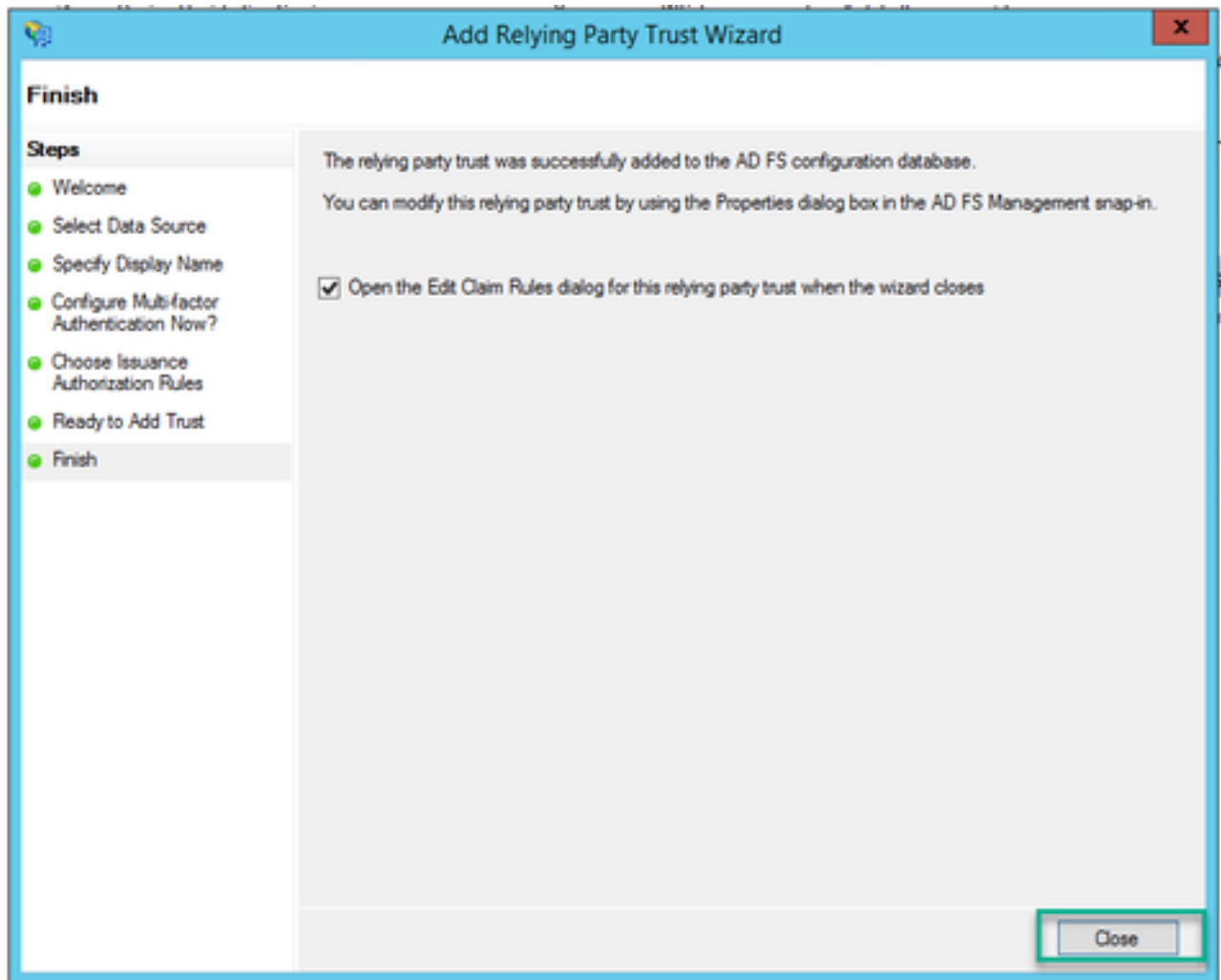
9. Nella pagina Scegli regole di autorizzazione rilascio, lasciare selezionata l'opzione selezionata per Consenti a tutti gli utenti di accedere a questo componente.



10. Nella pagina Pronto per aggiungere trust, i dettagli importati del relying trust party per Webbridge possono essere rivisti tramite le schede. Per i dettagli dell'URL del provider di servizi Webbridge, vedere Identifier and Endpoints.



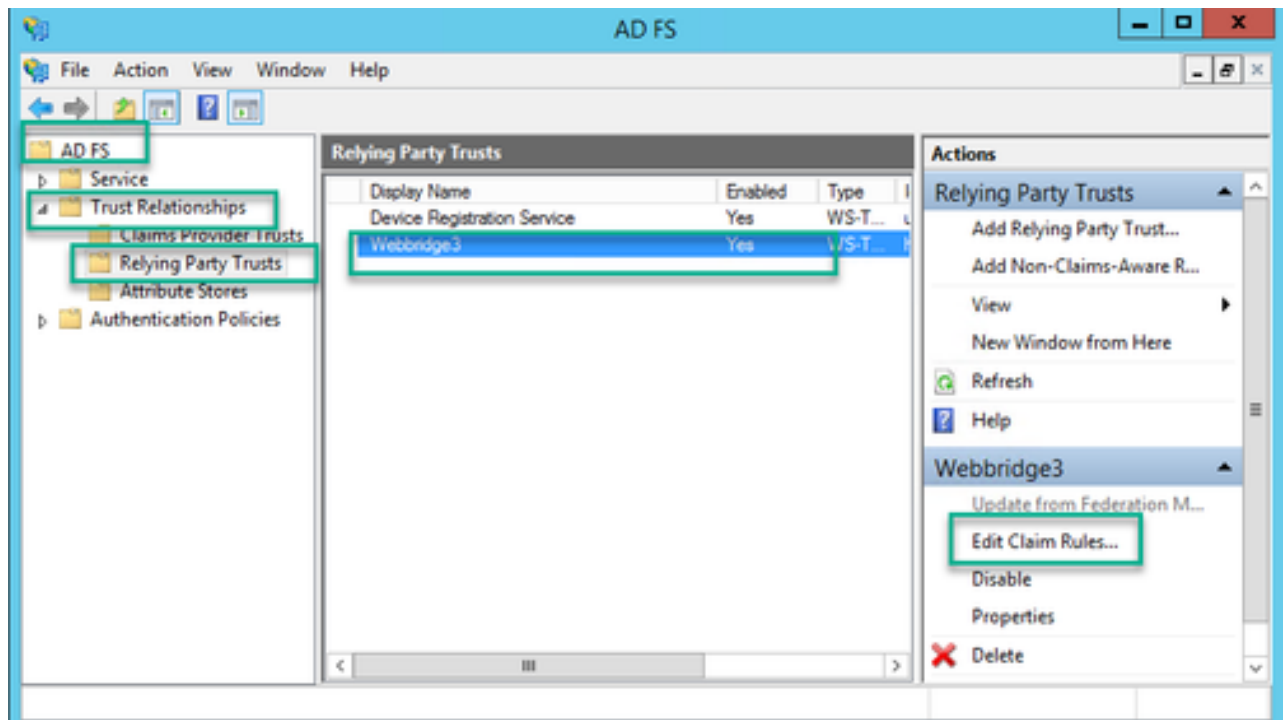
11. Nella pagina Fine, selezionare l'opzione Chiudi per chiudere la procedura guidata e continuare con la modifica delle regole attestazione.



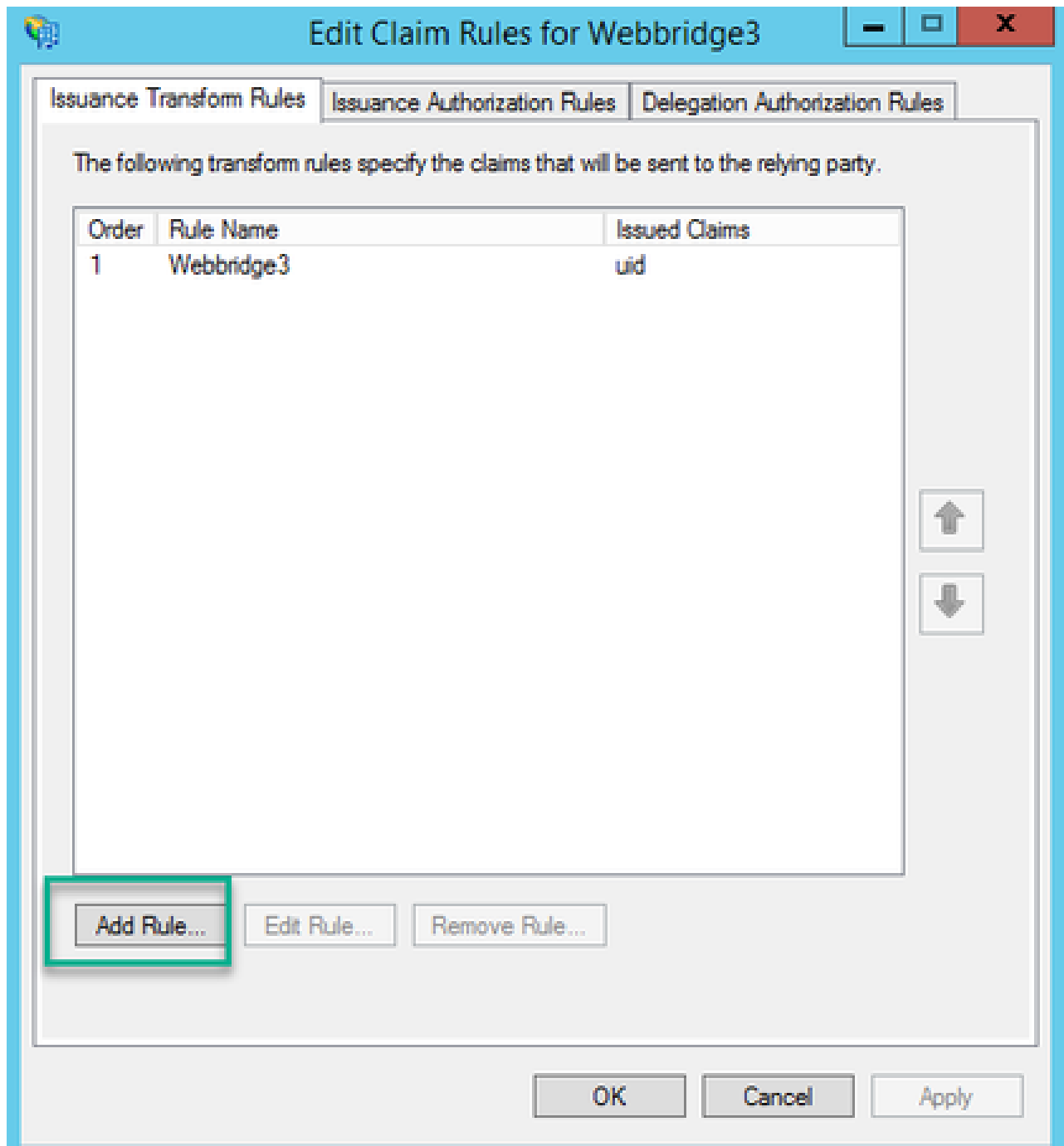
Crea regole attestazione per il servizio Webbridge nel provider di identità

Ora che l'attendibilità della relying party è stata creata per il webbridge, è possibile creare regole attestazione per abbinare attributi LDAP specifici a tipi attestazione in uscita da fornire al webbridge nella risposta SAML.

