Configuration et dépannage de l'authentification unique WebApp sur CMS

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Fond
- Configurer
- Diagramme du réseau
- Installation et configuration initiale d'ADFS
- Mapper les utilisateurs CMS au fournisseur d'identité (IdP)
- Créer un XML de métadonnées Webbridge pour IdP
- Importer des métadonnées pour Webbridge dans le fournisseur d'identité (IdP)
- Créer des règles de demande pour le service Webbridge sur le fournisseur d'identité
- Créer un fichier ZIP d'archivage SSO pour Webbridge :
  - Obtenir et configurer le fichier idp_config.xml
  - Créez le fichier config.json avec le contenu
  - Définissez sso_sign.key (FACULTATIF)
  - Définissez le fichier sso_encrypt.key (FACULTATIF)
  - Création du fichier ZIP SSO
  - Télécharger le ou les fichiers Zip SSO sur Webbridge
- Carte d'accès commune (CAC)
- Test de la connexion SSO via WebApp
- Dépannage
  - Dépannage de base
  - Codes d'échec Microsoft ADFS
  - Impossible d'obtenir authenticationID
  - Aucune assertion passée/correspondante dans la validation
  - Échec de la connexion sur Web App :
    - Scénario 1 :
    - Scénario 2 :
    - Scénario 3 :
  - Nom d'utilisateur non reconnu
    - Scénario 1 :
    - Scénario 2 :
  - Journal Webbridge affichant l'exemple de connexion en cours. Exemple généré à l'aide de ?trace=true dans l'URL de jointure :
- Foire aux questions (FAQ)
  - Le WebApp SSO JWT peut-il être étendu ?
  - Dois-je m'authentifier à nouveau sur WebApp si je ferme mon navigateur ?

Comment plusieurs domaines sont-ils pris en charge dans WebApp SSO ?

Informations connexes

Introduction

Ce document décrit comment configurer et dépanner l'implémentation de l'authentification unique (SSO) de Cisco Meeting Server (CMS) Web App.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- CMS Callbridge version 3.1 ou ultérieure
- CMS Webbridge version 3.1 ou ultérieure
- Serveur Active Directory
- Identifier le fournisseur (IdP)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

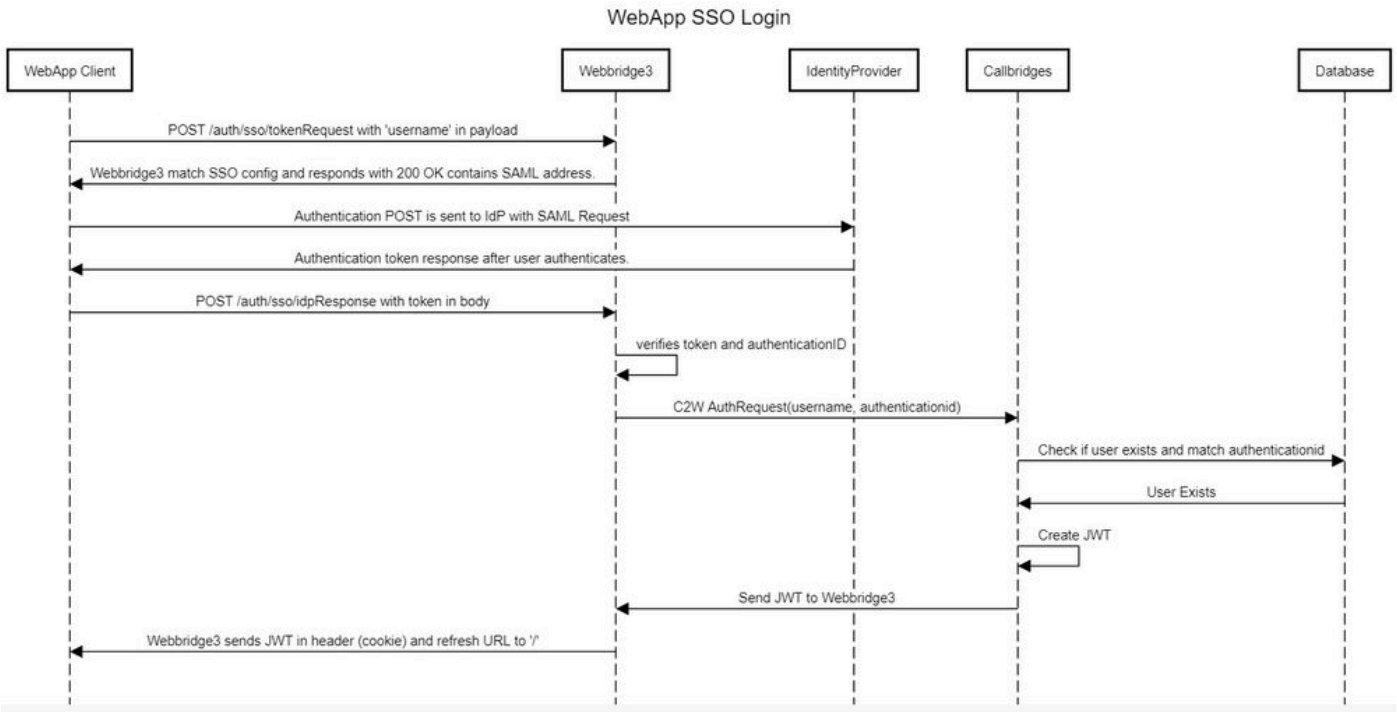
CMS 3.1 et versions ultérieures ont introduit la possibilité pour les utilisateurs de se connecter à l'aide d'un SSO sans avoir à entrer leur mot de passe chaque fois que l'utilisateur se connecte, car une seule session est créée avec le fournisseur d'identification.
Cette fonctionnalité utilise le langage SAML (Security Assertion Markup Language) version 2.0 comme mécanisme SSO.

Remarque : CMS prend uniquement en charge les liaisons HTTP-POST dans SAML 2.0 et rejette tout fournisseur d'identification sans liaisons HTTP-POST disponibles.

Remarque : Lorsque l'authentification unique est activée, l'authentification LDAP de base n'est plus possible.

Configurer

Diagramme du réseau



Installation et configuration initiale d'ADFS

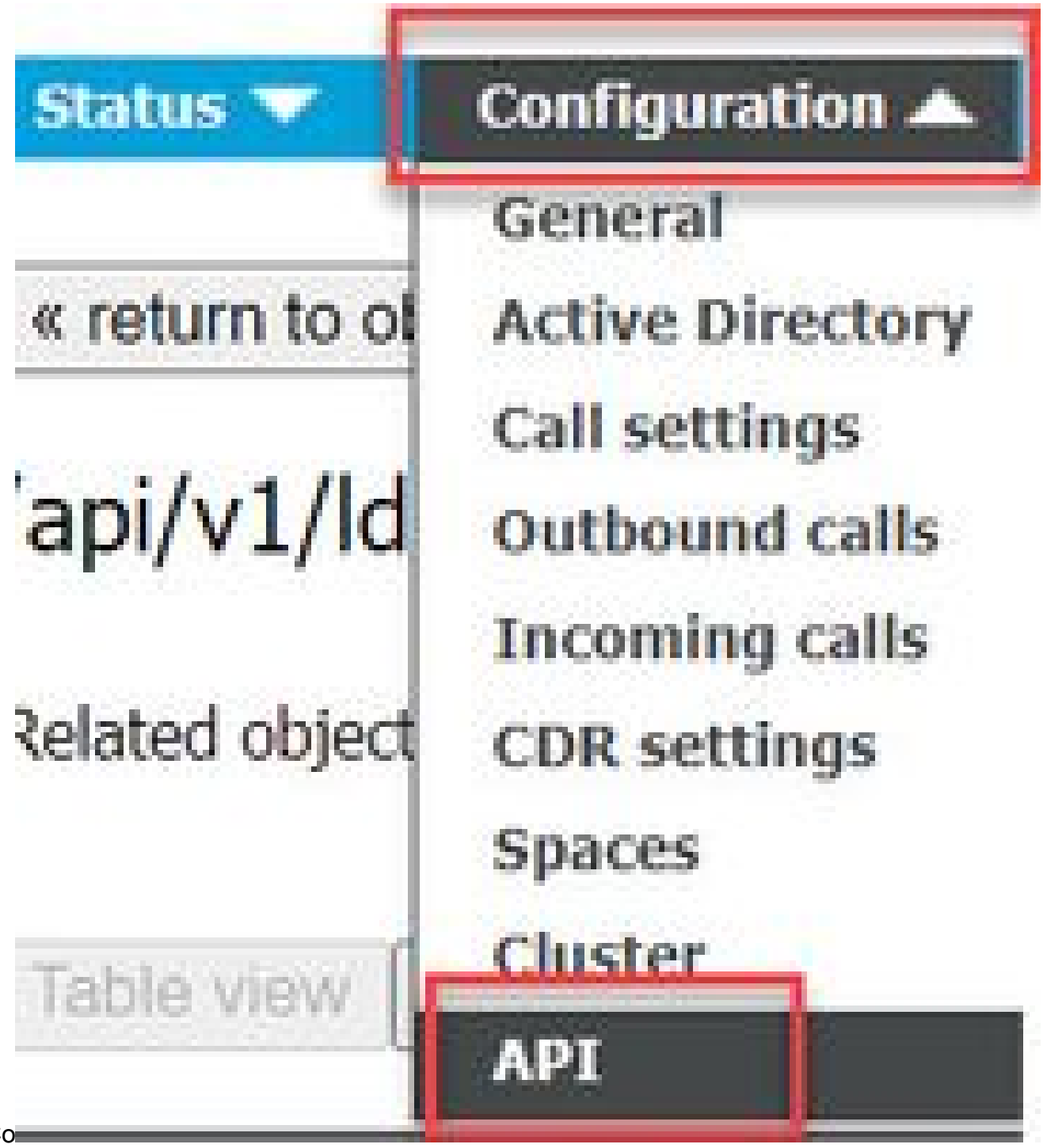
Ce scénario de déploiement utilise Microsoft Active Directory Federation Services (ADFS) comme fournisseur d'identités (IdP) et, par conséquent, il est conseillé d'avoir un ADFS (ou un IdP prévu) installé et en cours d'exécution avant cette configuration.

Mapper les utilisateurs CMS au fournisseur d'identité (IdP)

Pour que les utilisateurs obtiennent une authentification valide, ils doivent être mappés dans l'interface de programmation d'application (API) pour un champ de corrélation fourni par IdP.

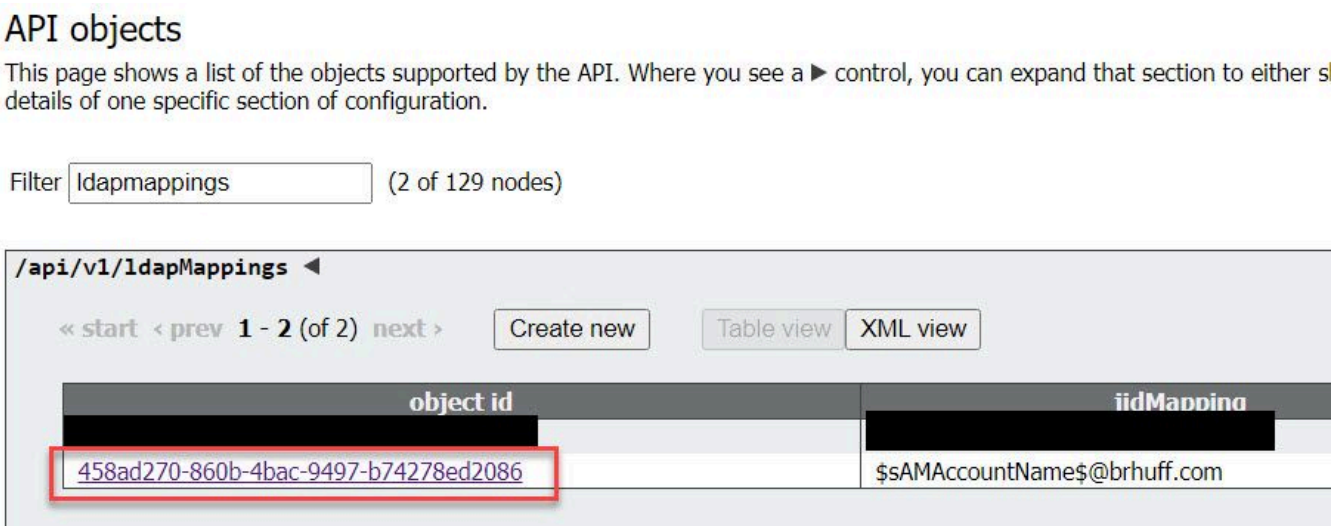
L'option utilisée pour cela est authenticationIdMapping dans le ldapMapping de l'API.

1. Accédez à Configuration > API sur l'interface utilisateur graphique de CMS Web Admin

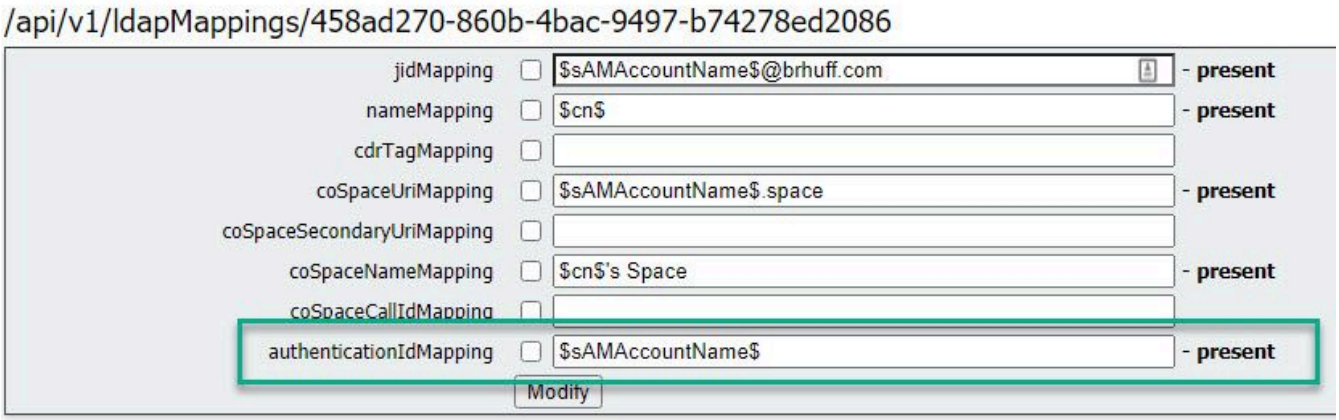


Co

2. Localisez le mappage LDAP existant (ou créez-en un nouveau) sous api/v1/ldapMappings/<GUID-of-Ldap-Mapping>.



3. Dans l'objet ldapMapping sélectionné, mettez à jour authenticationIdMapping vers l'attribut LDAP qui est passé du fournisseur d'identité. Dans l'exemple, l'option $sAMAccountName est utilisée comme attribut LDAP pour le mappage.

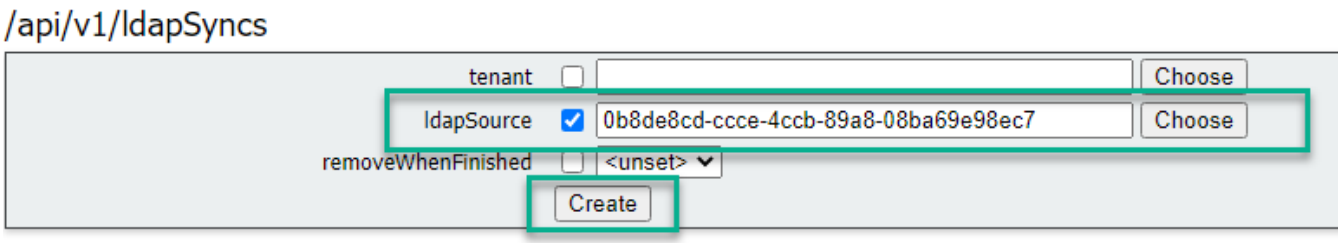


Remarque : Le authenticationIdMapping est utilisé par le pont d'appels/la base de données pour valider la revendication envoyée à partir de l'IdP dans la réponse SAMLR et fournir à l'utilisateur un JSON Web Token (JWT).

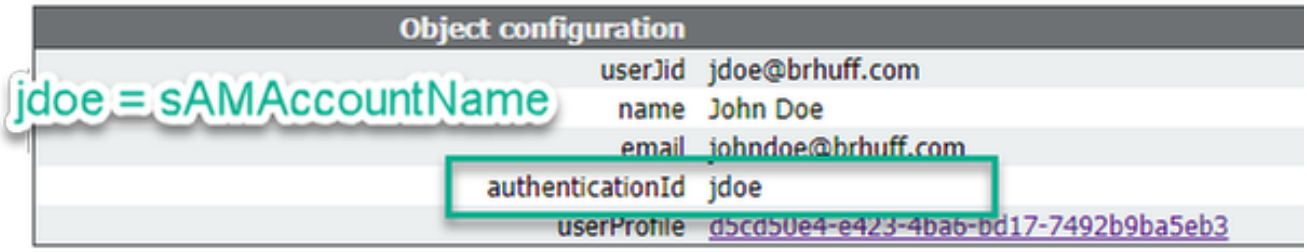
---

4. Effectuez une synchronisation LDAP sur le ldapSource associé au ldapMapping récemment modifié :

Exemple :



5. Une fois la synchronisation LDAP terminée, naviguez dans l'API CMS dans Configuration > api/v1/users et sélectionnez un utilisateur qui a été importé et vérifiez que l'authenticationId est correctement renseigné.



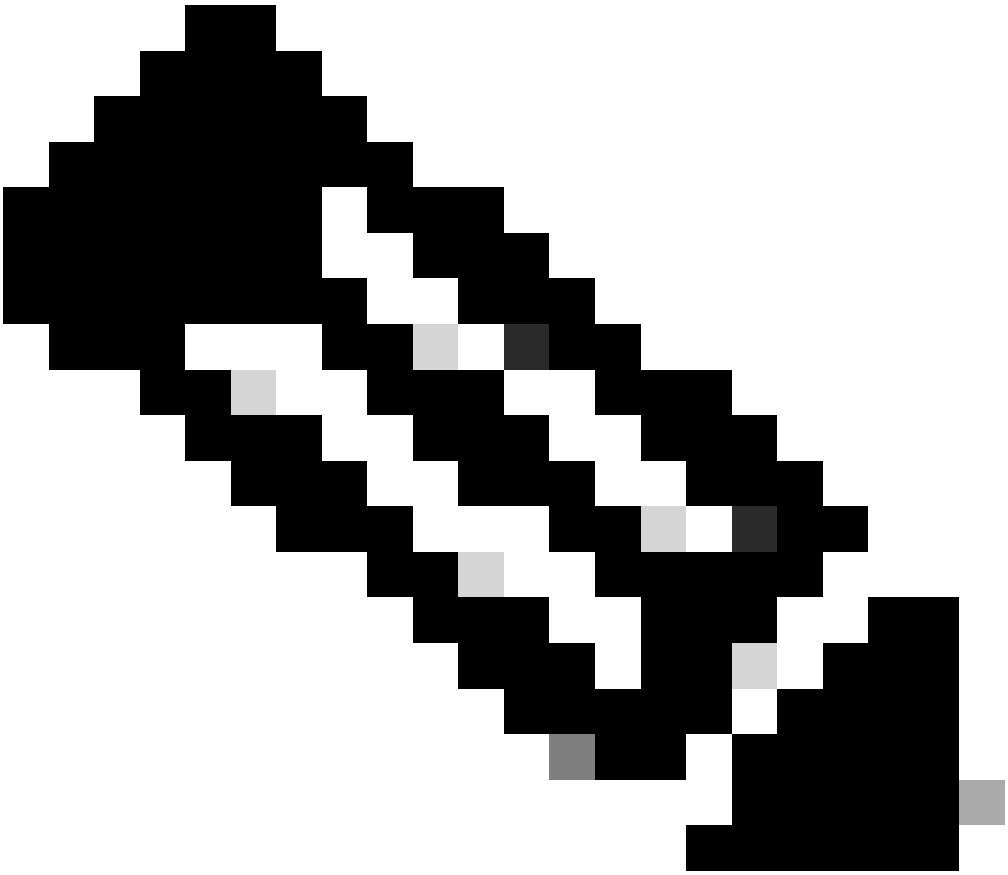
Créer un XML de métadonnées Webbridge pour IdP

Microsoft ADFS permet l'importation d'un fichier XML de métadonnées en tant que partie de confiance afin d'identifier le fournisseur de services utilisé. Il existe quelques façons de créer le fichier XML de métadonnées à cette fin, mais il y a quelques attributs qui doivent être présents dans le fichier :