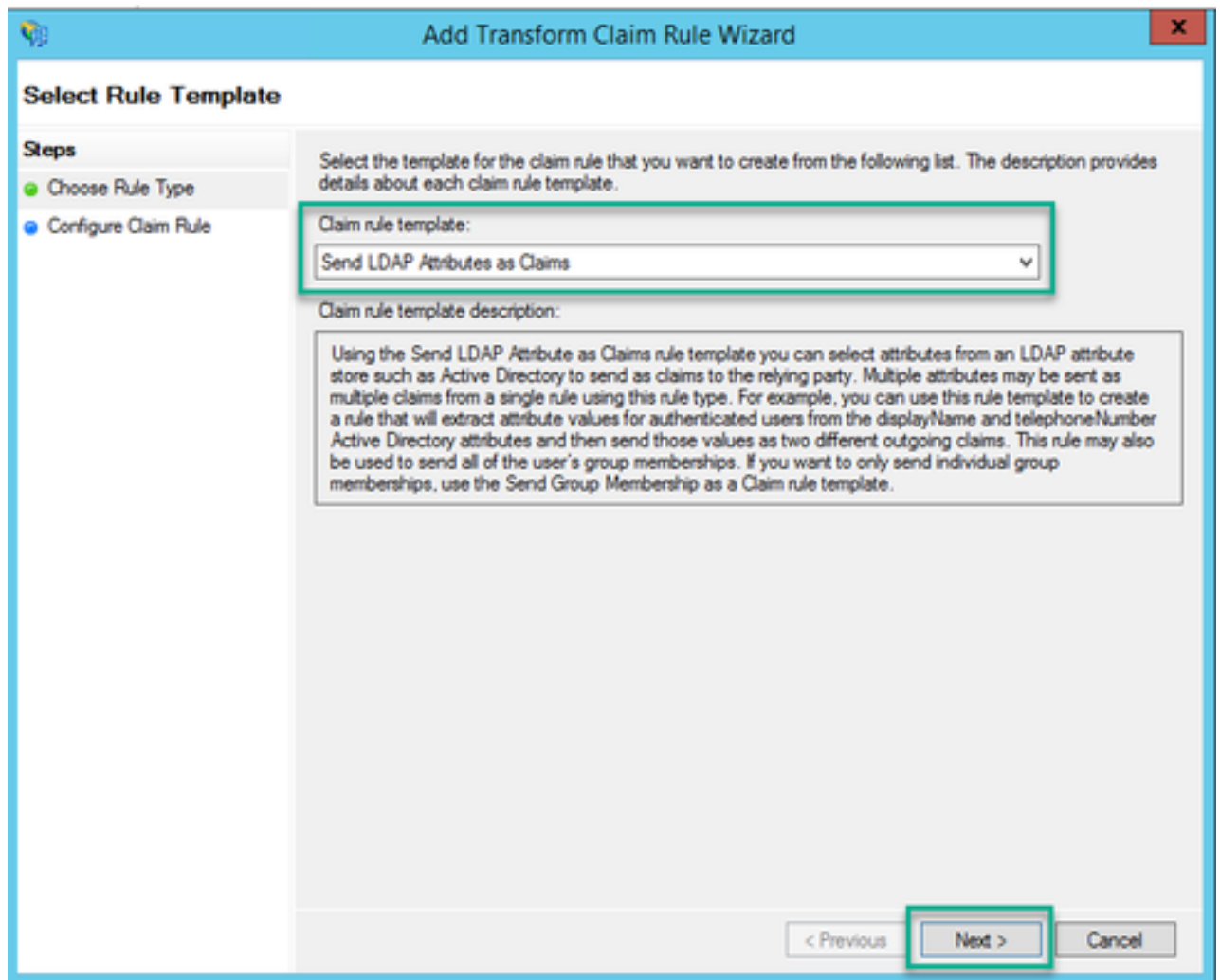
1. Nella console Gestione ADFS, evidenziare l'attendibilità componente per Webbridge e selezionare Modifica regole attestazione nel riquadro di destra.



2. Nella pagina Modifica regole attestazione per <DisplayName>, selezionare Aggiungi regola....



3. Nella pagina Aggiunta guidata regola attestazione di trasformazione, selezionare Invia attributi LDAP come attestazioni per l'opzione del modello di regola attestazione e selezionare Avanti.



4. Nella pagina Configura regola attestazione, configurare la regola attestazione per l'attendibilità componente con i seguenti valori:

1. Nome regola attestazione = deve essere un nome assegnato alla regola in ADFS (solo per riferimento regola)
2. Archivio attributi = Active Directory
3. Attributo LDAP = Deve corrispondere all'authenticationIdMapping nell'API Callbridge, ad esempio \$sAMAccountName\$.
4. Tipo attestazione in uscita = Deve corrispondere all'authenticationIdMapping nel file config.json di SSO di Webbridge. (ad esempio, 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

Crea file ZIP di archivio SSO per Webbridge:

Questa configurazione è quella a cui fa riferimento il webbridge per convalidare la configurazione SSO per i domini supportati, il mapping dell'autenticazione e così via. È necessario tenere in considerazione le seguenti regole per questa parte della configurazione:

- Il file ZIP DEVE iniziare con sso_prefisso al nome del file (ad esempio, sso_cmstest.zip).
- Una volta caricato il file, Webbridge disabilita l'autenticazione di base e può essere utilizzato SOLO SSO per il Webbridge in cui è stato caricato.
- Se vengono utilizzati più provider di identità, è necessario caricare un file ZIP separato con

uno schema di denominazione diverso (ancora preceduto da sso_).

- Quando si crea il file zip, accertarsi di evidenziare e comprimere il contenuto del file, di non inserire i file necessari in una cartella e di comprimere tale cartella.

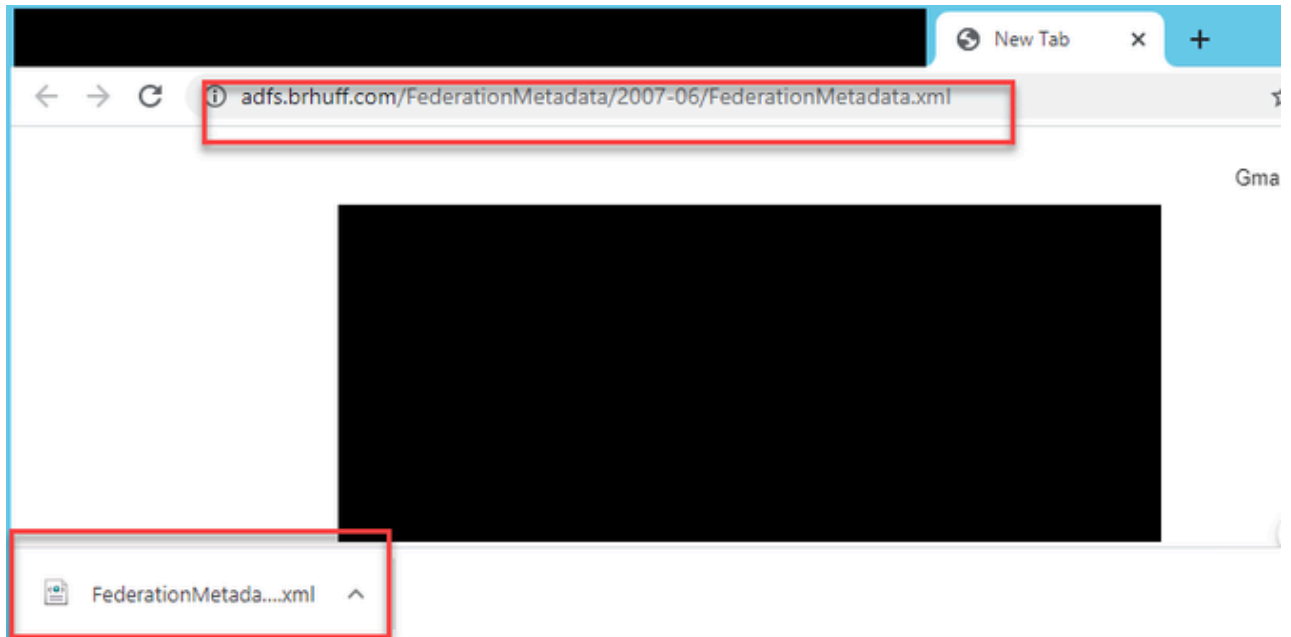
Il contenuto del file zip è costituito da 2 a 4 file, a seconda che si utilizzi o meno la crittografia.

Nome file	Descrizione	Obbligatorio?
idp_config.xml	Si tratta del file dei metadati che può essere raccolto dal provider di identità. In ADFS è possibile trovare questa cartella all'indirizzo <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml .	Sì
config.json	Si tratta del file JSON in cui Webbridge utilizza per convalidare i domini supportati, mapping di autenticazione per SSO.	Sì
sso_sign.key	Questa è la chiave privata per la chiave di firma pubblica configurata nel provider di identità. Necessario solo per la protezione dei dati firmati	NO
sso_encrypt.key	Questa è la chiave privata per la chiave di crittografia pubblica configurata nel provider di identità. Necessario solo per la protezione dei dati crittografati	NO

Ottenere e configurare idp_config.xml

1. Sul server ADFS (o in un percorso che ha accesso ad ADFS), aprire un browser Web.

2. Nel browser Web, immettere l'URL: <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml> (è possibile utilizzare anche localhost anziché il nome FQDN se si è connessi al server ADFS in locale). In questo modo viene scaricato il file FederationMetadata.xml.