Exemple de métadonnées Webbridge avec les valeurs requises :

```
<?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 - Il s'agit de l'adresse du serveur Webbridge3 (nom de domaine complet/nom d'hôte) et du port associé qui sont accessibles aux utilisateurs par les navigateurs.



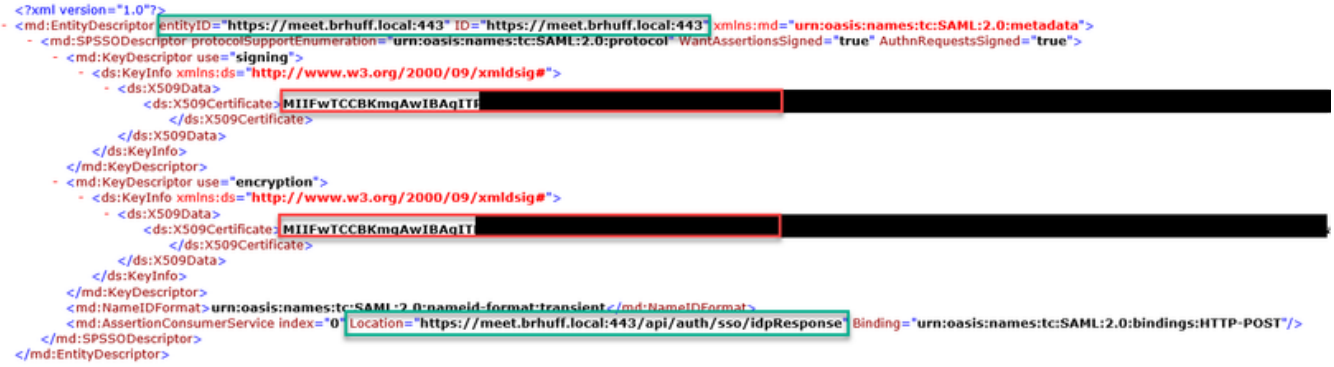
Remarque : S'il existe plusieurs ponts Web utilisant une seule URL, il doit s'agir d'une adresse d'équilibrage de charge.

2. Location : emplacement dans lequel le service HTTP-POST AssertionConsumerService de l'adresse Webbridge. C'est ce qui indique au fournisseur d'identité où rediriger un utilisateur authentifié après la connexion. Il doit être défini sur l'URL idpResponse : https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponse. Par exemple, https://join.example.com:443/api/auth/sso/idpResponse.

3. FACULTATIF - Clé publique pour la signature - il s'agit de la clé publique (certificat) pour la signature, qui est utilisée par le fournisseur d'identité pour vérifier la demande d'authentification à partir de Webbridge. Cette valeur DOIT correspondre à la clé privée « sso_sign.key » sur l'offre groupée SSO téléchargée sur Webbridge afin que le fournisseur d'identité puisse utiliser la clé publique (certificat) pour vérifier la signature. Vous pouvez utiliser un certificat existant de votre déploiement. Ouvrez le certificat dans un fichier texte et copiez le contenu dans le fichier de métadonnées Webbridge. Utilisez la clé correspondante pour le certificat utilisé dans votre fichier sso_xxxx.zip comme fichier sso_sign.key.

4. FACULTATIF - Clé publique pour le chiffrement - il s'agit de la clé publique (certificat) que le fournisseur d'identité utilise pour chiffrer les informations SAML renvoyées à Webbridge. Cette valeur DOIT correspondre à la clé privée « sso_encrypt.key » sur le bundle SSO téléchargé sur Webbridge, afin que Webbridge puisse déchiffrer ce qui est renvoyé par IdP. Vous pouvez utiliser un certificat existant de votre déploiement. Ouvrez le certificat dans un fichier texte et copiez le contenu dans le fichier de métadonnées Webbridge. Utilisez la clé correspondante pour le certificat utilisé dans votre fichier sso_xxxx.zip comme fichier sso_encrypt.key.

Exemple de métadonnées Webbridge à importer dans IdP avec des données de clé publique (certificat) facultatives :

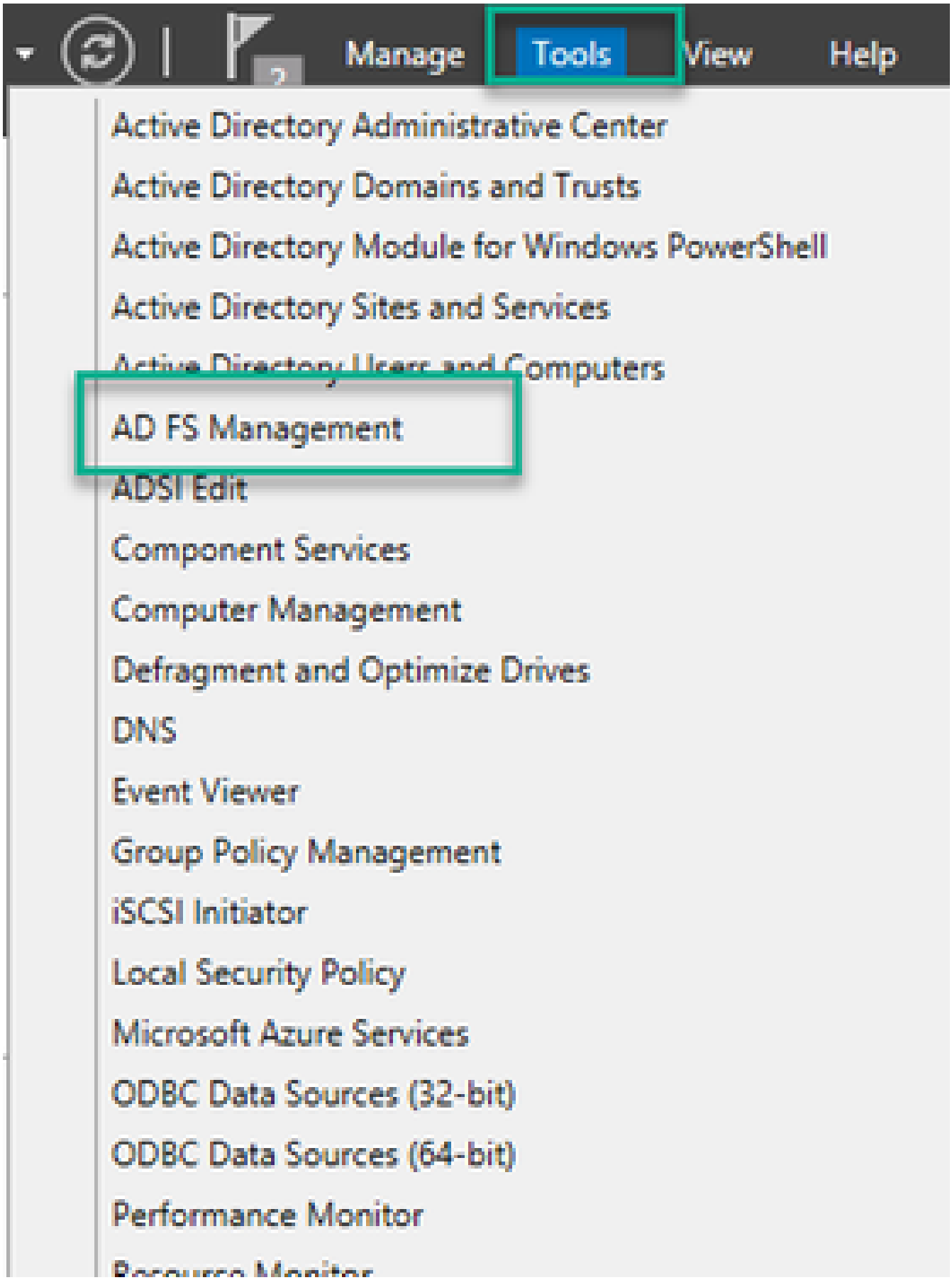


Importer des métadonnées pour Webbridge dans le fournisseur d'identité (IdP)

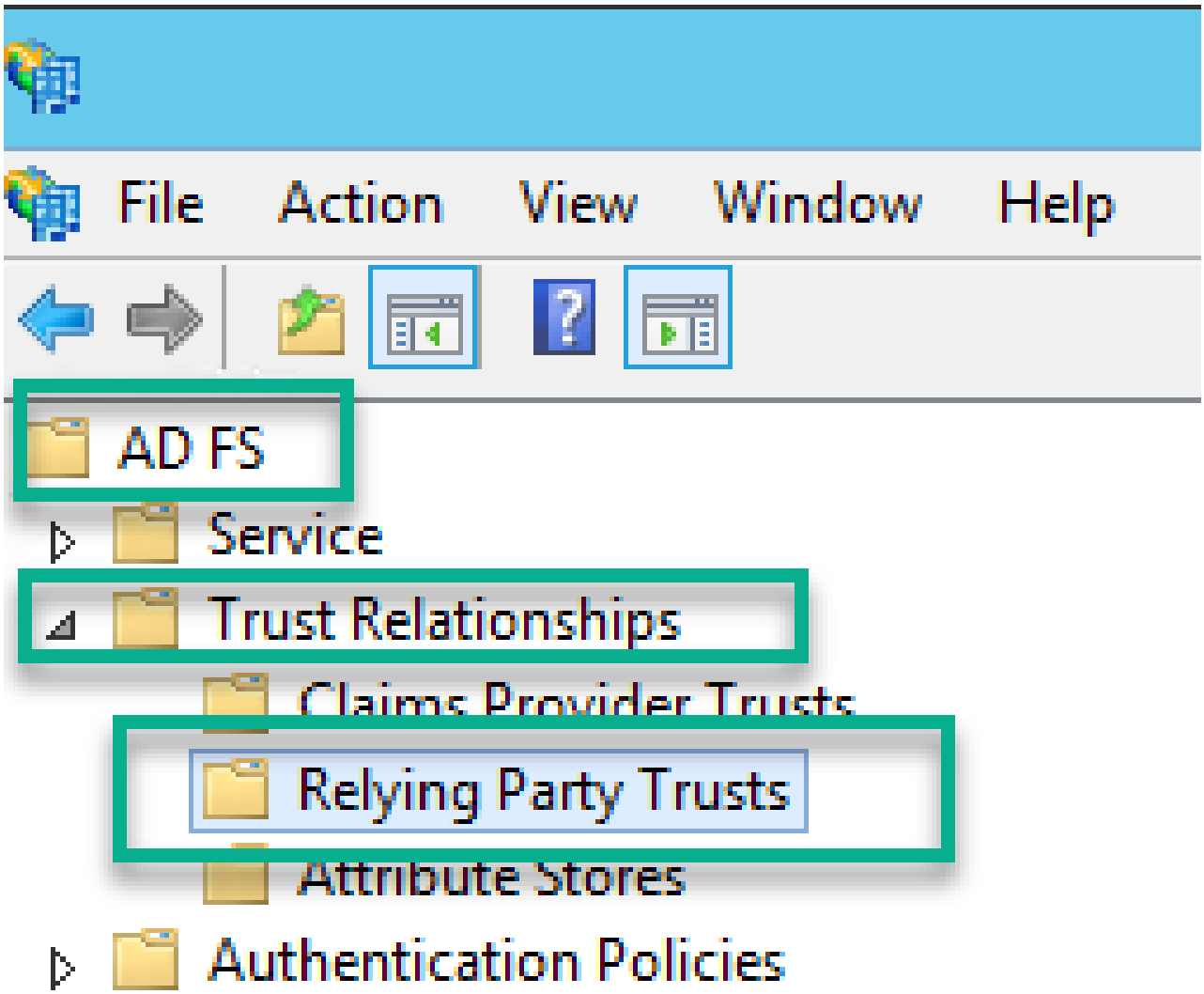
Une fois que le fichier XML de métadonnées a été créé avec les attributs appropriés, le fichier peut être importé sur le serveur Microsoft ADFS pour créer une partie d'approbation de confiance.

1. Bureau à distance dans le serveur Windows hébergeant les services ADFS

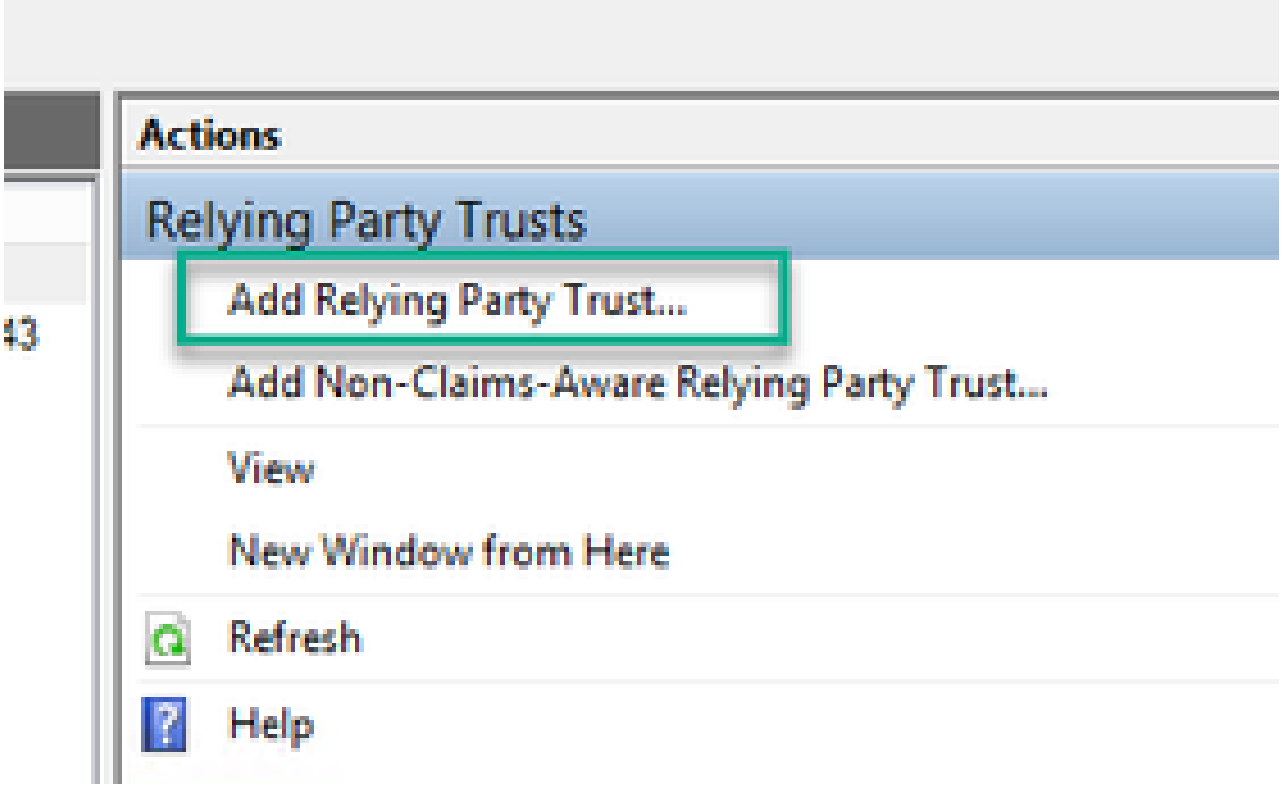
2. Ouvrez la console de gestion AD FS, qui est généralement accessible via le Gestionnaire de serveur.



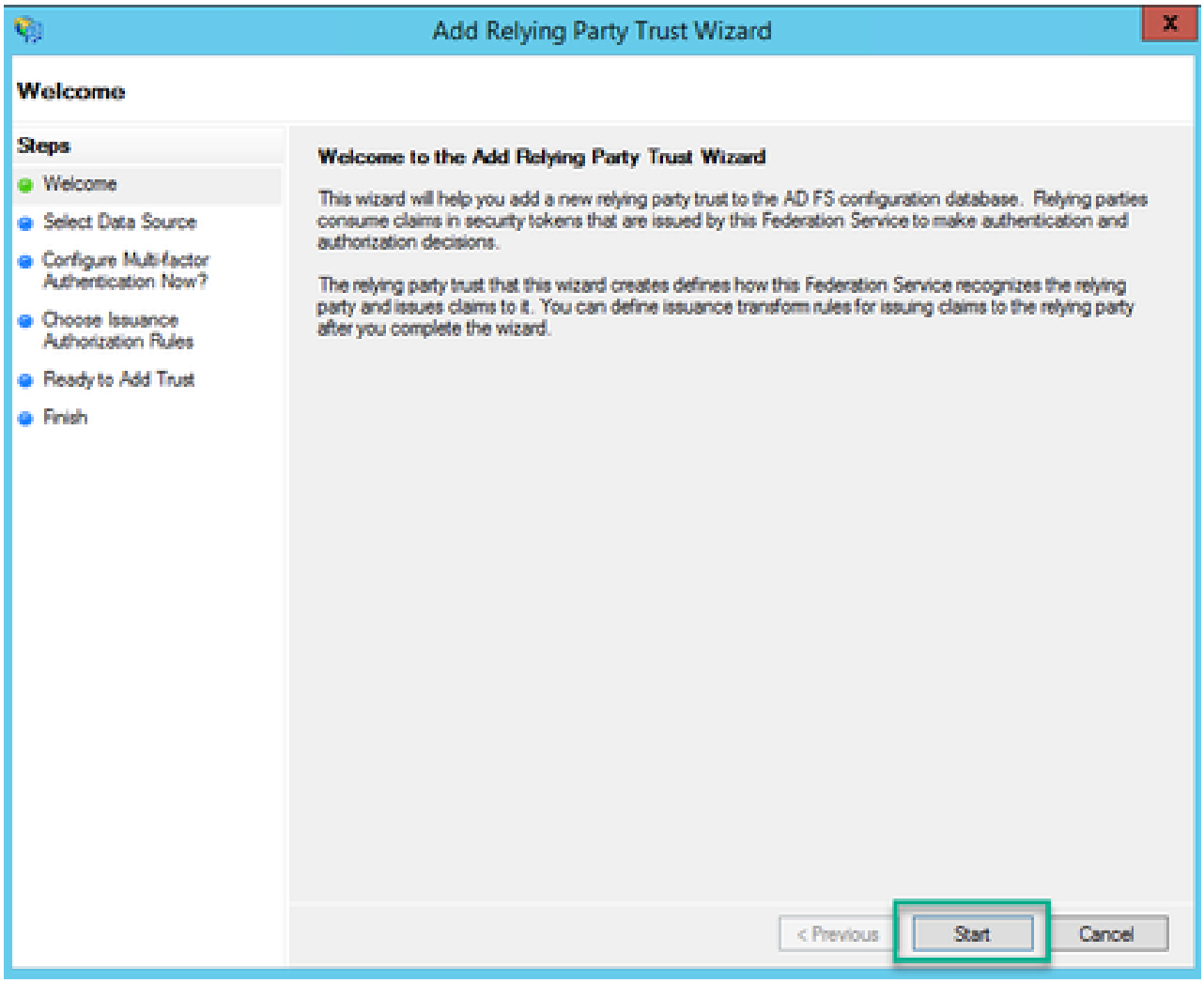
3. Une fois dans la console de gestion ADFS, accédez à ADFS > Relations d'approbation > Approbation de la partie de confiance dans le volet de gauche.



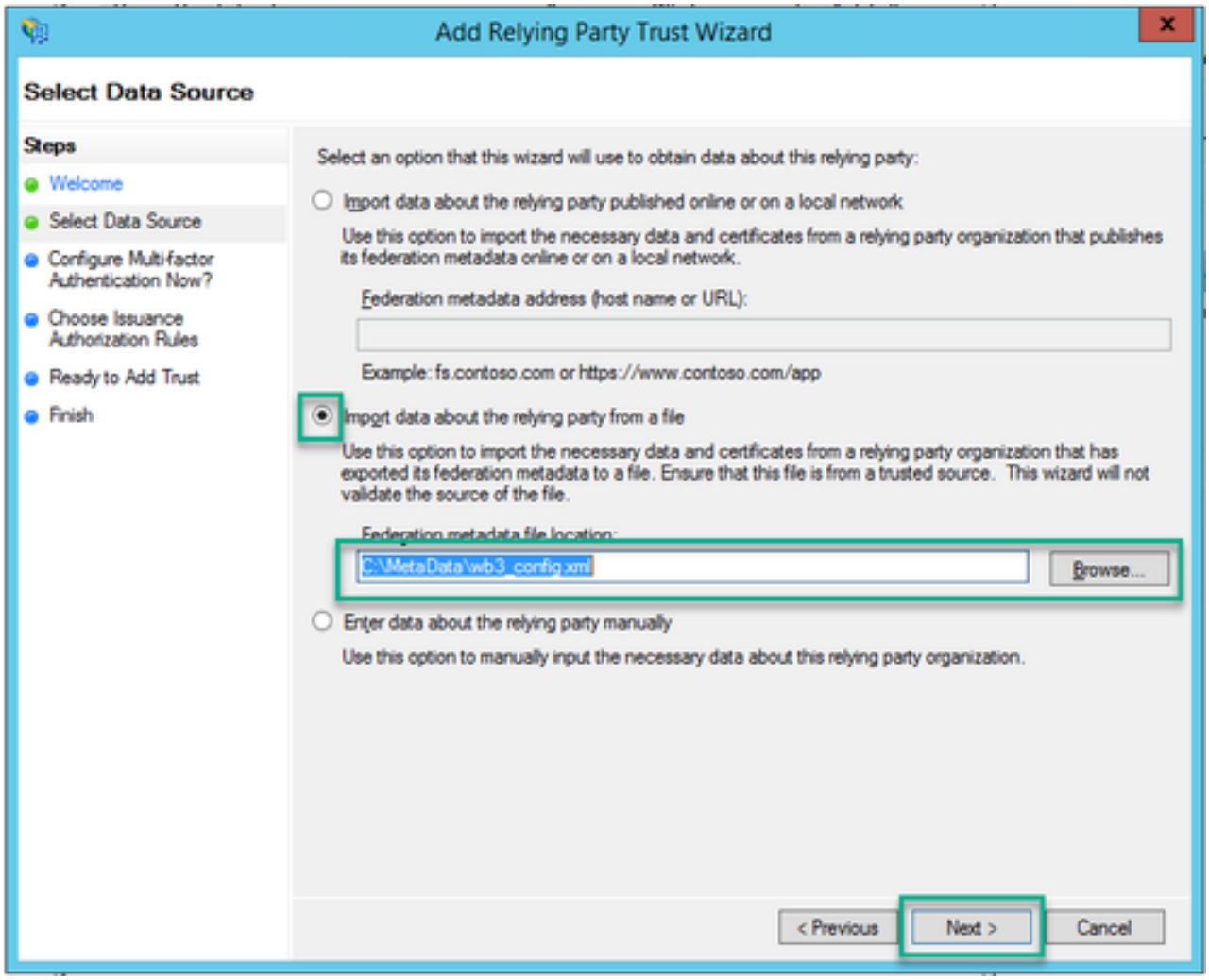
4. Dans le volet droit de la console de gestion ADFS, sélectionnez l'option Ajouter une approbation de partie de confiance... de l'assistant.



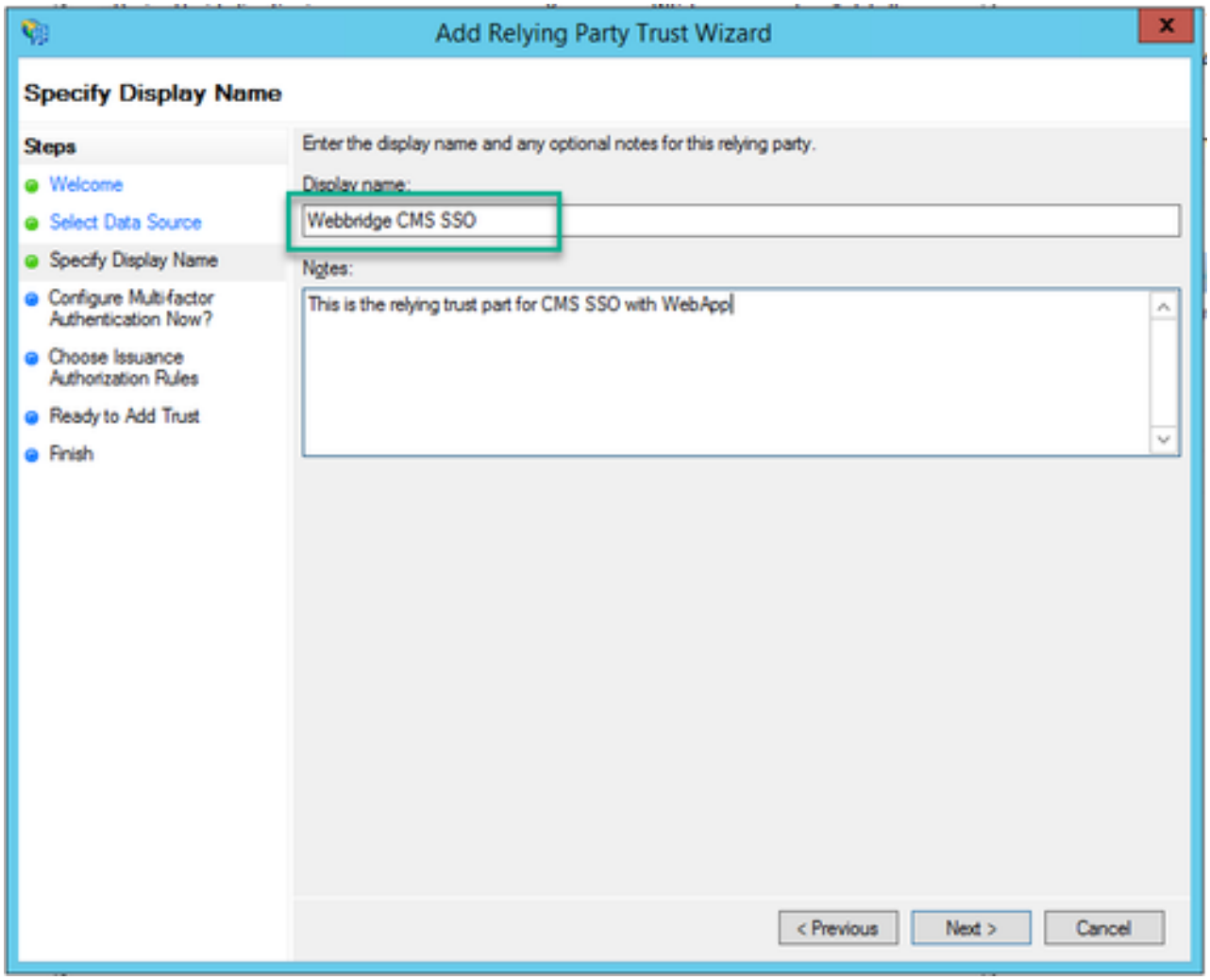
5. Après avoir effectué cette sélection, l'Assistant Ajout d'approbation de partie de confiance s'ouvre. Sélectionnez l'option Start.



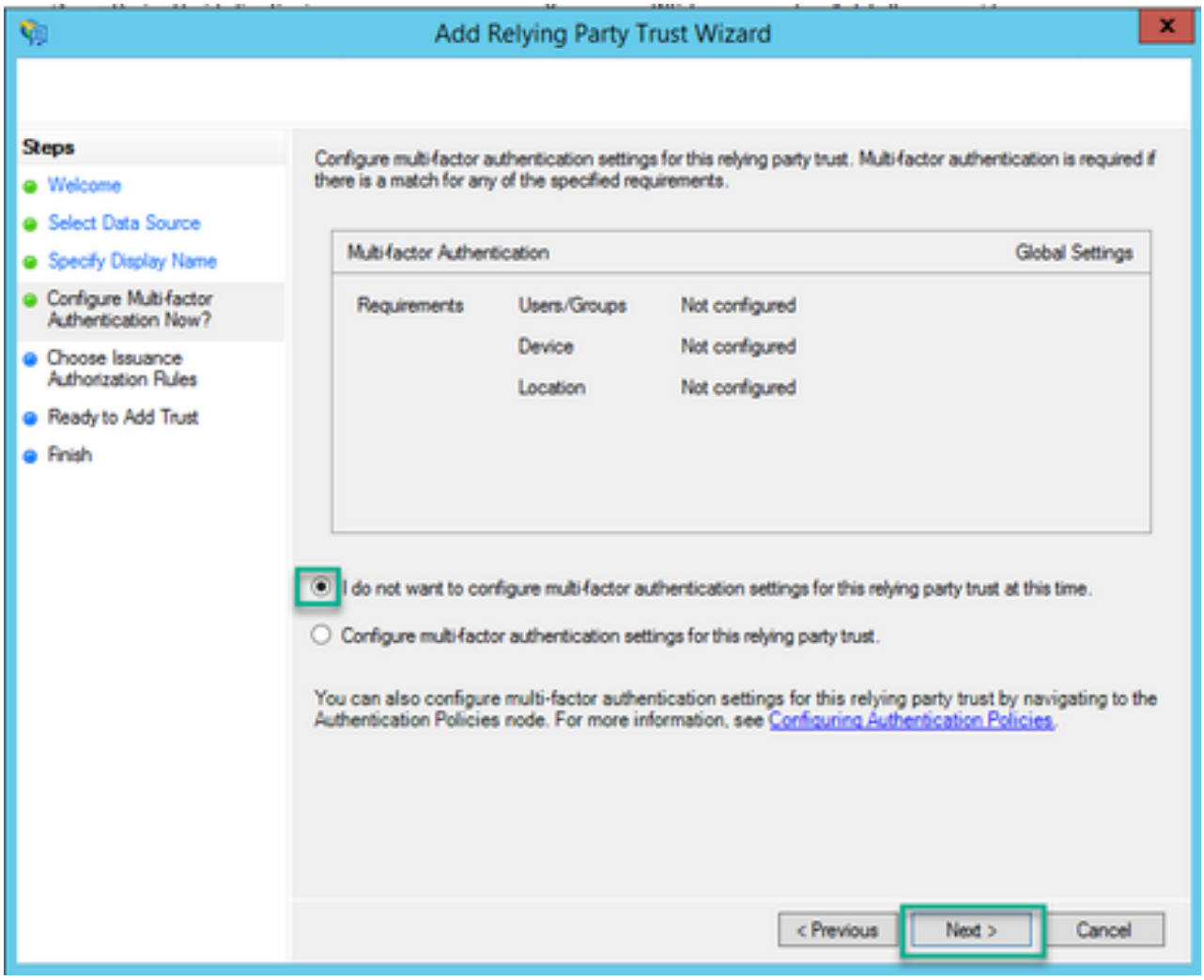