3. Copiare il file scaricato nella posizione in cui si sta creando il file zip e rinominarlo in idp_config.xml.

Name

config.json

FederationMetadata.xml

Open

Edit

Share with Skype

Move to OneDrive

7-Zip

CRC SHA

Edit with Notepad++

Share

Open with

Cisco AMP For Endpoints

Restore previous versions

Send to

Cut

Copy

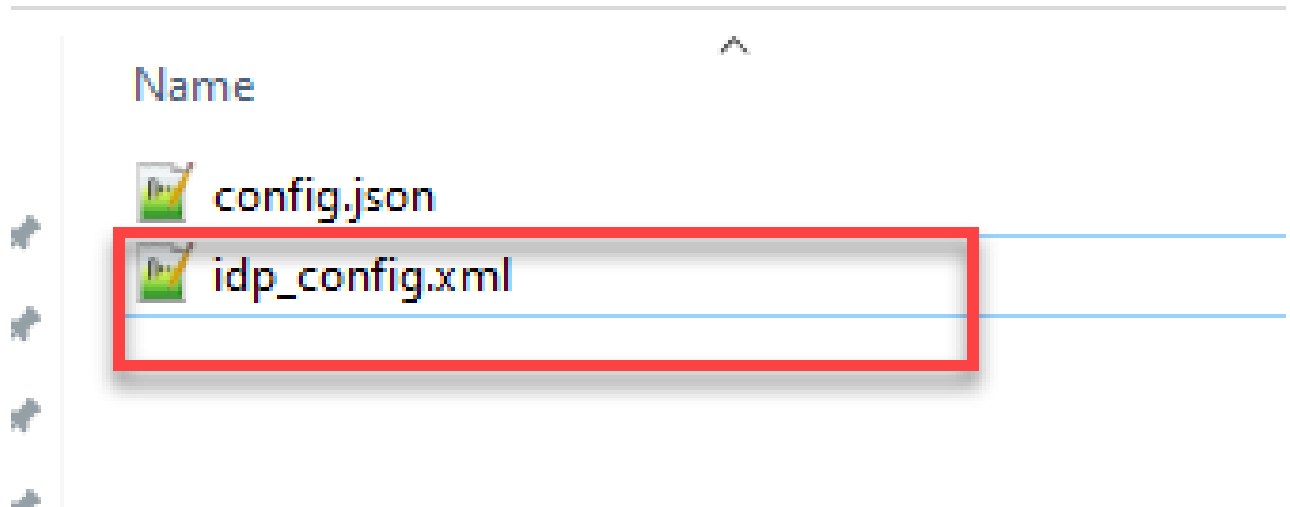
Create shortcut

Delete

Rename

Properties

Local Disk (D:) > brentssoconfig > SSOconfig



Creazione del file config.json con il relativo contenuto

Il file config.json contiene i tre attributi seguenti e deve essere racchiuso tra parentesi graffe { }:

1. supportedDomains: elenco di domini controllati per l'autenticazione SSO con IdP. Più domini possono essere separati da una virgola.
2. authenticationIdMapping: parametro restituito come parte della regola attestazione in uscita da ADFS/IdP. Deve corrispondere al valore del nome del tipo di attestazione in uscita nell'IdP. Regola attestazione.
3. ssoServiceProviderAddress: URL FQDN a cui il provider di identità invia le risposte SAML. Deve essere il nome di dominio completo (FQDN) di Webbridge.

Configured as 'uid' to match outgoing claim on ADFS

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

the URL of Webbridge for IdP to send response to

supported domain of 'brhuff.com' for SSO authentication

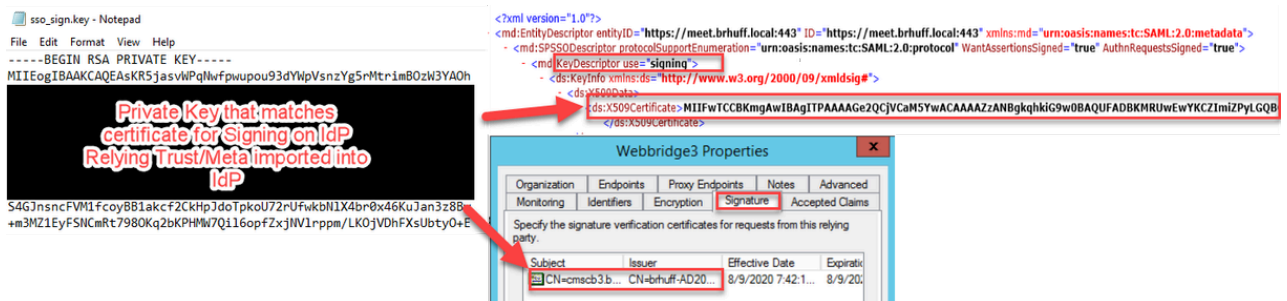
Make sure the LDAP attribute used in ADFS for the Claim rule matches the authenticationIdMapping in the CMS API

Impostare sso_sign.key (FACOLTATIVO)

Il file deve contenere la chiave privata del certificato utilizzato per l'accesso ai metadati di Webbridge importati nel provider di identità. Il certificato utilizzato per la firma può essere impostato durante l'importazione dei metadati di Webbridge in ADFS popolando il certificato X509 con le informazioni sul certificato nella sezione <KeyDescriptor use=signature>. Può inoltre essere visualizzato (e importato) in ADFS nel componente attendibile di Webbridge in Proprietà > Firma.

Nell'esempio successivo è possibile visualizzare il certificato callbridge (CN=cmscb3.brhuff.local), che è stato aggiunto ai metadati di Webbridge prima di essere importato in ADFS. La chiave privata inserita in sso_sign.key è quella che corrisponde al certificato cmscb3.brhuff.local.

Questa configurazione è facoltativa e necessaria solo se si intende crittografare le risposte SAML.

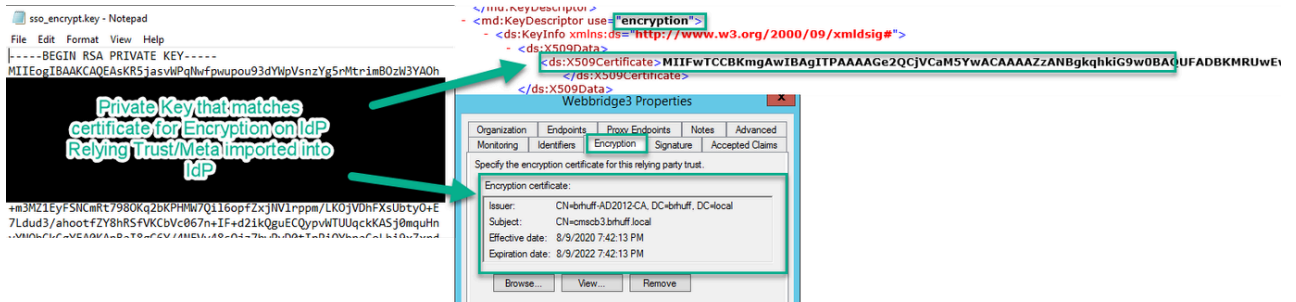


Impostare sso_encrypt.key (FACOLTATIVO)

Il file deve contenere la chiave privata del certificato utilizzato per la crittografia nei metadati di webbridge importati nel provider di identità. Il certificato utilizzato per la crittografia può essere impostato durante l'importazione dei metadati di Webbridge in ADFS popolando il certificato X509 con le informazioni sul certificato nella sezione <KeyDescriptor use=encryption>. Può inoltre essere visualizzato (e importato) in ADFS nel componente attendibile di Webbridge in Proprietà > Crittografia.

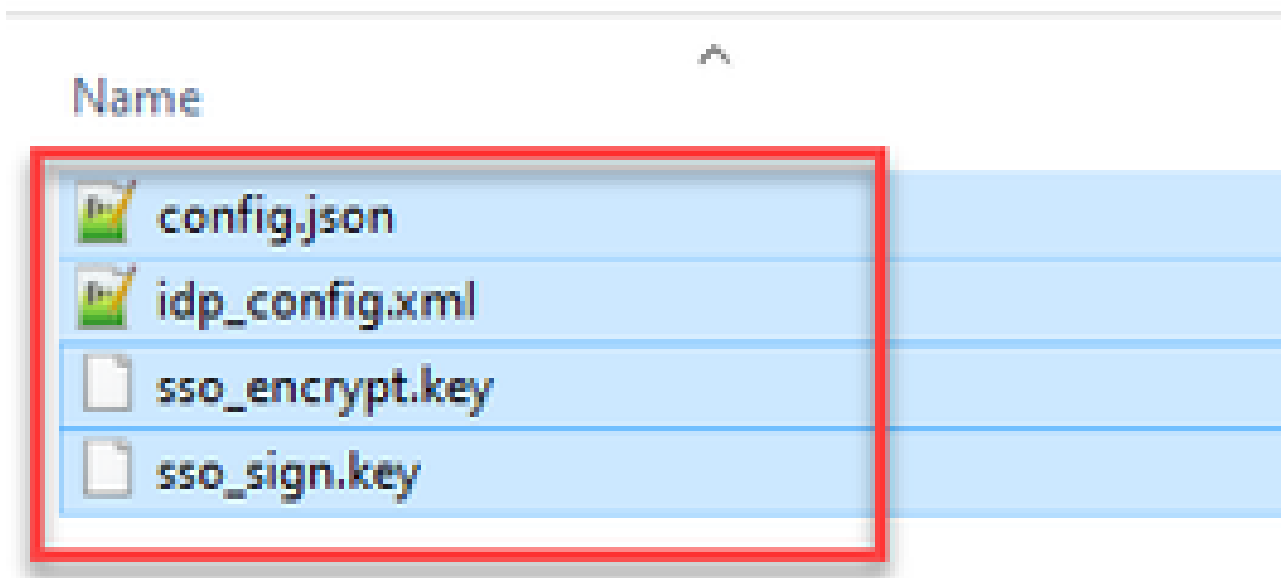
Nell'esempio seguente viene illustrato il certificato callbridge (CN=cmscb3.brhuff.local), aggiunto ai metadati di Webbridge prima dell'importazione in ADFS. La chiave privata inserita in 'sso_encrypt.key' è quella che corrisponde al certificato cmscb3.brhuff.local.

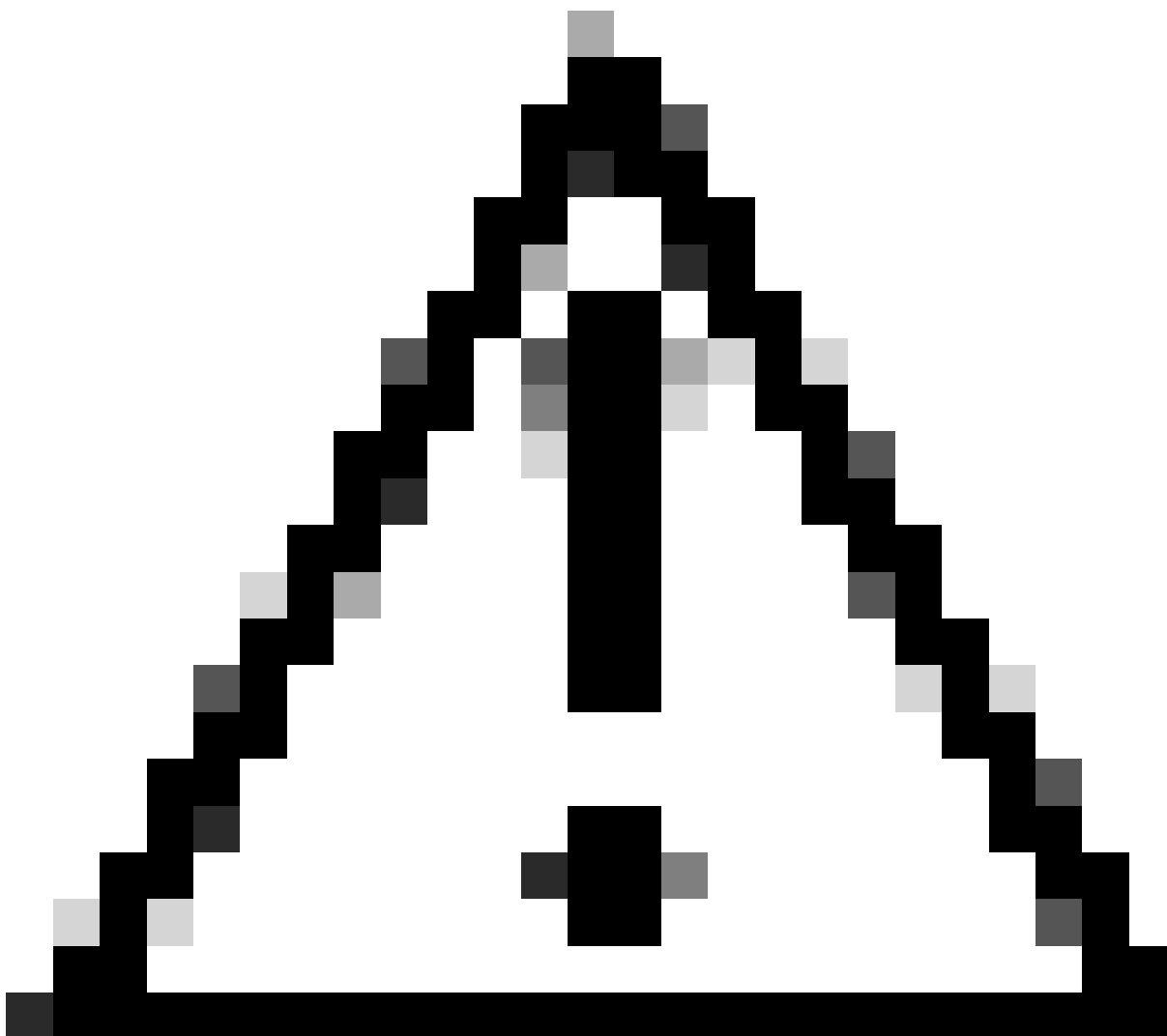
Si tratta di una configurazione facoltativa, necessaria solo se si desidera crittografare le risposte SAML.



Creazione del file ZIP SSO

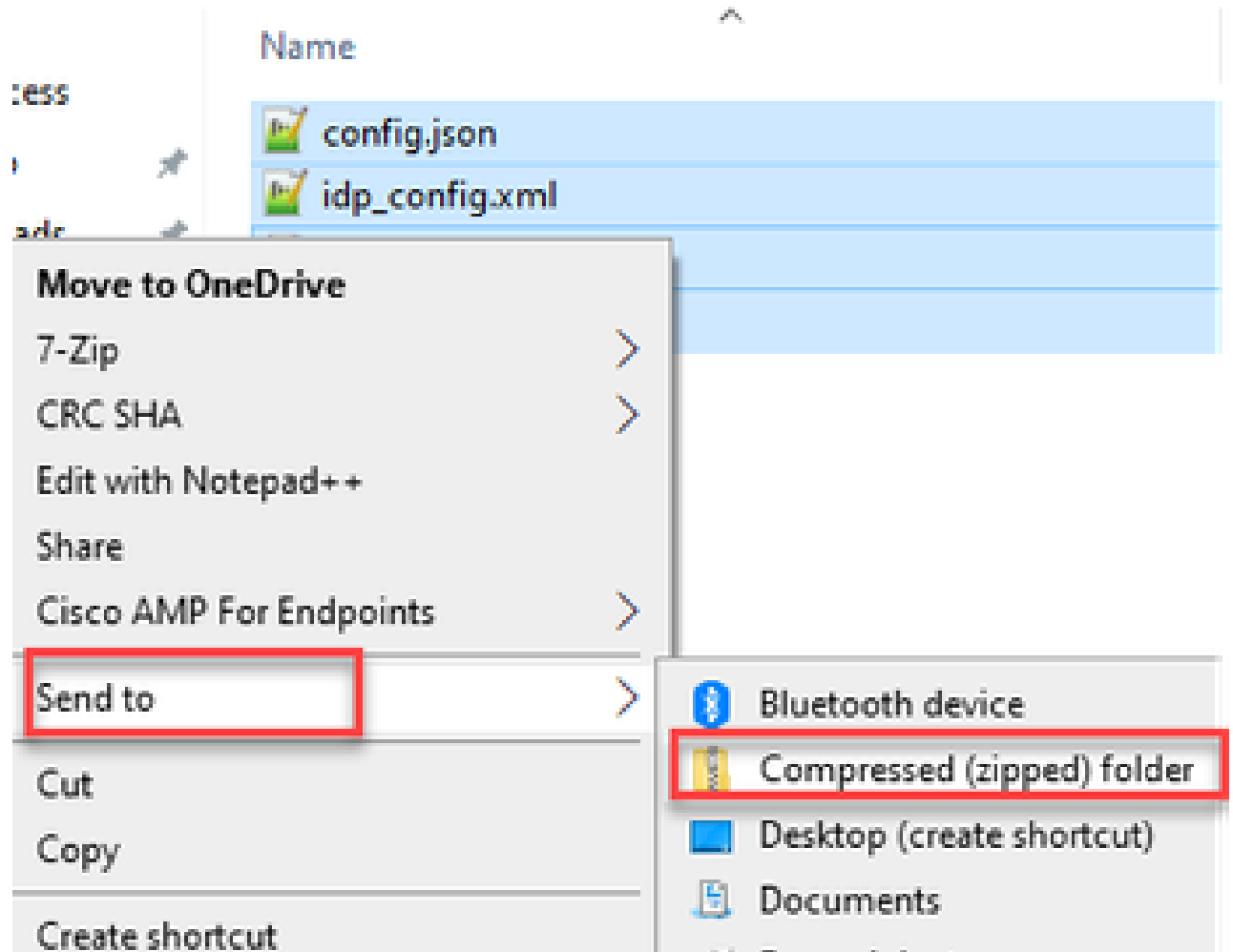
1. Evidenziare tutti i file da utilizzare per il file di configurazione SSO.



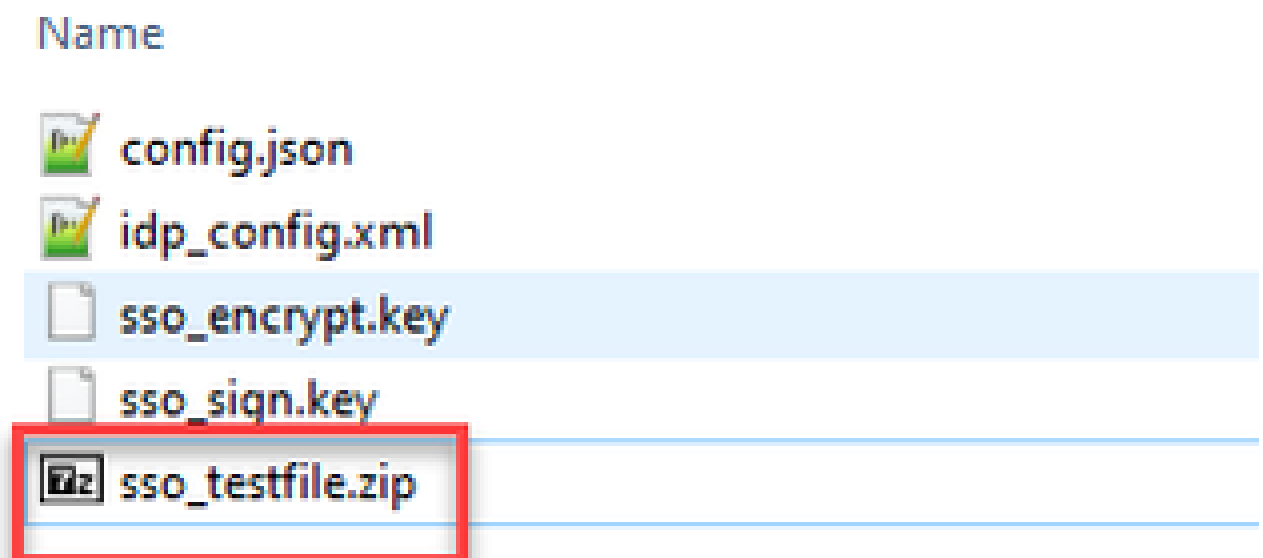


Attenzione: non comprimere la cartella contenente i file, in quanto l'SSO non funziona.