6. Sur la page Sélectionner la source de données, sélectionnez la case d'option Importer les données relatives à la partie de confiance à partir d'un fichier et sélectionnez Parcourir et accédez à l'emplacement du fichier de métadonnées Webbridge.



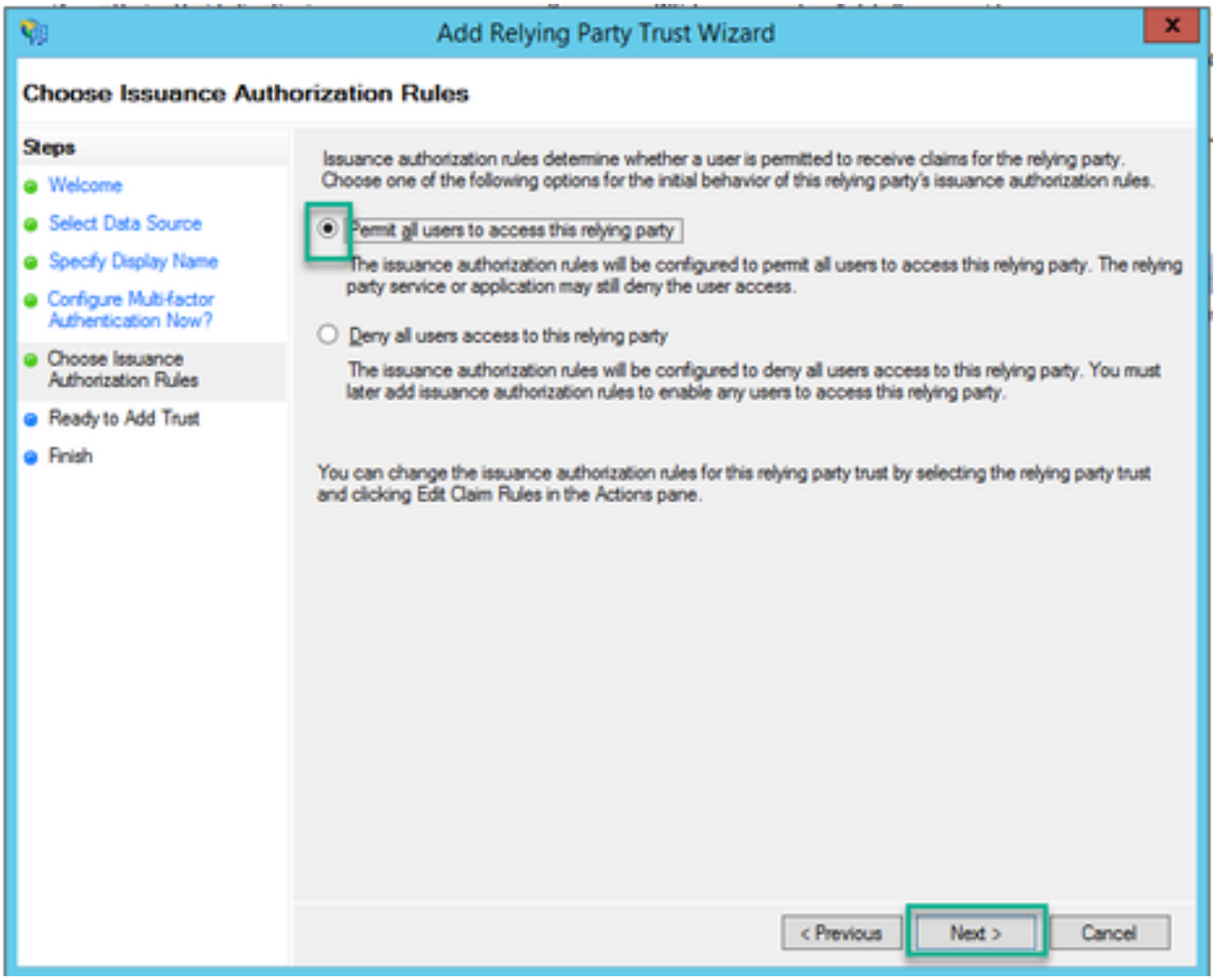
7. Sur la page Spécifier le nom d'affichage, entrez un nom à afficher pour l'entité dans ADFS (le nom d'affichage n'est pas un rôle de serveur pour la communication ADFS et est purement informatif).



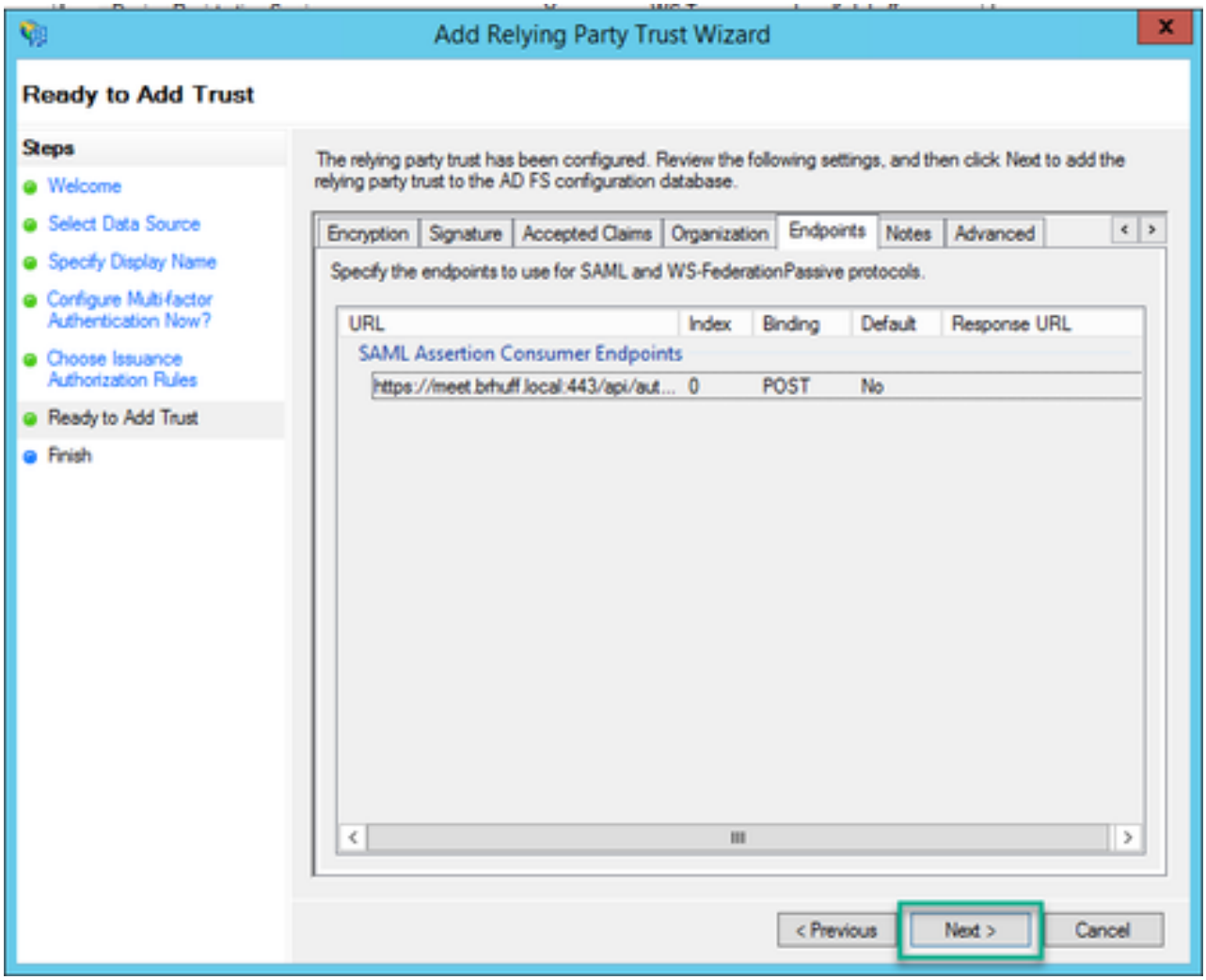
8. Dans la section Configurer l'authentification multifacteur maintenant ? , conservez la valeur par défaut et sélectionnez Suivant.



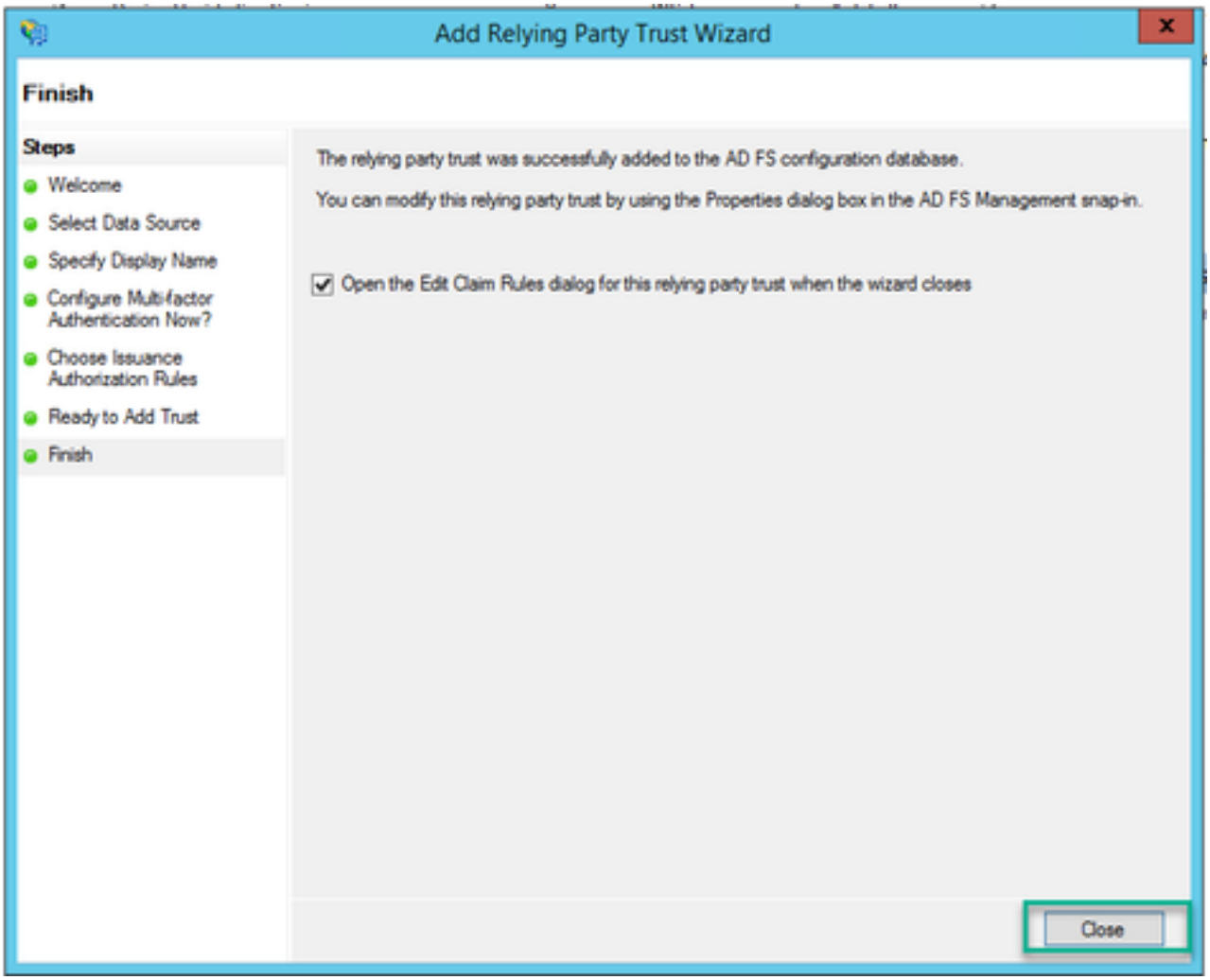
9. Sur la page Choisir des règles d'autorisation d'émission, laissez la case Autoriser tous les utilisateurs à accéder à cette partie de confiance sélectionnée.



10. Sur la page Prêt à ajouter une approbation, les détails importés de la partie d'approbation de confiance pour Webbridge peuvent être examinés à travers les onglets. Consultez les Identificateurs et les Terminaux pour les détails d'URL pour le fournisseur de service Webbridge.



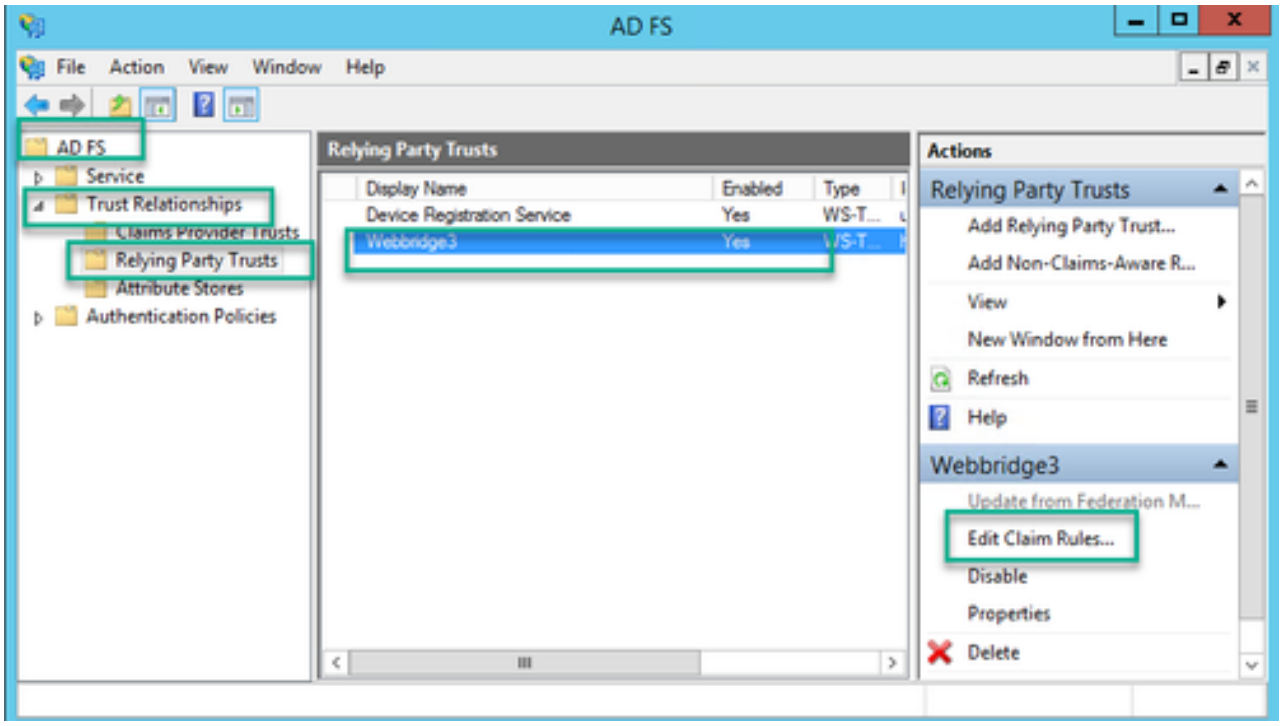
11. Sur la page Terminer, sélectionnez l'option Fermer pour fermer l'assistant et continuer à modifier les règles de réclamation.



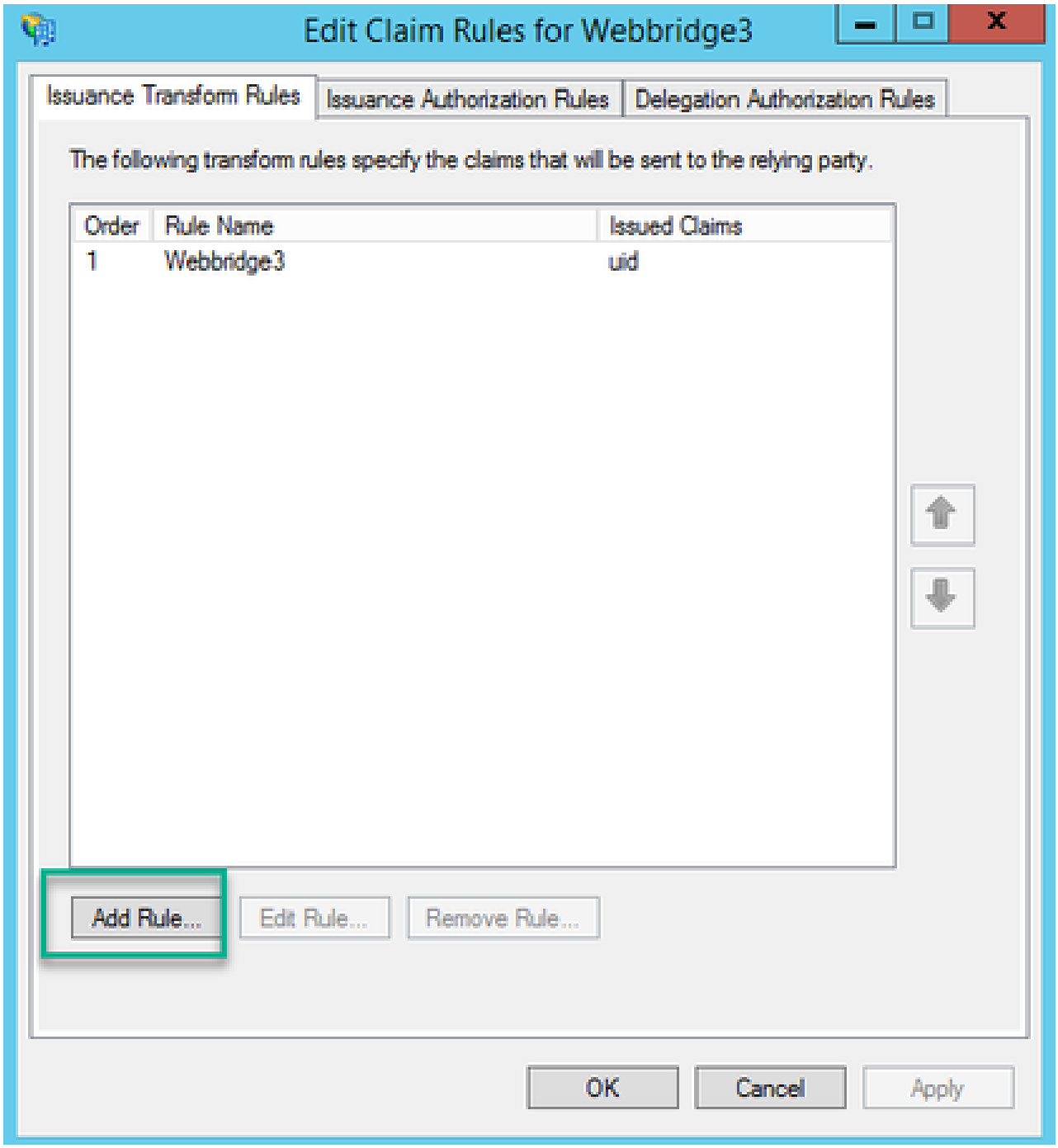
Créer des règles de demande pour le service Webbridge sur le fournisseur d'identité

Maintenant que l'approbation de la partie de confiance a été créée pour le Webbridge, des règles de revendication peuvent être créées pour faire correspondre des attributs LDAP spécifiques aux types de revendications sortantes à fournir au Webbridge dans la réponse SAML.

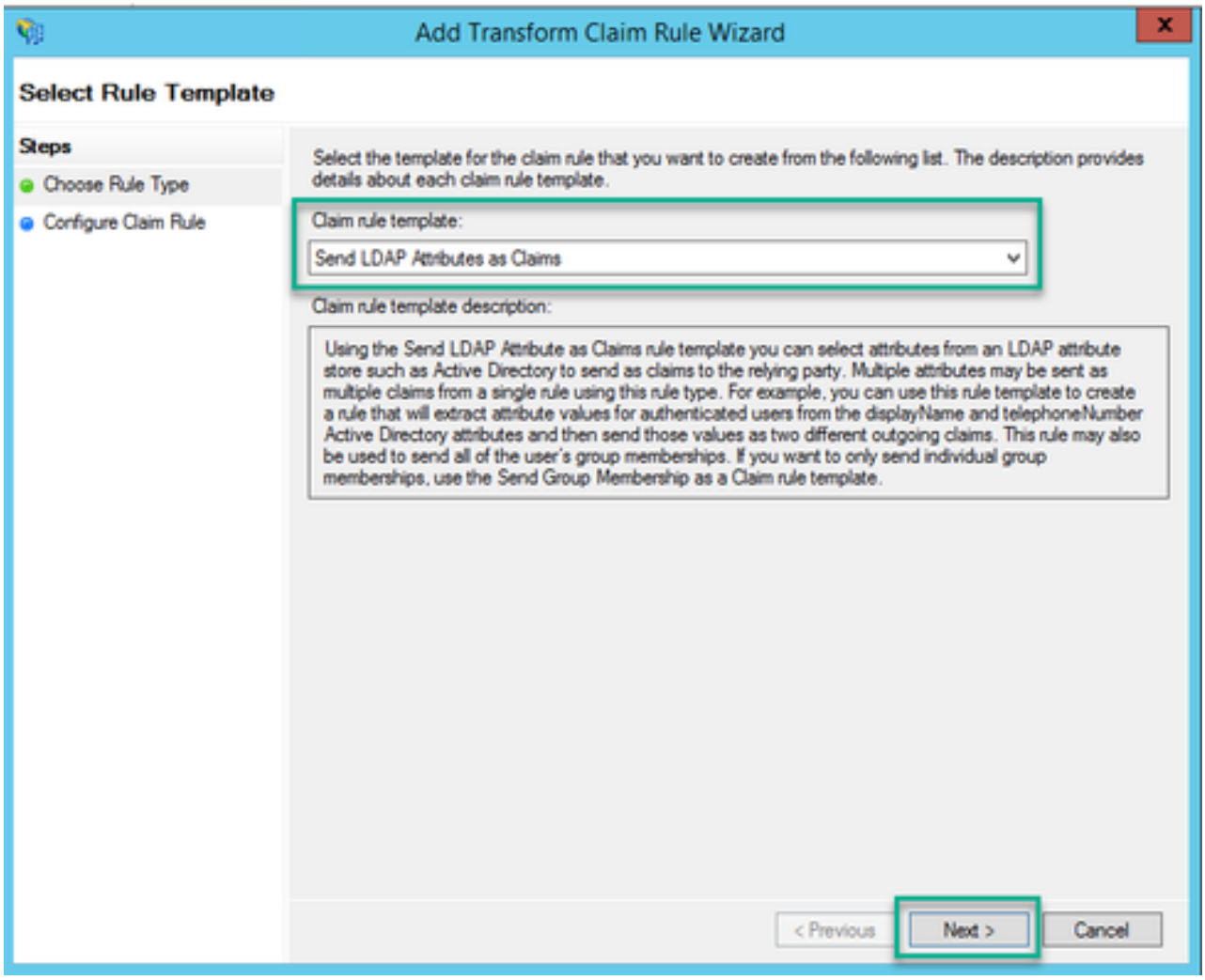
1. Dans la console de gestion ADFS, mettez en surbrillance l'approbation de la partie de confiance pour le Webbridge et sélectionnez Modifier les règles de revendication dans le volet droit.



2. Sur la page Modifier les règles de revendication pour <DisplayName>, sélectionnez Ajouter une règle....

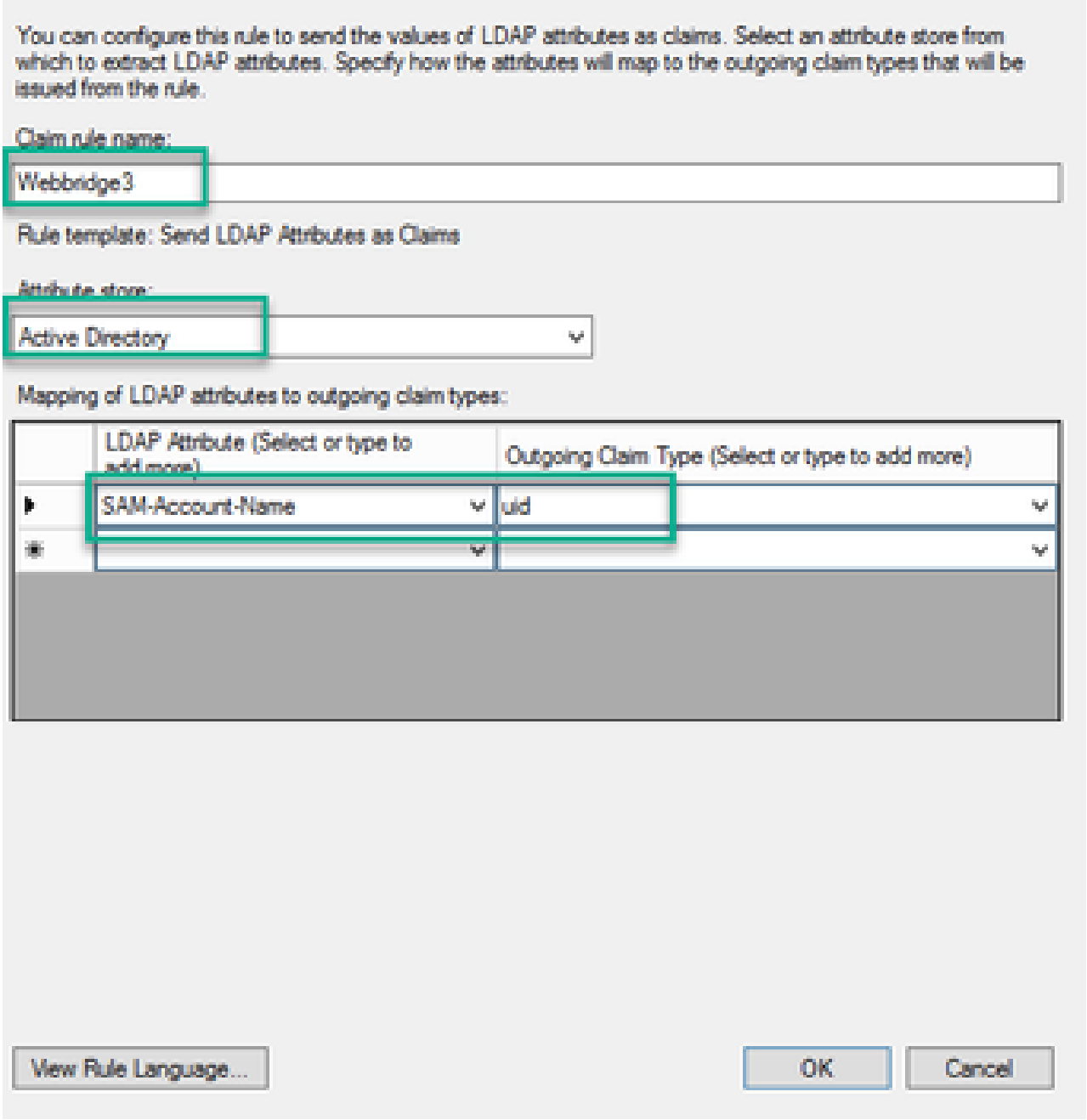


3. Sur la page Assistant Ajouter une règle de revendication de transformation, sélectionnez Envoyer les attributs LDAP en tant que revendications pour l'option de modèle de règle de revendication et sélectionnez Suivant.



4. Sur la page Configurer la règle de revendication, configurez la règle de revendication pour l'approbation de la partie de confiance avec les valeurs suivantes :

1. Nom de la règle de revendication = il doit s'agir d'un nom donné à la règle dans ADFS (pour référence à la règle uniquement)
2. Magasin d'attributs = Active Directory
3. Attribut LDAP = Il doit correspondre à l'authenticationIdMapping dans l'API Callbridge. (Par exemple, $sAMAccountName$.)
4. Type de revendication sortante = Il doit correspondre à authenticationIdMapping dans le fichier Webbridge SSO config.json. (Par exemple, uid.)



Créer un fichier ZIP d'archivage SSO pour Webbridge :

Cette configuration est celle que Webbridge référence pour valider la configuration SSO pour les domaines pris en charge, le mappage d'authentification, etc. Ces règles doivent être prises en compte pour cette partie de la configuration :

- Le fichier ZIP DOIT commencer par sso_ préfixé au nom du fichier (par exemple, sso_cmstest.zip).
- Une fois ce fichier téléchargé, Webbridge désactive l'authentification de base et SEUL SSO peut être utilisé pour le Webbridge sur lequel il a été téléchargé.

- Si plusieurs fournisseurs d'identité sont utilisés, un fichier ZIP séparé doit être téléchargé avec un schéma d'attribution de noms différent (toujours précédé du sso_).
- Lors de la création du fichier zip, veillez à mettre en surbrillance et à zipper le contenu du fichier et ne placez pas les fichiers requis dans un dossier et zippez ce dossier.

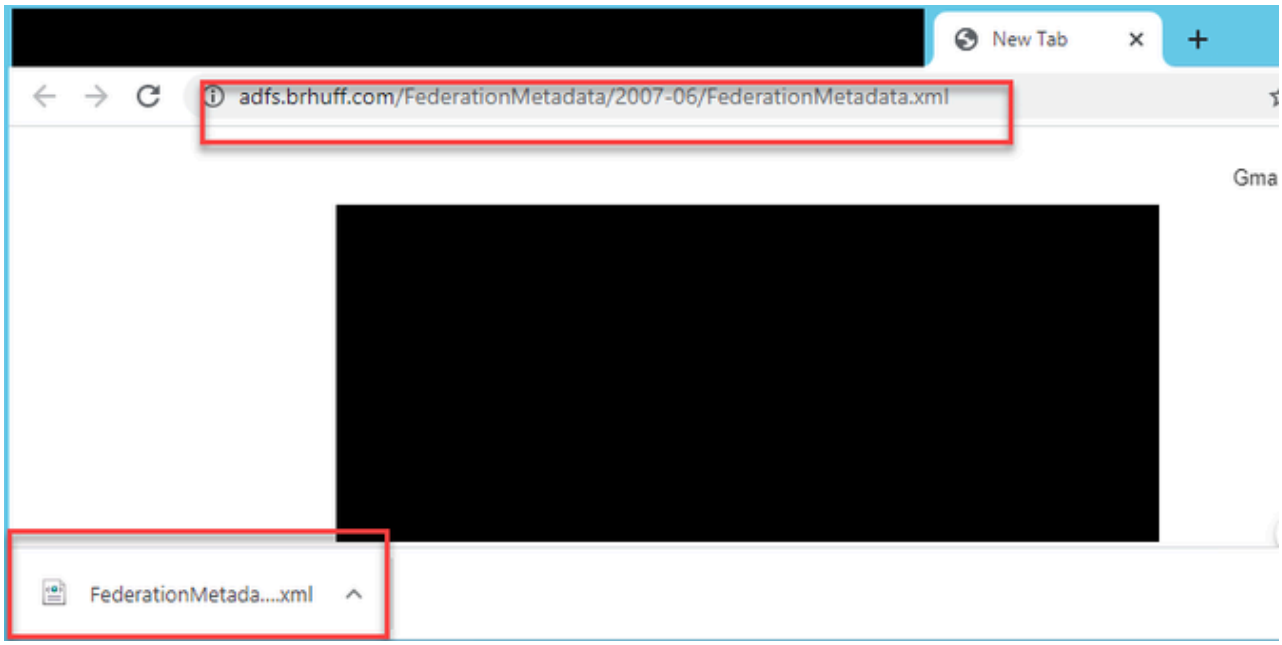
Le contenu du fichier zip est composé de 2 à 4 fichiers, selon que le chiffrement est utilisé ou non.

Nom du fichier	Description	Requis ?
idp_config.xml	Il s'agit du fichier MetaData qui peut être collecté par l'idP. Dans ADFS, vous pouvez le localiser en accédant à https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml.	OUI
config.json	Il s'agit du fichier JSON dans lequel Webbridge utilise pour valider les domaines pris en charge, le mappage d'authentification pour SSO.	OUI
sso_sign.key	Il s'agit de la clé privée de la clé de signature publique configurée sur le fournisseur d'identification. Uniquement nécessaire pour sécuriser les données signées	NON
sso_encrypt.key	Il s'agit de la clé privée de la clé de chiffrement publique configurée sur le fournisseur d'identification. Nécessaire uniquement pour sécuriser les données chiffrées	NON

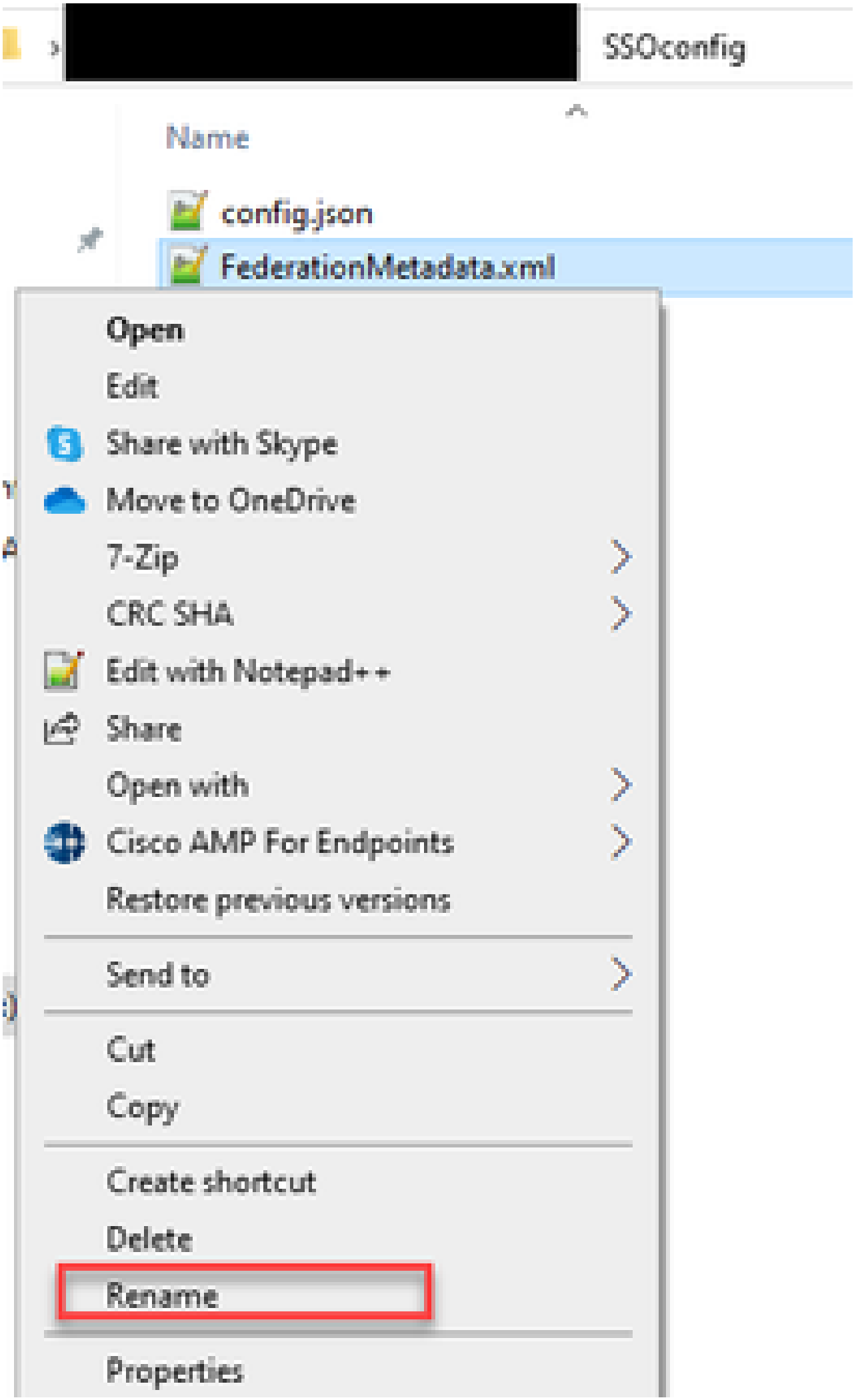
Obtenir et configurer le fichier idp_config.xml

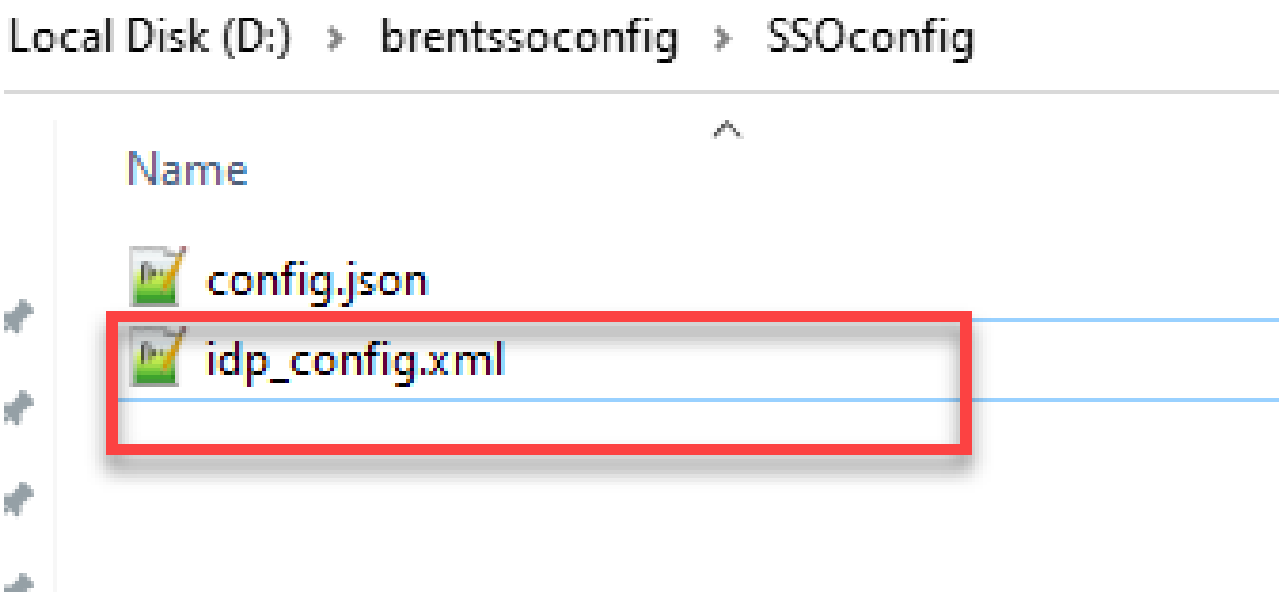
1. Sur le serveur ADFS (ou à un emplacement ayant accès à ADFS), ouvrez un navigateur Web.

2. Dans le navigateur Web, saisissez l'URL suivante : https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml (Vous pouvez également utiliser localhost à la place du nom de domaine complet si vous vous trouvez localement sur le serveur ADFS). Le fichier FederationMetadata.xml est téléchargé.



3. Copiez le fichier téléchargé à un emplacement où le fichier zip est en cours de création et renommez-le en idp_config.xml.

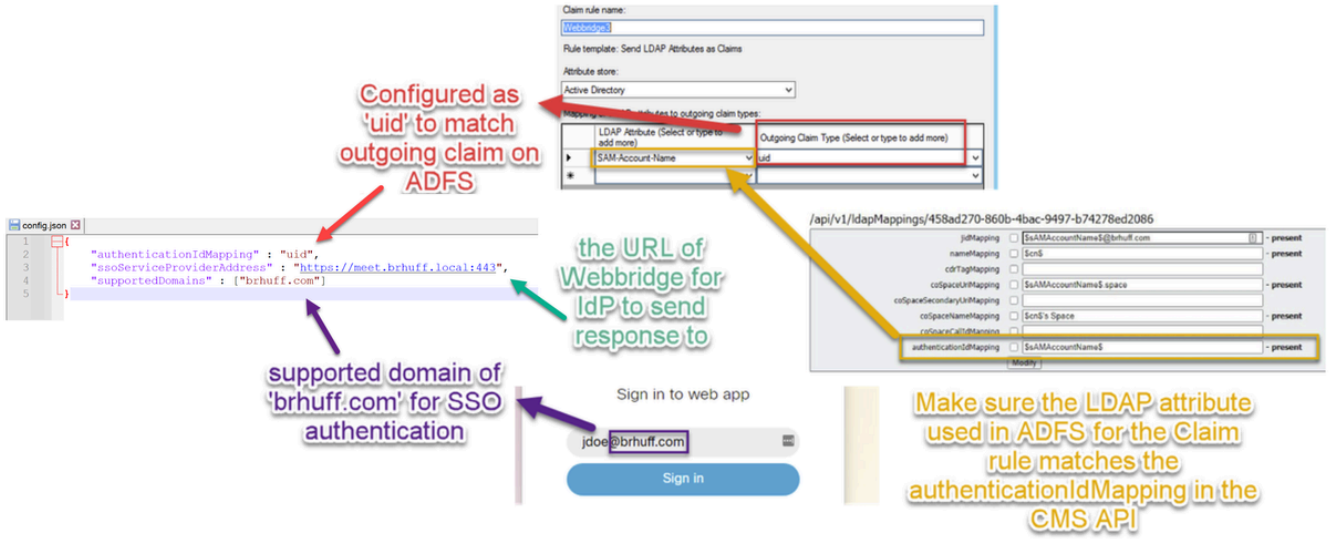

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



Créez le fichier config.json avec son contenu

Le fichier config.json contient ces 3 attributs et ils doivent être contenus entre crochets, { }:

1. supportedDomains : liste des domaines pour lesquels l'authentification SSO est vérifiée par rapport au fournisseur d'identité. Plusieurs domaines peuvent être séparés par une virgule.
2. authenticationIdMapping - Il s'agit du paramètre qui est transmis en tant que partie de la règle de revendication sortante depuis ADFS/IdP. Cela doit correspondre à la valeur du nom du type de revendication sortante sur le fournisseur d'identité. Règle de demande.
3. ssoServiceProviderAddress : il s'agit de l'URL FQDN à laquelle le fournisseur d'identification envoie les réponses SAML. Il doit s'agir du nom de domaine complet Webbridge.

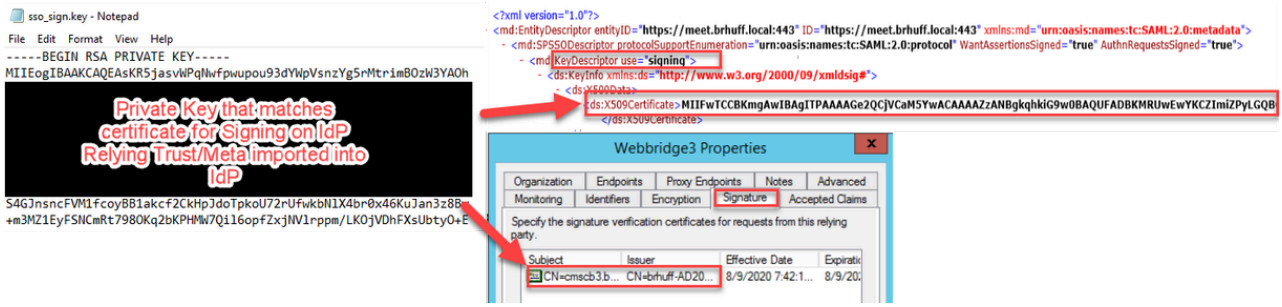


Définissez sso_sign.key (FACULTATIF)

Ce fichier doit contenir la clé privée du certificat utilisé pour signer les métadonnées Webbridge qui ont été importées dans le fournisseur d'identité. Le certificat utilisé pour la signature peut être défini lors de l'importation des métadonnées Webbridge dans ADFS en renseignant le X509Certificate avec les informations de certificat sous la section <KeyDescriptor use=signing>. Il peut également être affiché (et importé) sur ADFS dans la partie Webbridge Relying Trust sous Properties > Signature.

Dans l'exemple suivant, vous pouvez voir le certificat de pont d'appel (CN=cmscb3.brhuff.local), qui a été ajouté aux métadonnées Webbridge avant d'être importé dans ADFS. La clé privée insérée dans le sso_sign.key est celle qui correspond au certificat cmscb3.brhuff.local.

Cette configuration est facultative et n'est nécessaire que si vous prévoyez de chiffrer les réponses SAML.



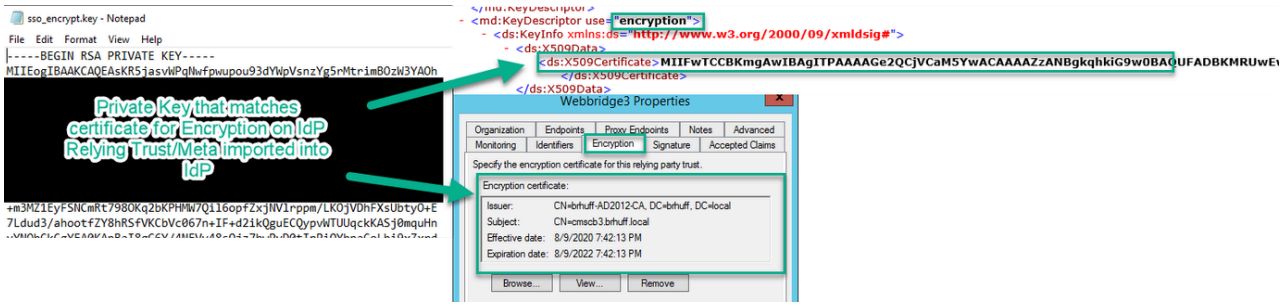