2. Fare clic con il pulsante destro del mouse sui file evidenziati e selezionare Invia a > Cartella compressa.



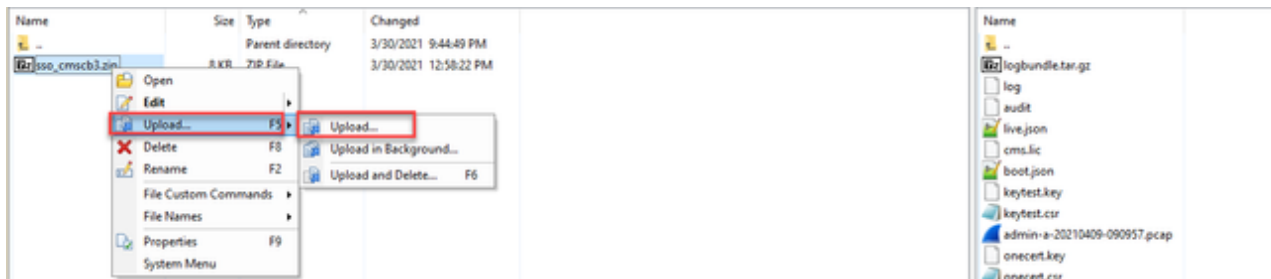
3. Dopo aver compresso i file, rinominarli con il nome desiderato con il prefisso sso_:



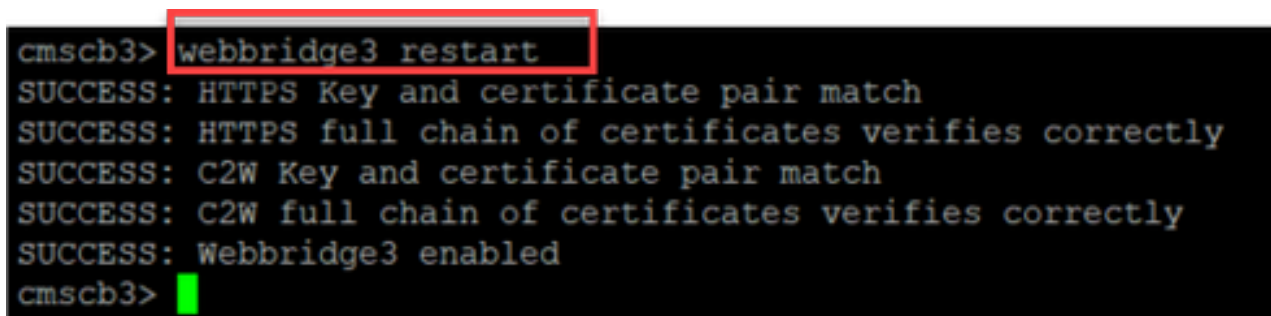
Carica i file SSO Zip in Webbridge

Aprire un client SFTP/SCP, in questo esempio viene utilizzato WinSCP e connettersi al server che ospita Webbridge3.

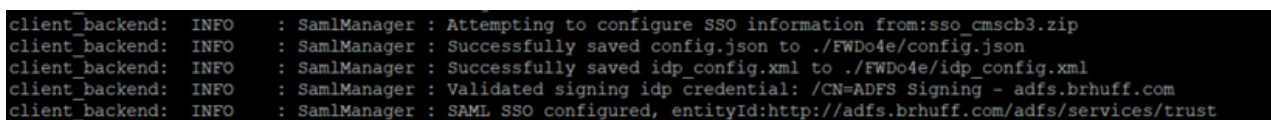
1. Nel riquadro di sinistra, spostarsi nella posizione in cui si trova il file ZIP SSO e fare clic con il pulsante destro del mouse per selezionare il caricamento o trascinare il file.



2. Una volta caricato completamente il file sul server Webbridge3, aprire una sessione SSH ed eseguire il comando webbridge3 restart.



3. Nel syslog, questi messaggi indicano che l'abilitazione SSO è riuscita:



Scheda CAC (Common Access Card)

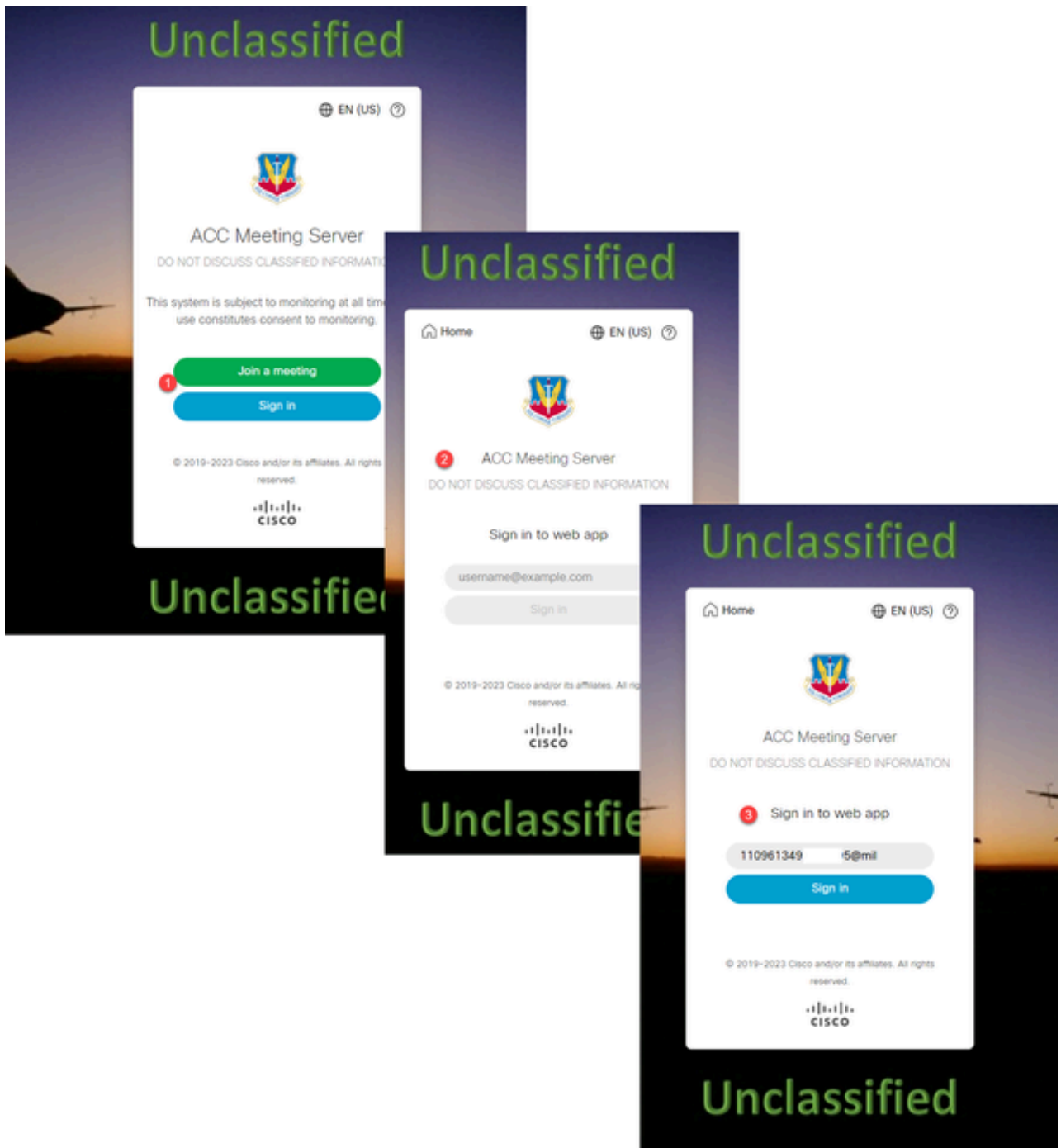
Una Common Access Card (CAC) è una smart card che serve come identificazione standard per il personale militare in servizio attivo, i dipendenti civili del Dipartimento della Difesa e il personale terzista idoneo.

Di seguito è riportato l'intero processo di accesso per gli utenti che utilizzano le schede CAC:

1. Accendere il PC e inserire la scheda CAC
2. Accedere (a volte selezionare il certificato) e immettere Pin
3. Apri browser
4. Passare all'URL di partecipazione e visualizzare le opzioni Partecipa a riunione o Accedi
5. Accesso: immettere il nome utente configurato come jidMapping previsto per Active

Directory da un accesso CAC

6. Accedi
7. La pagina ADFS viene visualizzata brevemente e viene popolata automaticamente
8. L'utente verrà connesso a questo punto



Configurare `jidMapping` (ovvero il nome di accesso dell'utente) in `Ldapmapping` nello stesso modo in cui ADFS utilizza la scheda CAC. `$userPrincipalName$`, ad esempio (con distinzione tra maiuscole e minuscole)

Impostare inoltre lo stesso attributo LDAP per `authenticationIdMapping` in modo che corrisponda all'attributo utilizzato nella regola Attestazione in ADFS.

La regola di attestazione mostra che invierà `$userPrincipalName$` nuovamente a CMS come UID.

153 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
⊕		

Test dell'accesso SSO tramite WebApp

Ora che SSO è stato configurato, è possibile testare il server:

1. Passare all'URL di Webbridge per l'app Web e selezionare il pulsante Accedi.



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

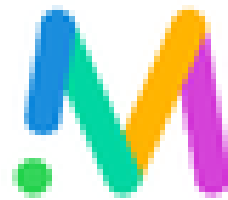
Join a meeting

Sign in

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



2. All'utente viene offerta la possibilità di inserire il proprio nome utente (in questa pagina non è presente l'opzione per l'immissione della password).