Définissez le fichier sso_encrypt.key (FACULTATIF)

Ce fichier doit contenir la clé privée du certificat utilisé pour le chiffrement dans les métadonnées du pont Web qui ont été importées dans le fournisseur d'identité. Le certificat utilisé pour le chiffrement peut être défini lors de l'importation des métadonnées Webbridge dans ADFS en

renseignant le X509Certificate avec les informations de certificat sous la section <KeyDescriptor use=encryption>. Il peut également être affiché (et importé) sur ADFS dans la partie Webbridge Relying Trust sous Properties > Encryption.

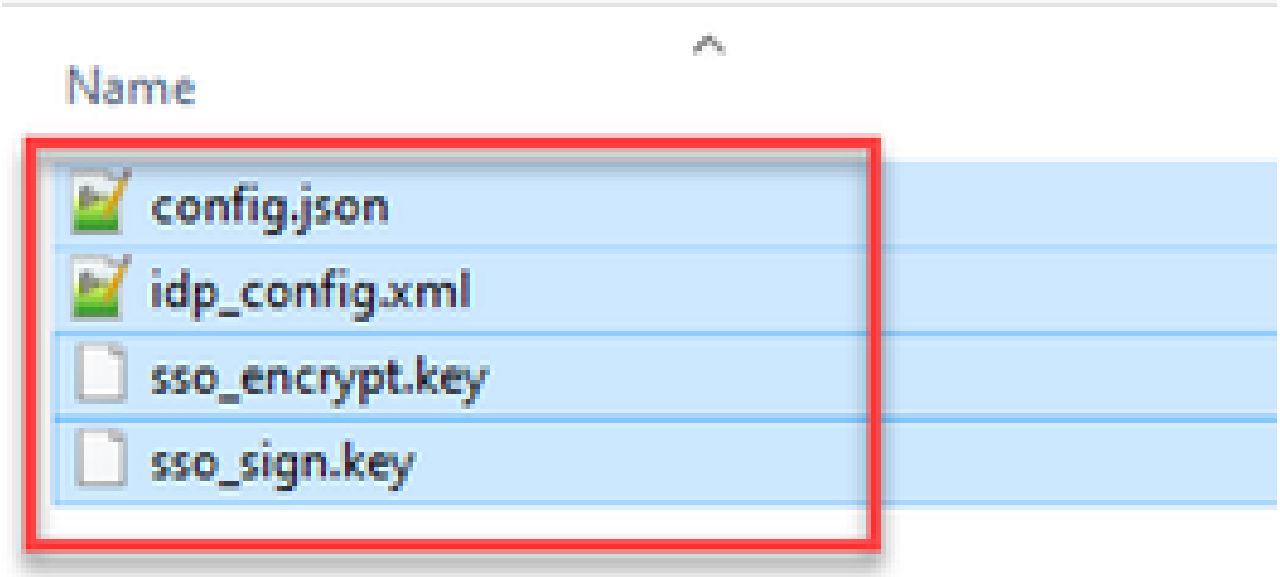
Dans l'exemple suivant, vous pouvez voir le certificat de pont d'appel (CN=cmscb3.brhuff.local), qui a été ajouté aux métadonnées Webbridge avant d'être importé dans ADFS. La clé privée insérée dans le fichier « sso_encrypt.key » correspond au certificat cmscb3.brhuff.local.

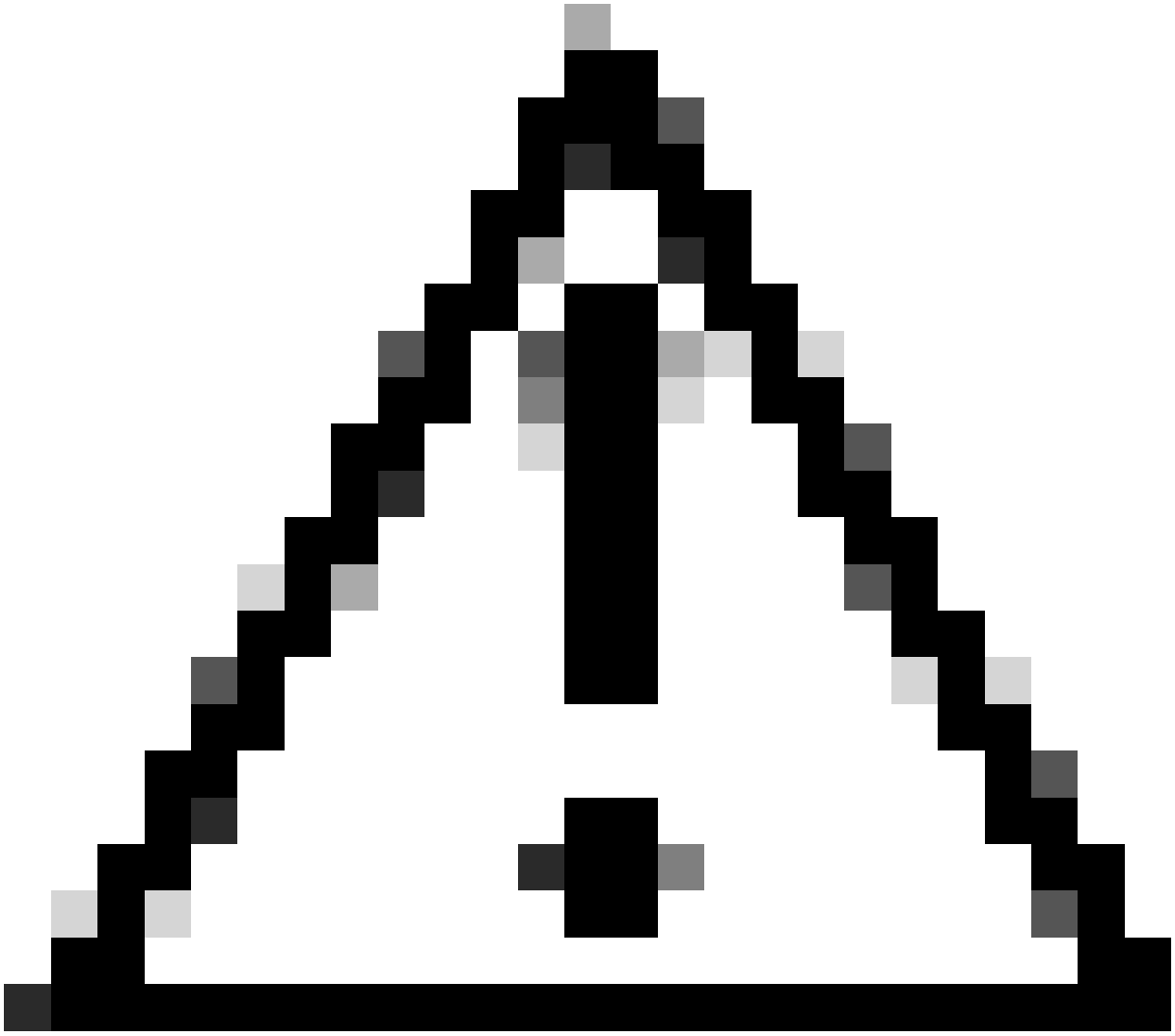
Cette configuration est facultative et n'est nécessaire que si vous avez l'intention de chiffrer les réponses SAML.



Création du fichier ZIP SSO

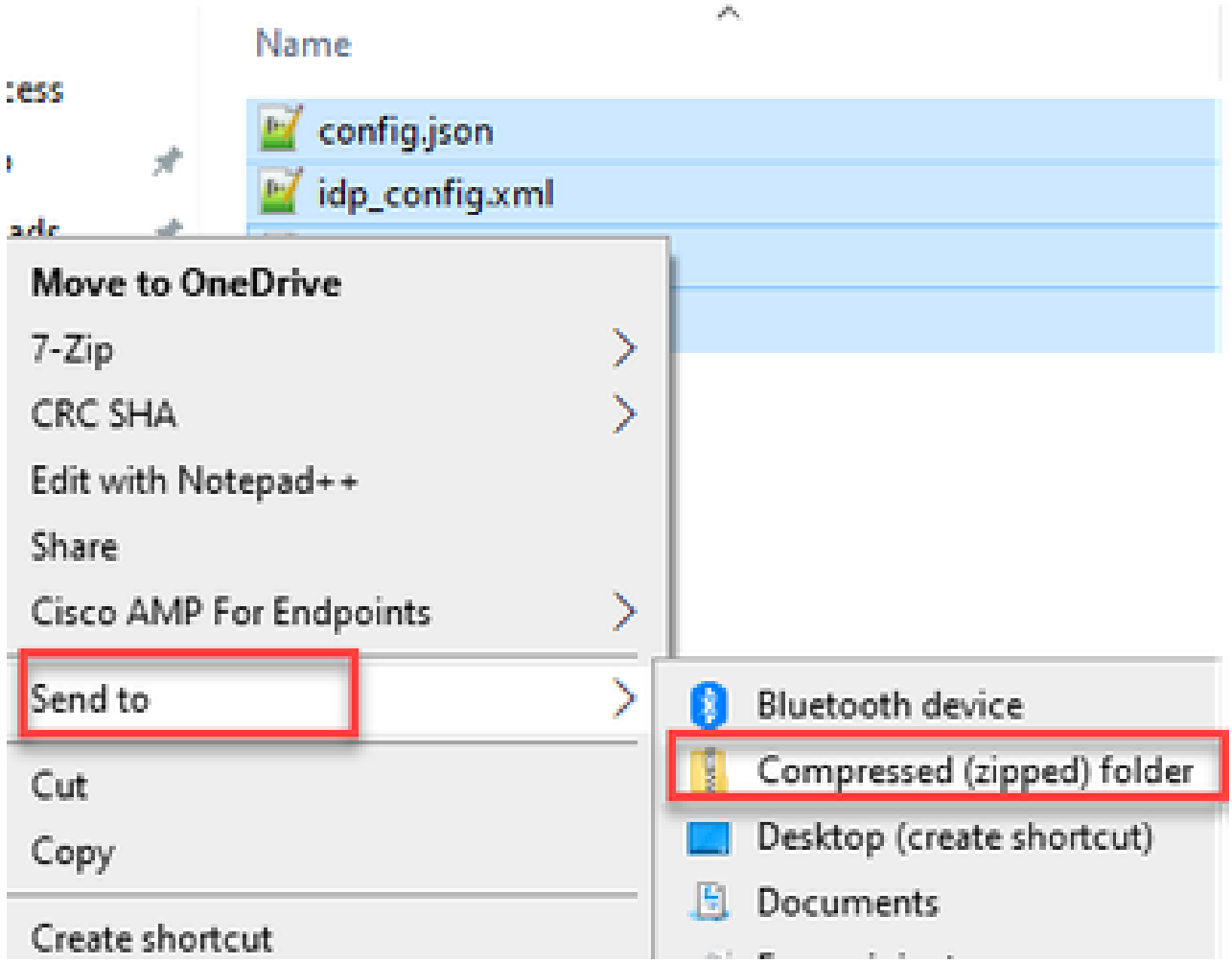
1. Mettez en surbrillance tous les fichiers destinés à être utilisés pour le fichier de configuration SSO.



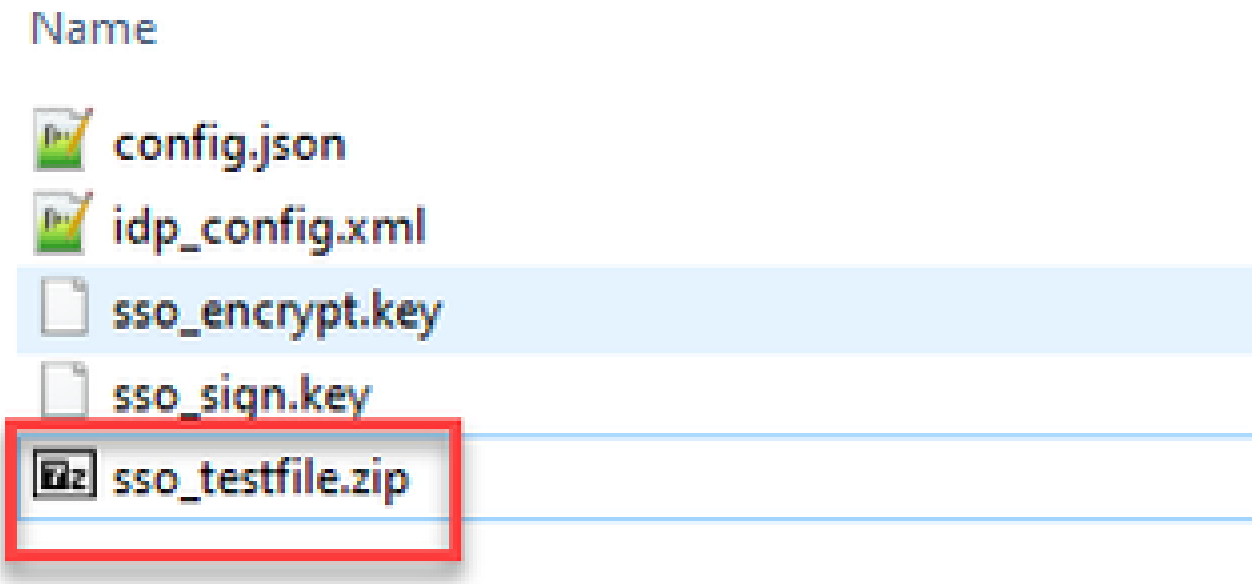


Mise en garde : Ne zippez pas le dossier contenant les fichiers, car l'authentification unique ne fonctionne pas.

2. Cliquez avec le bouton droit sur les fichiers en surbrillance et sélectionnez Envoyer à > Compressé (zippé) dossier.



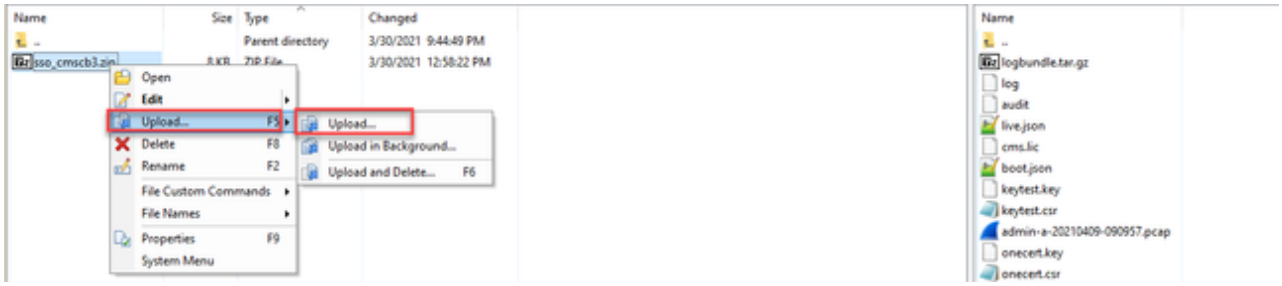
3. Une fois les fichiers compressés, renommez-les au nom souhaité avec le préfixe sso_ :



Télécharger le ou les fichiers Zip SSO sur Webbridge

Ouvrez un client SFTP/SCP, dans cet exemple WinSCP est utilisé, et connectez-vous au serveur hébergeant Webbridge3.

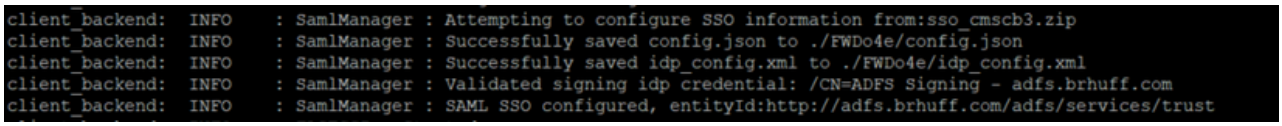
1. Dans le volet de gauche, naviguez jusqu'à l'emplacement dans lequel se trouve le fichier Zip SSO et cliquez avec le bouton droit de la souris sur télécharger ou faites glisser le fichier.



2. Une fois le fichier complètement téléchargé sur le serveur Webbridge3, ouvrez une session SSH et exécutez la commande webbridge3 restart.



3. Dans le journal système, ces messages indiquent que l'activation de l'authentification unique a réussi :



Carte d'accès commune (CAC)

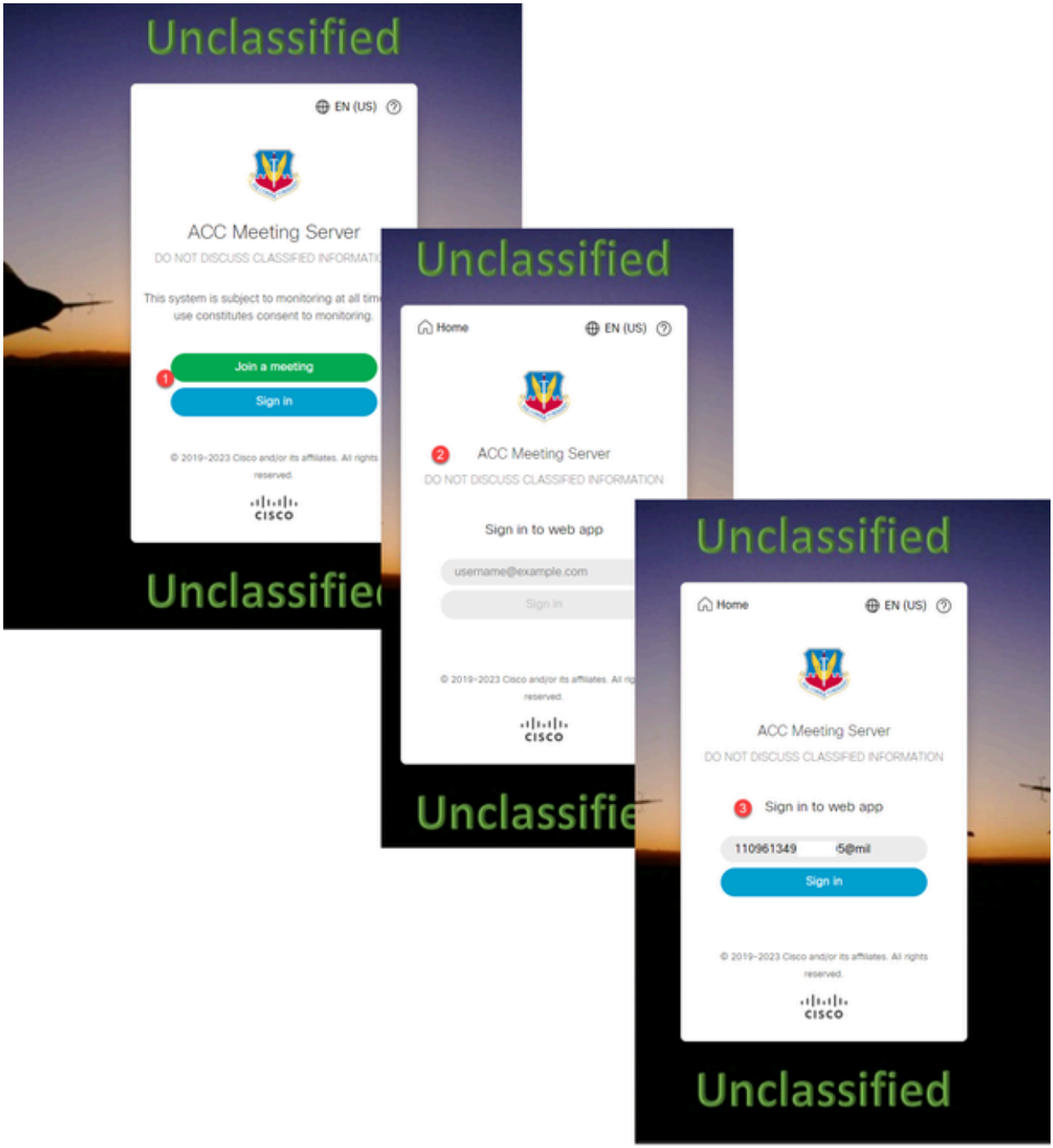
Une carte d'accès commune (CAC) est une carte à puce qui sert d'identification standard pour le personnel militaire en service actif, les employés civils du ministère de la Défense et le personnel de l'entrepreneur admissible.

Voici l'intégralité du processus de connexion pour les utilisateurs qui utilisent des cartes CAC :

1. Mettez le PC sous tension et insérez la carte CAC
2. Connectez-vous (sélectionnez un certificat parfois) et saisissez Pin
3. Ouvrir le navigateur
4. Accédez à l'URL de participation et consultez les options Participer à une téléconférence

ou Connexion

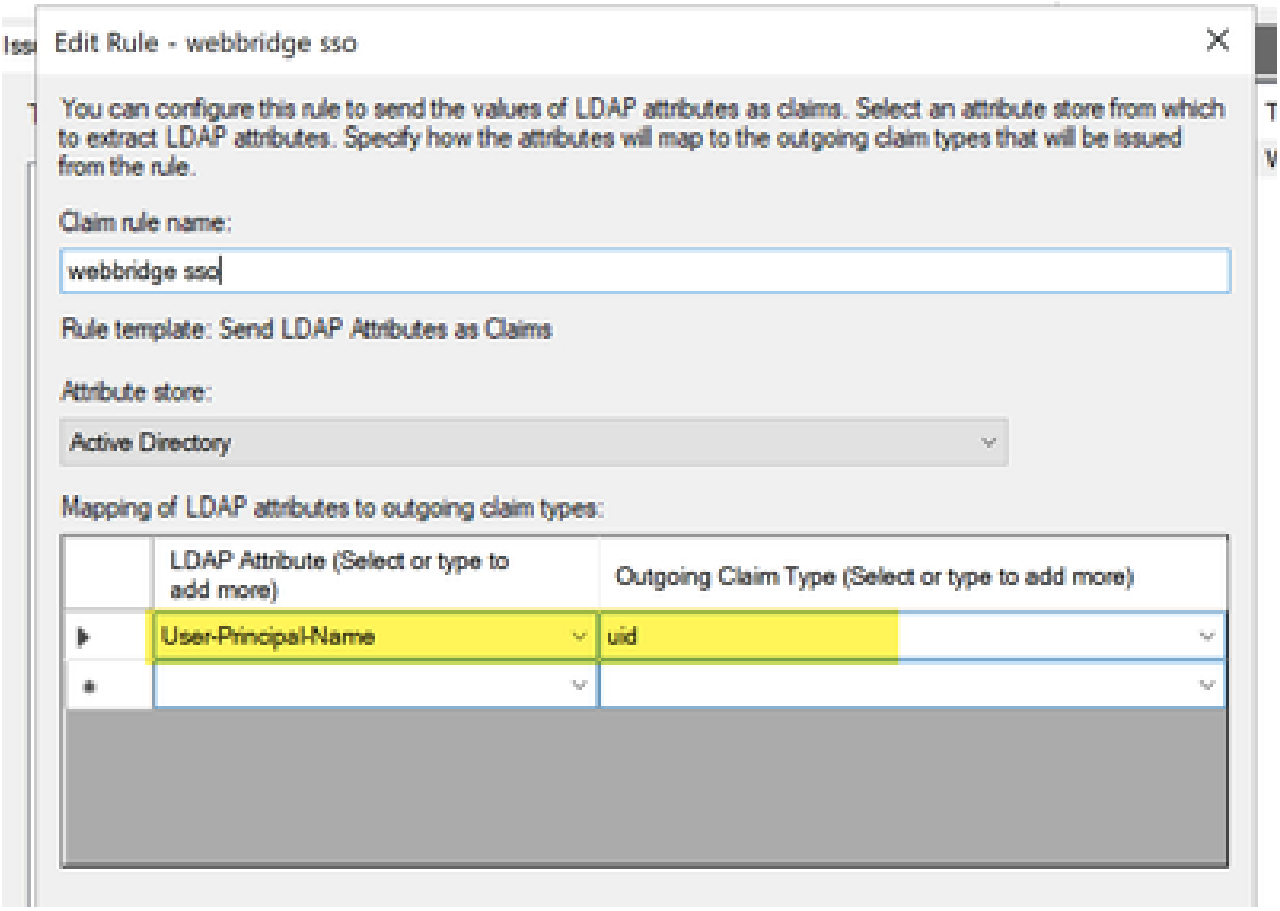
5. Se connecter : Entrez le nom d'utilisateur configuré comme jidMapping qu'Active Directory attend d'une connexion CAC
6. Appuyez sur Connexion
7. La page ADFS s'affiche brièvement et est remplie automatiquement
8. L'utilisateur est connecté à ce stade



Configurez jidMapping (il s'agit du nom de connexion des utilisateurs) dans Ldapmapping de la même manière que ce qu'ADFS utilise pour la carte CAC. $userPrincipalName$ par exemple (sensible à la casse)

Définissez également le même attribut LDAP pour authenticationIdMapping pour qu'il corresponde à l'attribut qui est utilisé dans la règle de revendication dans ADFS.