Cisco Meeting Server

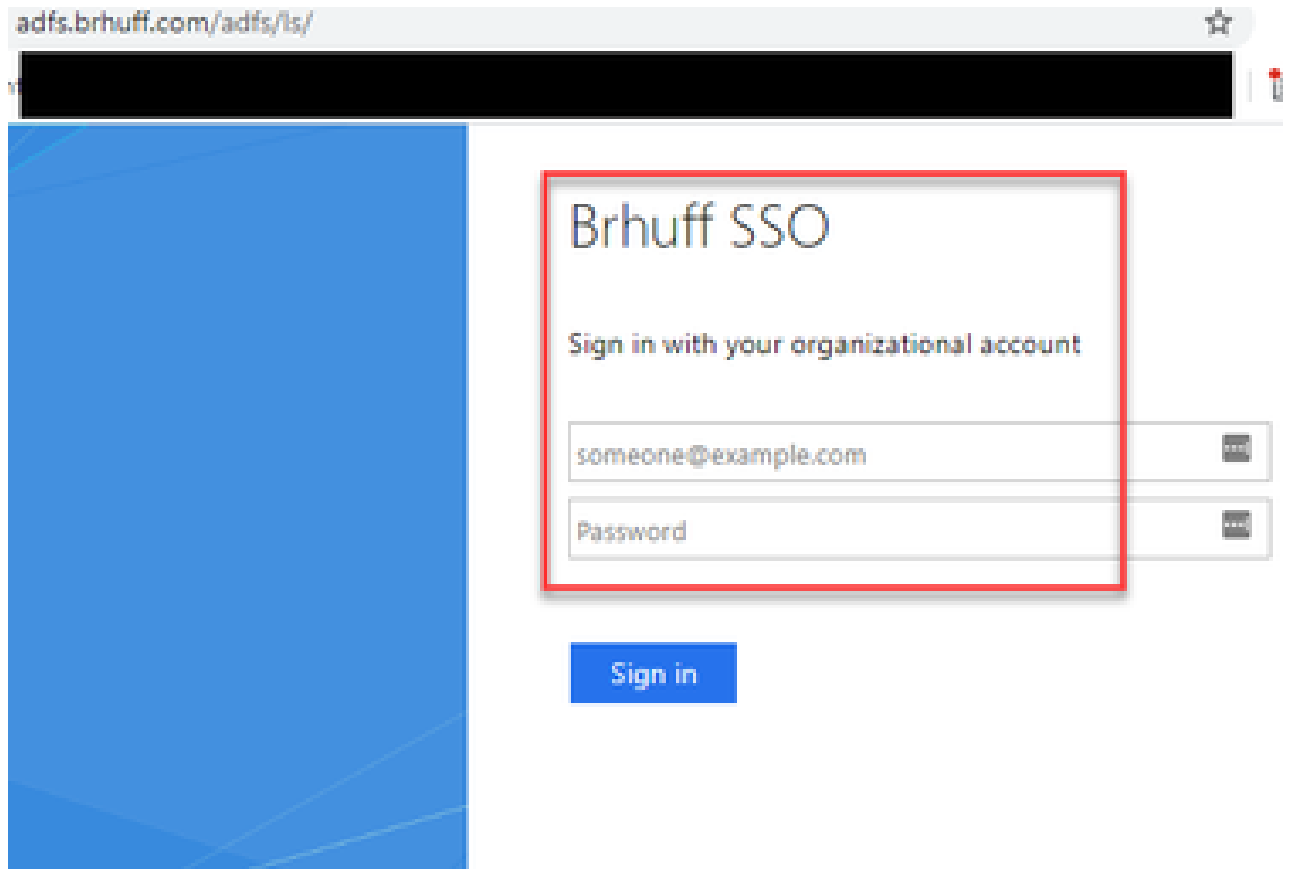
web app

Sign in to web app

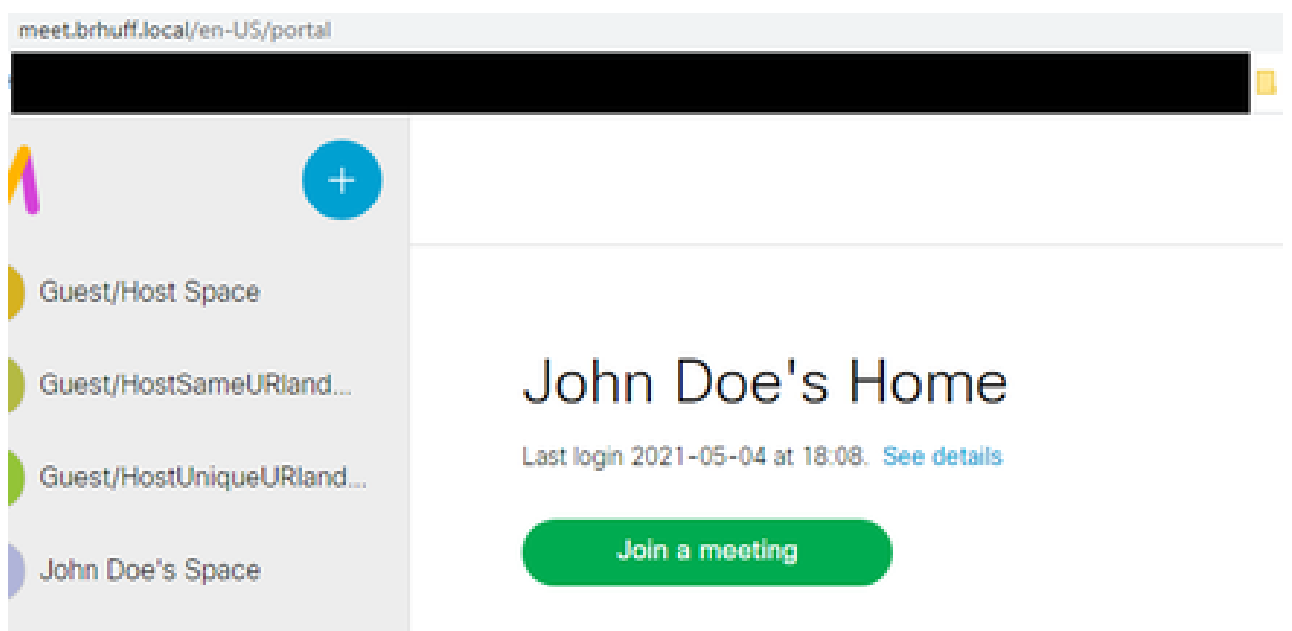
© 2020 Cisco and/or its affiliates. All rights reserved.



3. L'utente viene quindi reindirizzato alla pagina ADFS (dopo aver immesso i dettagli dell'utente) in cui l'utente deve immettere le proprie credenziali per l'autenticazione a IdP.



4. L'utente, dopo aver immesso e convalidato le credenziali con IdP, viene reindirizzato con il token per accedere alla home page dell'app Web:



Risoluzione dei problemi

Risoluzione dei problemi di base

Per la risoluzione dei problemi di base relativi all'SSO:

1. Verificare che i metadati costruiti per Webbridge3 utilizzati per l'importazione come trust di dipendenza in IdP siano configurati correttamente e che l'URL configurato corrisponda esattamente all'indirizzo ssoServiceProviderAddress in config.json.
2. Verificare che i metadati forniti dall'IdP e compressi nel file di configurazione di Webbridge3 siano i più recenti dell'IdP, come se fossero state apportate modifiche al nome host del server, ai certificati e così via, è necessario riesportarli e comprimere il file di configurazione.
3. Se si utilizzano chiavi private di firma e crittografia per crittografare i dati, verificare che le chiavi corrispondenti corrette facciano parte del file sso_XXXX.zip caricato in webbridge. Se possibile, provare senza le chiavi private opzionali per verificare se SSO funziona senza questa opzione crittografata.
4. Verificare che config.json sia configurato con i dettagli corretti per i domini SSO, l'URL di Webbridge3 e il mapping di autenticazione previsto per la corrispondenza da SAMLResponse.

Sarebbe inoltre ideale tentare la risoluzione dei problemi dal punto di vista del log:

1. Quando si passa all'URL di Webbridge, posizionare `?trace=true` alla fine dell'URL per abilitare una registrazione dettagliata nel syslog CMS. (ad esempio: <https://join.example.com/en-US/home?trace=true>).
2. Eseguire il syslog follow sul server Webbridge3 per acquisire informazioni durante il test oppure eseguire il test con l'opzione trace aggiunta all'URL e raccogliere il logbundle.tar.gz dai server Webbridge3 e CMS Callbridge. Se webbridge e callbridge si trovano sullo stesso server, è necessario solo il file logbundle.tar.gz.

Codici di errore di Microsoft ADFS

A volte si verifica un errore del processo SSO che può causare un errore nella configurazione o nella comunicazione dell'IdP con l'IdP. Se si utilizza l'ADFS, è consigliabile esaminare il collegamento successivo per verificare il problema riscontrato e adottare le misure necessarie per risolverlo:

[Codici di stato Microsoft](#)

Di seguito è riportato un esempio:

```
client_backend: ERROR : SamlManager : richiesta di autenticazione SAML _e135ca12-4b87-4443-abe1-30d396590d58 non riuscita. Motivo: urn:oasis:names:tc:SAML:2.0:status:Responder
```

Questo errore indica che, in base alla documentazione precedente, l'errore si è verificato a causa di IdP o ADFS e pertanto deve essere gestito dall'amministratore di ADFS per risolverlo.

Impossibile ottenere authenticationID

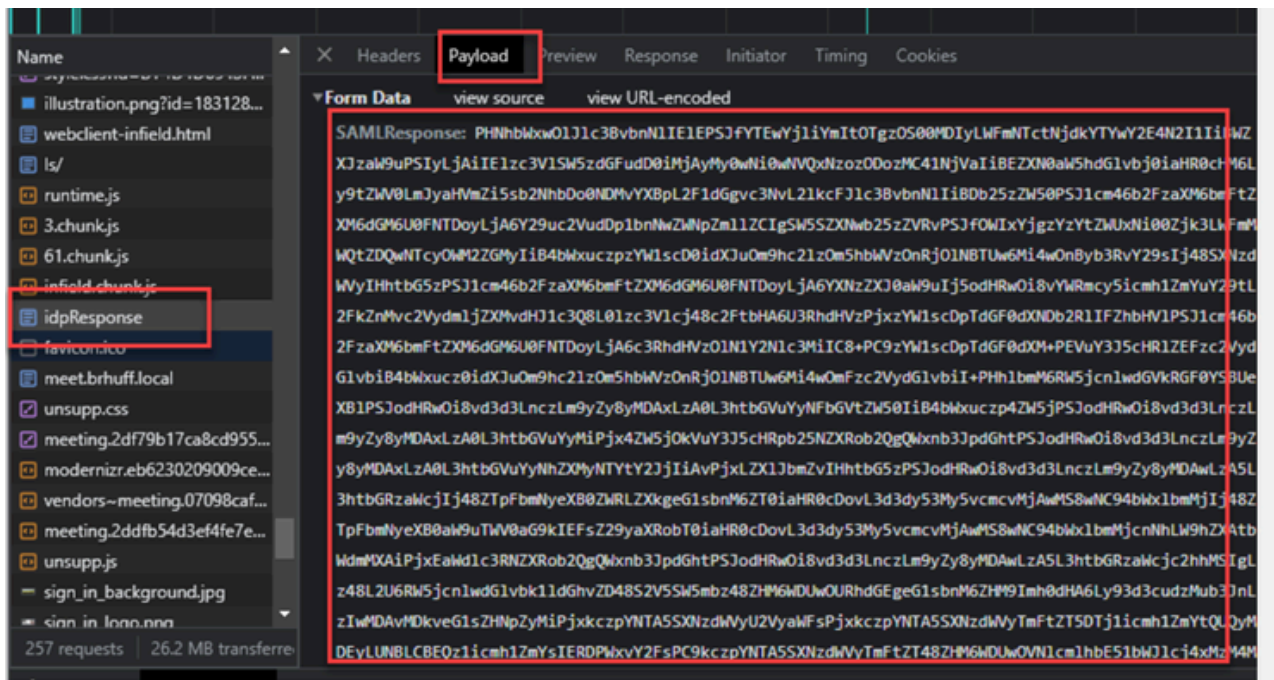
In alcuni casi, durante lo scambio di SAMLResponse dall'IdP, il Webbridge può visualizzare questo messaggio di errore nei registri con un errore di accesso tramite SSO:

```
client_backend: INFO : SamlManager : [57dff9e3-862e-4002-b4fa-683e4aa6922c] Impossibile ottenere un ID di autenticazione
```

Ciò significa che durante la revisione dei dati SAMLResponse restituiti dall'IdP durante lo scambio di autenticazione, Webbridge3 non ha trovato un attributo corrispondente valido nella risposta rispetto al relativo config.json per l'authenticationId.

Se la comunicazione non è crittografata con l'uso delle chiavi private di firma e crittografia, la risposta SAML può essere estratta dalla registrazione in rete degli strumenti di sviluppo tramite un browser Web e decodificata utilizzando base64. Se la risposta è crittografata, è possibile richiedere la risposta SAML decrittografata dal lato IdP.

Nell'output di registrazione della rete degli strumenti di sviluppo, noto anche come dati HAR, cercare idpResponse nella colonna del nome e selezionare Payload per visualizzare la risposta SAML. Come accennato in precedenza, questa può essere decodificata utilizzando il decodificatore base64.



Quando si ricevono i dati SAMLResponse, controllare la sezione di <AttributeStatement> per individuare i nomi attributo restituiti e all'interno di questa sezione è possibile trovare i tipi di attestazione configurati e inviati dall'IdP. Ad esempio:

```
<IstruzioneAttributo>  
<Attribute Name="<URL per nomecomune">  
<AttributeValue>testuser1</AttributeValue>  
</Attribute>  
<Attribute Name="<URL for NameID">  
<AttributeValue>testuser1</AttributeValue>  
</Attribute>  
<Attribute Name="uid">  
<AttributeValue>testuser1</AttributeValue>  
</Attribute>  
</AttributeStatement>
```

Esaminando i nomi precedenti, è possibile controllare <AttributeName> nella sezione Istruzione Attribute e confrontare ogni valore con quello impostato nella sezione authenticationIdmapping di SSO config.json.

Nell'esempio precedente è possibile vedere che la configurazione per authenticationIdMapping NON corrisponde esattamente a quanto passato e pertanto non è possibile individuare un elemento authenticationId corrispondente:

mapping ID autenticazione : <http://example.com/claims/NameID>

Per risolvere questo problema, è possibile tentare di utilizzare due metodi:

1. La regola di attestazione in uscita IdP può essere aggiornata in modo da avere un'attestazione corrispondente esattamente a quella configurata in

authenticationIdMapping di config.json sul WebBridge3. (Regola attestazione aggiunta in IdP per <http://example.com/claims/NameID>)

O

2. È possibile aggiornare config.json in Webbridge3 in modo che 'authenticationIdMapping' corrisponda esattamente a quella configurata come una delle regole attestazioni in uscita configurate in IdP. ovvero 'authenticationIdMapping' da aggiornare in modo che corrisponda a uno dei nomi di attributo, che può essere "uid", "<URL>/NameID" o "<URL>/CommonName". Purché corrisponda (esattamente) al valore previsto configurato nell'API Callbridge quando passato

Nessuna asserzione passata/associata nella convalida

Talvolta, durante lo scambio di SAMLResponse dall'IdP, il Webbridge visualizza questo errore per indicare che non è possibile soddisfare l'asserzione e ignora le asserzioni che non corrispondono alla configurazione del server:

```
client_backend: ERRORE : SamlManager : nessuna asserzione ha superato la convalida
client_backend: INFO : SamlManager : Asserzione ignorata senza l'utilizzo di nei destinatari consentiti
```

Questo errore indica che durante la revisione di SAMLResponse dall'IdP, Webbridge non è riuscito a individuare le asserzioni corrispondenti, ignorando quindi gli errori di mancata corrispondenza e provocando un errore di accesso SSO.

Per individuare questo problema, è consigliabile esaminare SAMLResponse dall'IdP. Se la comunicazione non è crittografata con l'utilizzo delle chiavi private di firma e crittografia, la risposta SAML può essere estratta dalla registrazione di rete degli strumenti di sviluppo tramite un browser Web e decodificata utilizzando base64. Se la risposta è crittografata, è possibile richiedere la risposta SAML decrittografata dal lato IdP.

Quando si esaminano i dati SAMLResponse, osservando la sezione <AudienceRestriction> della risposta, è possibile trovare tutti i gruppi di destinatari per i quali questa risposta è limitata:

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

Utilizzando il valore della sezione <Audience> (<https://cisco.example.com>) è possibile confrontarlo con il valore ssoServiceProviderAddress nel file config.json della configurazione di Webbridge e verificare se corrisponde esattamente. Nell'esempio, la causa dell'errore è rappresentata dal fatto che il gruppo di destinatari NON corrisponde all'indirizzo del provider di servizi nella configurazione, perché al nome del gruppo di destinatari è stato aggiunto :443:

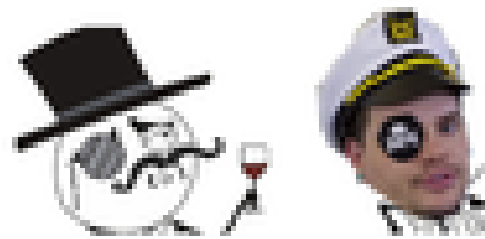
Indirizzo ssoServiceProvider : <https://cisco.example.com:443>

Ciò richiede una corrispondenza esatta tra questi due elementi per non generare un errore come questo. In questo esempio, la correzione potrebbe essere eseguita in uno dei due metodi seguenti:

1. È possibile rimuovere :443 dall'indirizzo nella sezione ssoServiceProviderAddress del file config.json, in modo che corrisponda al campo Audience fornito in SAMLResponse dall'IdP.
O

2. È possibile aggiornare i metadati OR del trust party di connessione per Webbridge3 nell'IdP in modo che :443 venga aggiunto all'URL. Se i metadati vengono aggiornati, è necessario importarli nuovamente come trust party di connessione nell'ADFS. Se tuttavia si modifica il componente attendibile direttamente dalla procedura guidata IdP, non sarà necessario importarlo di nuovo.)

Accesso non riuscito all'app Web:



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign in

 Sign in failed

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



), webbridge verifica che il dominio utilizzato corrisponda a quello nel file config.json, quindi invia le informazioni SAML al client, indicando a quest'ultimo dove connettersi per l'autenticazione. Il client tenterà di connettersi all'IdP presente nel token SAML. Nell'esempio seguente, il browser visualizza questa pagina perché non è in grado di raggiungere il server ADFS.



Errore nel browser client

Tracce di CMS Webbridge (mentre viene utilizzato ?trace=true)

Mar 19 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Corrispondente a SSO sso_2024.zip nella richiesta di token SAML

Mar 19 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Tentativo di trovare SSO nella richiesta di token SAML

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

Scenario 2:

L'utente ha tentato di accedere utilizzando un dominio che non si trova nel file zip SSO nella pagina di accesso a webbridge. Il client invia un tokenRequest con un payload del nome utente immesso dall'utente. Webbridge interrompe immediatamente il tentativo di accesso.

Tracce di CMS Webbridge (mentre viene utilizzato ?trace=true)

Mar 18 14:54:52.698 utente.err cmscb3-1 client_backend: ERRORE : SamlManager :

Tentativo di accesso SSO non valido

Mar 18 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Impossibile trovare un SSO nella richiesta di token SAML

Mar 18 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Tentativo di trovare SSO nella richiesta di token SAML

Scenario 3:

L'utente ha immesso il nome utente corretto e viene visualizzata la pagina di accesso SSO. Anche in questo caso l'utente immette il nome utente e la password corretti, ma ottiene comunque Accesso non riuscito

Tracce di CMS Webbridge (mentre viene utilizzato ?trace=true)