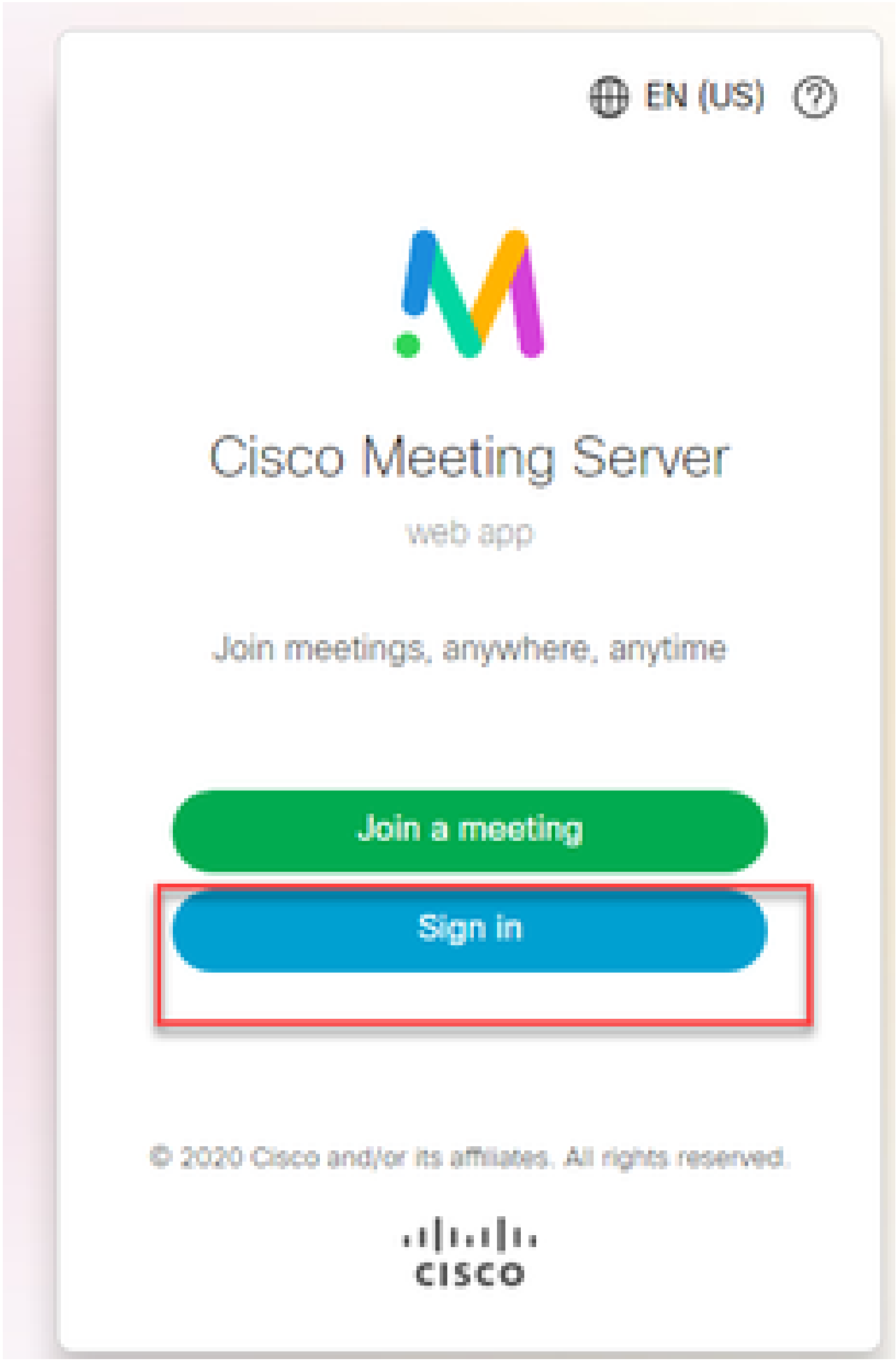
Ici, la règle de revendication indique qu'elle va renvoyer $userPrincipalName$ à CMS en tant qu'UID.



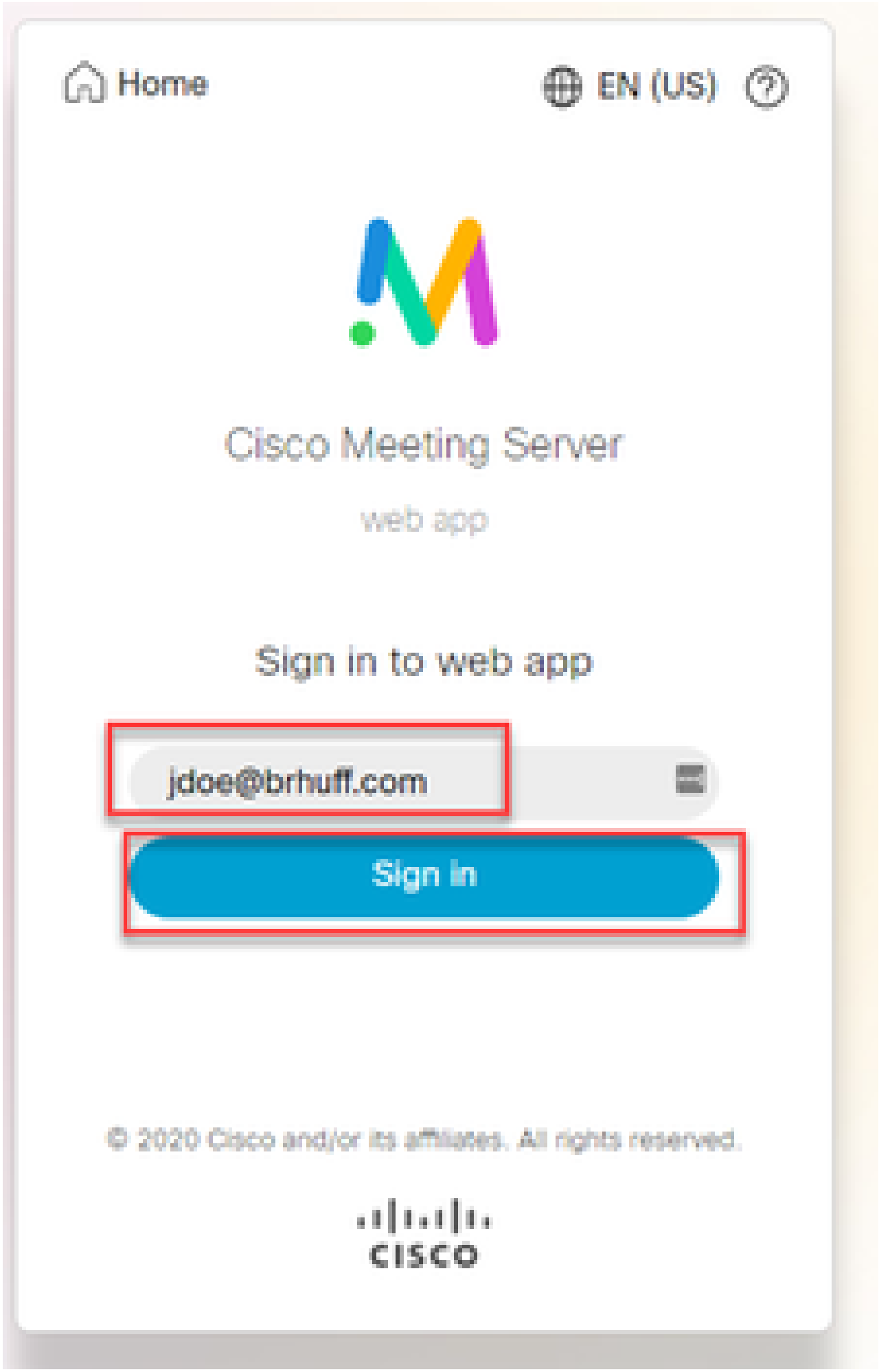
Test de la connexion SSO via WebApp

Maintenant que l'authentification unique a été configurée, vous pouvez tester le serveur :

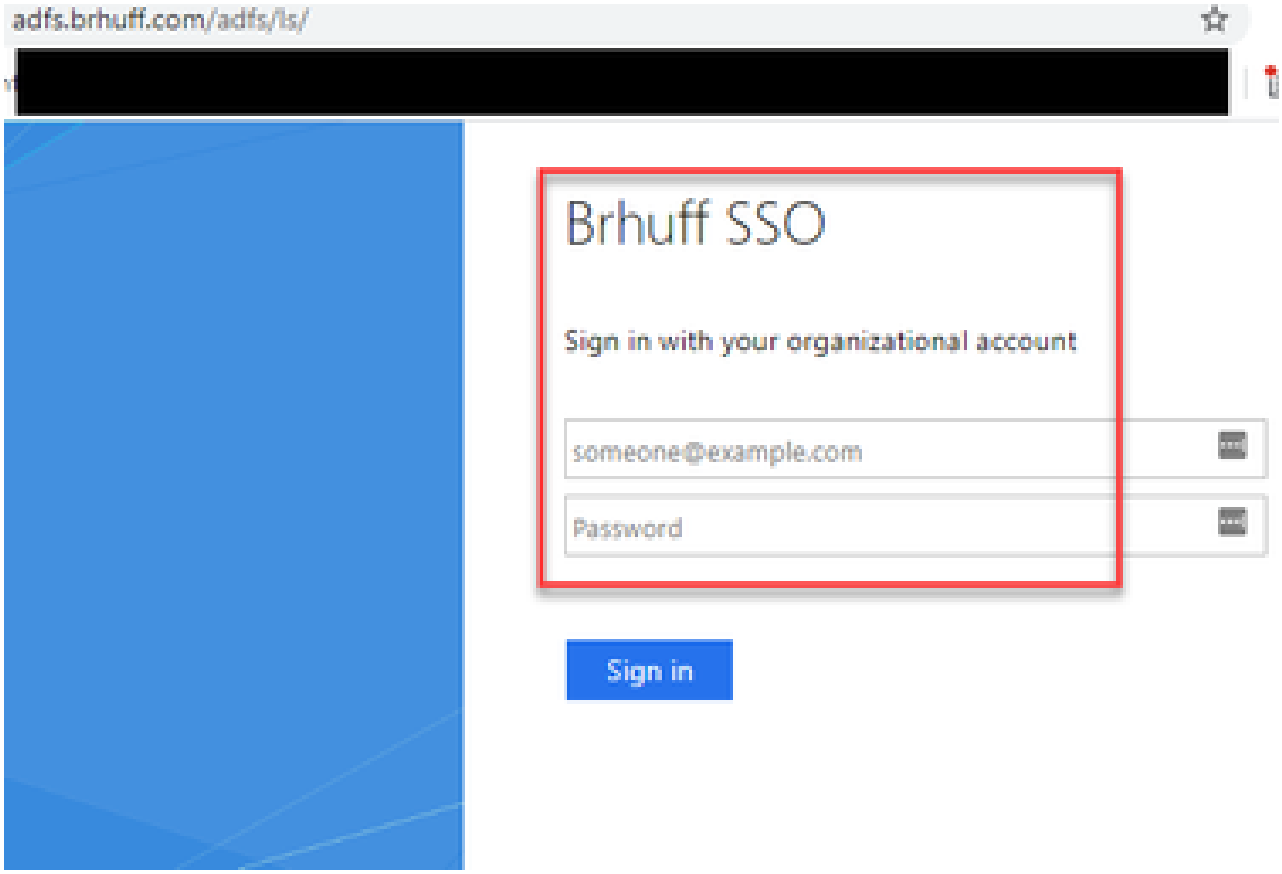
1. Accédez à l'URL de Webbridge pour l'application Web et sélectionnez le bouton Connexion.


EN (US)
Cisco Meeting Server
web app
Join meetings, anywhere, anytime
Join a meeting
Sign in
© 2020 Cisco and/or its affiliates. All rights reserved.
cisco

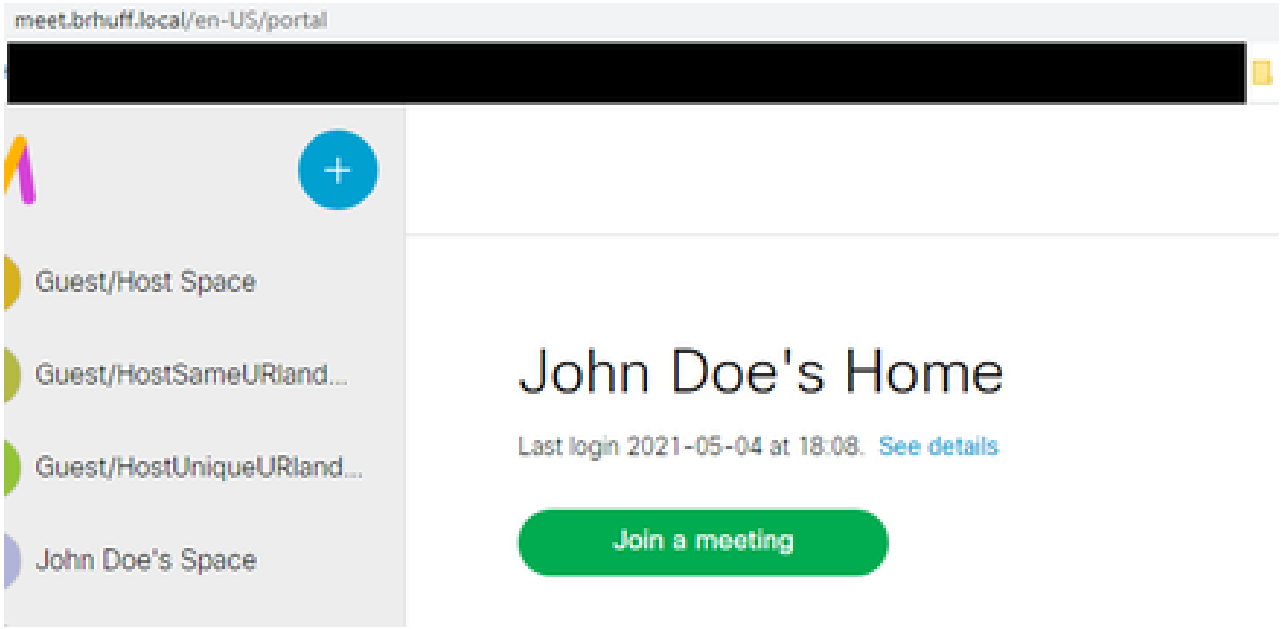
2. L'utilisateur a la possibilité de saisir son nom d'utilisateur (notez l'option no password sur cette page).


Home
EN (US)
Cisco Meeting Server
web app
Sign in to web app
jdoe@brhuff.com
Sign in
© 2020 Cisco and/or its affiliates. All rights reserved.
CISCO

3. L'utilisateur est ensuite redirigé vers la page ADFS (après avoir saisi les détails de l'utilisateur) où il doit saisir ses informations d'identification pour s'authentifier auprès d'IdP.



4. Après avoir saisi et validé les informations d'identification avec le fournisseur d'identité, l'utilisateur est redirigé avec le jeton pour accéder à la page d'accueil de Web App :



Dépannage

Dépannage de base

Pour le dépannage de base de tout problème SSO :

1. Assurez-vous que les métadonnées construites pour le Webbridge3 utilisé pour importer en tant qu'approbation de confiance dans IdP sont configurées correctement et que l'URL configurée correspond exactement à ssoServiceProviderAddress dans le fichier config.json.
2. Assurez-vous que les métadonnées fournies par le fournisseur d'identités et compressées dans le fichier de configuration Webbridge3 sont les dernières en date du fournisseur d'identités, comme si des modifications avaient été apportées au nom d'hôte du serveur, aux certificats, etc., elles doivent être réexportées et compressées dans le fichier de configuration.
3. Si vous utilisez des clés privées de signature et de chiffrement pour chiffrer des données, assurez-vous que les clés correspondantes correctes font partie du fichier sso_xxxx.zip que vous avez téléchargé sur webbridge. Si possible, essayez de tester sans les clés privées facultatives pour voir si SSO fonctionne sans cette option chiffrée.
4. Assurez-vous que le fichier config.json est configuré avec les détails corrects pour les domaines SSO, l'URL Webbridge3 ET le mappage d'authentification attendu pour correspondre à partir de SAMLResponse.

Il serait également idéal de tenter le dépannage du point de vue du journal :

1. Lorsque vous accédez à l'URL de Webbridge, placez ?trace=true à la fin de l'URL pour activer une journalisation détaillée sur le syslog CMS. (ex : https://join.example.com/en-US/home?trace=true).
2. Exécutez la commande syslog follow sur le serveur Webbridge3 pour capturer en direct pendant le test ou exécutez le test avec l'option trace ajoutée à l'URL et collectez le fichier logbundle.tar.gz à partir des serveurs Webbridge3 et CMS Callbridge. Si webbridge et callbridge sont sur le même serveur, cela ne nécessite que le seul fichier logbundle.tar.gz.

Codes d'échec Microsoft ADFS

Parfois, il y a un échec pour le processus SSO qui peut entraîner un échec pour la configuration de l'IdP ou sa communication avec l'IdP. Si vous utilisez le système ADFS, il serait idéal d'examiner la liaison suivante pour confirmer la défaillance observée et prendre des mesures

correctives :

Codes d'état Microsoft

En voici un exemple :