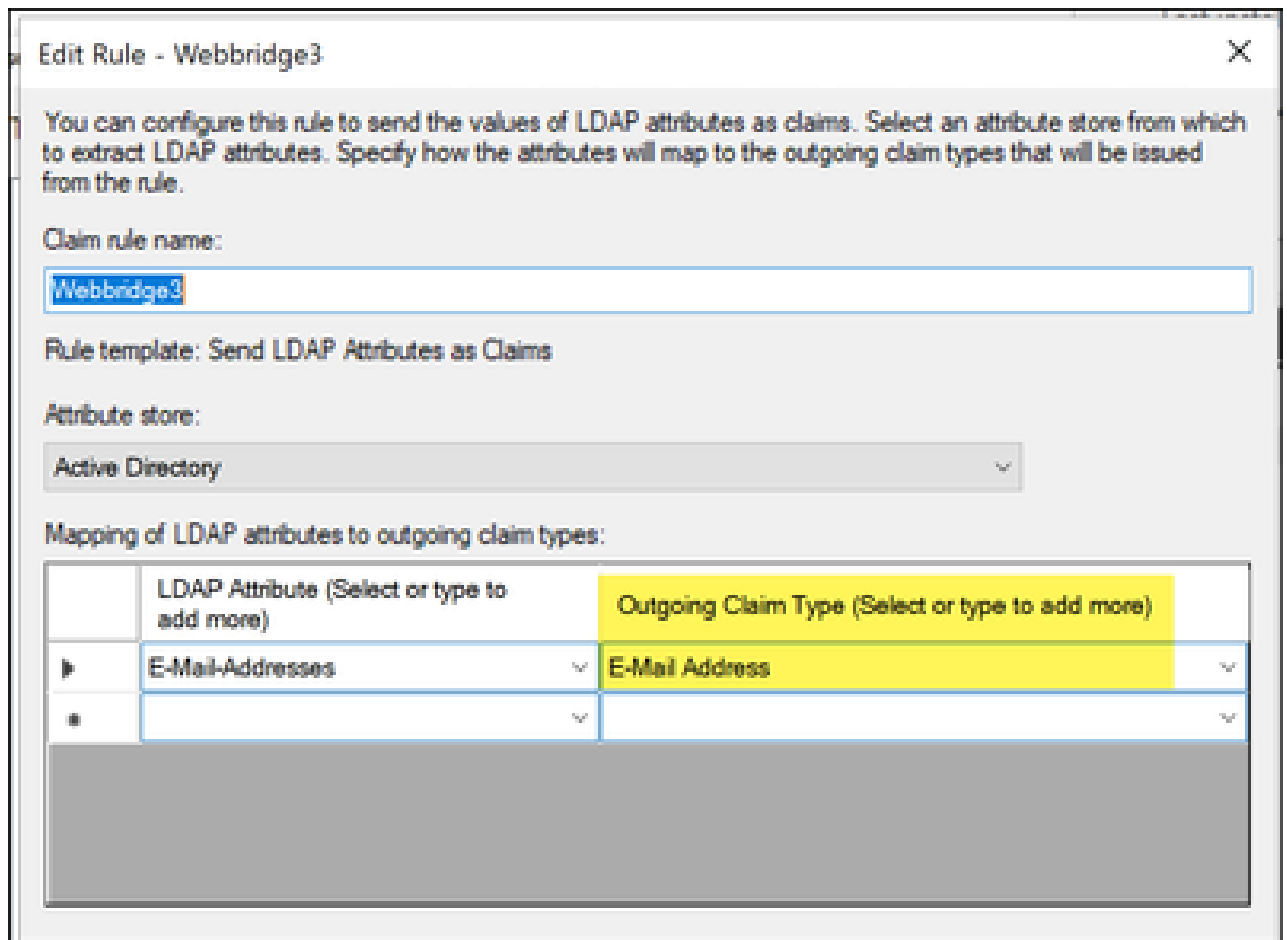
Mar 19 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Corrispondente a SSO_2024.zip nella richiesta di token SAML

Mar 19 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Tentativo di trovare SSO nella risposta IDP SAML

Mar 19 16:39:17.720 user.err cmscb3-1 client_backend: ERROR : SamlManager : Nessun elemento mappato authenticationId trovato nelle asserzioni SAML firmate

Mar 19 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Impossibile ottenere un ID di autenticazione

La causa per lo scenario 3 è stata l'utilizzo da parte della regola attestazione nel provider di identità di un tipo di attestazione non corrispondente all'elemento authenticationIdMapping nel file config.json utilizzato nel file zip SSO caricato in webbridge. Webbridge sta analizzando la risposta SAML e si aspetta che il nome dell'attributo corrisponda a quello configurato nel file config.json.



Regola attestazione in ADFS

```

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

```

esempio di config.json

Nome utente non riconosciuto

Scenario 1:

L'utente ha eseguito l'accesso con un nome utente errato (il dominio corrisponde a quello presente nel file zip SSO caricato in webbridge3, ma l'utente non esiste)



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 non corrisponde all'attributo LDAP configurato utilizzato per la regola attestazione in ADFS. La riga seguente, che indica "AuthenticationID:darmckin@brhuff.com" ottenuto correttamente, indica che ADFS dispone di una regola attestazione configurata con l'attributo che ottiene darmckin@brhuff.com da Active Directory, ma l'elemento AuthenticationID in CMS API > Users indica che è previsto il darmckin. In CMS ldapMappings, AuthenticationID è configurato come \$\$sAMAccountName\$, ma la regola attestazione in ADFS è configurata per l'invio degli indirizzi di posta elettronica, pertanto questa regola non corrisponde.

Come risolvere il problema:

Effettuare una delle seguenti operazioni:

1. Modificare l'ID di autenticazione nel mapping LDAP del CMS in modo che corrisponda a quello utilizzato nella regola attestazione in ADFS ed eseguire una nuova sincronizzazione
2. Modificare l'attributo LDAP utilizzato nella regola attestazione ADFS in modo che corrisponda a quello configurato in ldapmapping CMS

Related objects: </api/v1/ldapMappings>

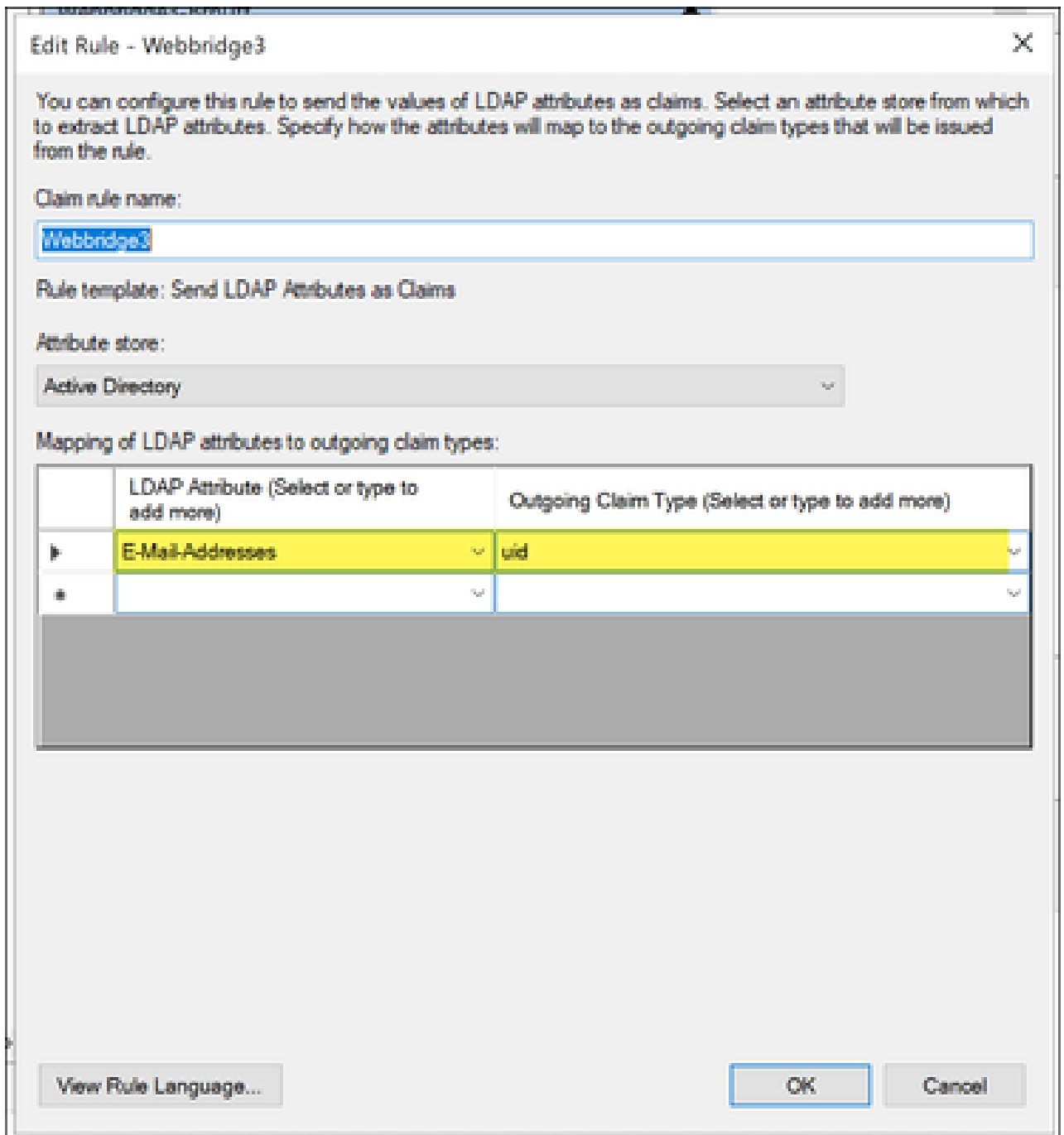
Table view XML view

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

Mapping LDAP API

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

Esempio di utente API



Regola attestazione da ADFS

Esempio di log di Webbridge che mostra il log di lavoro. Esempio generato utilizzando `?trace=true` nell'URL di join:

```
Mar 18 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Corrispondente a SSO_2024.zip nella richiesta di token SAML
```

```
Mar 18 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Tentativo di trovare SSO nella risposta IDP SAML
```

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

[7979f13c-d490-4f8b-899c-0c82853369ba] Autenticazione ottenuta
correttamenteID: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-691e17 83aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5
(utente=darmckin@brhuff.com)

Mar 18 14:24:01.130 user.info cmscb3-1 host:server: INFO : richiesta di accesso riuscita da darmckin@brhuff.com

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

Mar 18 14:24:01.132 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] invio risposta di autenticazione (jwt length=1064, connection=64004556-faea-479f-aabe-69 1e17783aa5)

Mar 18 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/220 24:18:24:01 +0000] stato 200 "POST
/api/auth/sso/idpResponse HTTP/1.1" byte_send 0 http_referring "<https://adfs.brhuff.com/>"
http_user_agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, come Gecko) Chrome/122.0.0.0 Safari/537.3 Da 6" a monte 192.0.2.2:9000:
upstream_response_time 0.038 request_time 0.039 msec 1710786241.133
upstream_response_length 24 200

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).