> client_backend : ERREUR : SamlManager : La demande d'authentification SAML _e135ca12-4b87-4443-abe1-30d396590d58 a échoué pour la raison suivante : urn:oasis:names:tc:SAML:2.0:status:Responder

Cette erreur indique que, selon la documentation précédente, l'échec s'est produit en raison du fournisseur d'identité ou du système ADFS et qu'il a donc été nécessaire que l'administrateur du système ADFS le traite pour le résoudre.

Impossible d'obtenir authenticationID

Il peut y avoir des cas dans lesquels pendant l'échange de SAMLResponse à partir de l'IdP, le Webbridge peut afficher ce message d'erreur dans les journaux avec un échec dans la connexion via SSO :

> client_backend : INFO : SamlManager : [57dff9e3-862e-4002-b4fa-683e4aa6922c] Échec de l'obtention d'un authenticationId

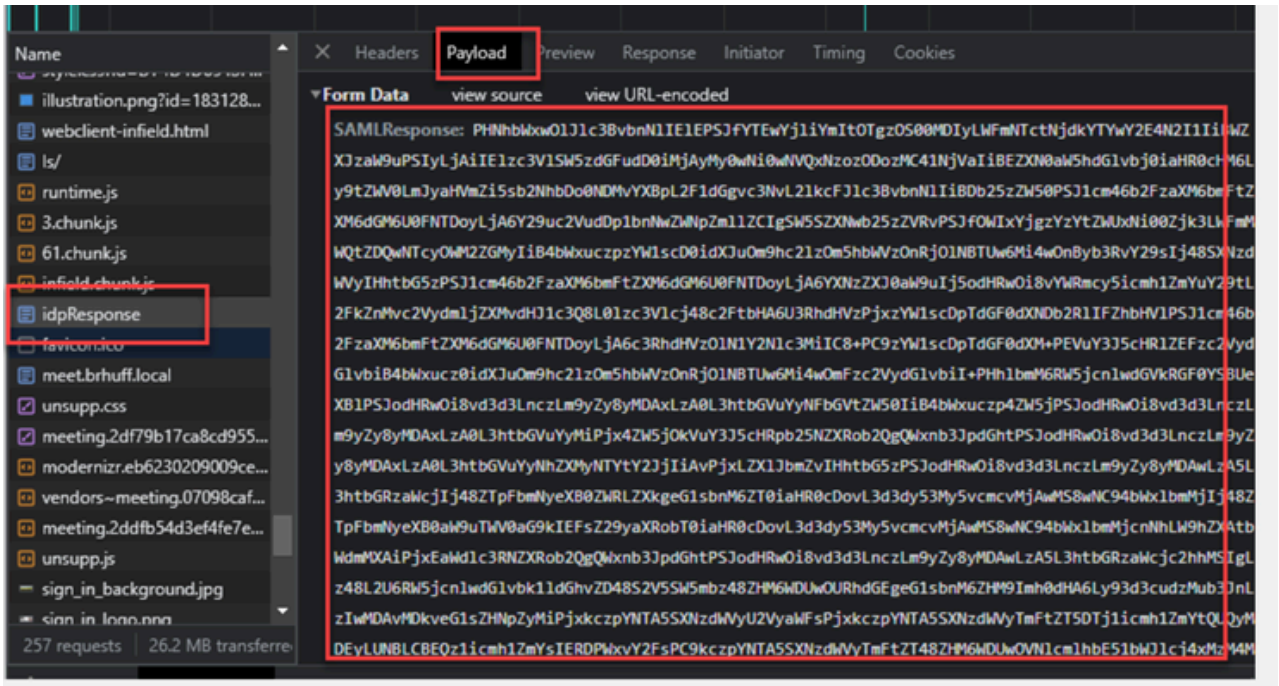
Cela indique que lors de l'examen des données SAMLResponse renvoyées par l'IdP pendant l'échange d'authentification, le Webbridge3 n'a pas trouvé d'attribut correspondant valide dans la réponse par rapport à son config.json pour l'authenticationId.

Si la communication n'est pas chiffrée à l'aide des clés privées de signe et de chiffrement, la réponse SAML peut être extraite de la journalisation réseau des outils de développement via un navigateur Web et décodée à l'aide de base64. Si la réponse est chiffrée, vous pouvez demander la réponse SAML déchiffrée du côté IdP.

Lors de l'enregistrement des journaux réseau, assurez-vous que la case Conserver le journal est cochée, afin que les journaux ne soient pas écrasés lorsque la page change.



Dans la sortie de journalisation réseau des outils de développement, également appelée données HAR, recherchez idpResponse sous la colonne name et sélectionnez Payload pour voir la réponse SAML. Comme mentionné précédemment, ceci peut être décodé à l'aide d'un décodeur base64.



Lors de la réception des données SAMLResponse, vérifiez la section de <AttributeStatement> pour localiser les noms d'attributs renvoyés et dans cette section, vous pouvez trouver les types de revendications configurés et envoyés à partir du fournisseur d'identité. Exemple :

<InstructionAttribut>
<Attribute Name="<URL pour nom commun">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="<URL pour NameID">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="uid">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
</AttributeStatement>

En examinant les noms précédents, vous pouvez vérifier <AttributeName> sous la section Attribute Statement et comparer chaque valeur à ce qui est défini dans la section authenticationIdmapping de SSO config.json.

Dans l'exemple précédent, vous pouvez voir que la configuration pour le authenticationIdMapping ne correspond PAS exactement à ce qui est passé et entraîne donc l'échec de la localisation d'un authenticationId correspondant :

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

Afin de résoudre ce problème, il existe deux méthodes possibles à essayer :

1. La règle de revendication de trafic sortant IdP peut être mise à jour pour avoir une revendication correspondante qui correspond exactement à ce qui est configuré dans

authenticationIdMapping du fichier config.json sur le pont Web 3. (Règle de revendication ajoutée sur IdP pour http://example.com/claims/NameID)
OU

2. Le fichier config.json peut être mis à jour sur le pont Web 3 pour que le paramètre « authenticationIdMapping » corresponde exactement à ce qui est configuré comme l'une des règles de revendication sortante configurées sur le fournisseur d'identité. (Il s'agit de 'authenticationIdMapping' à mettre à jour pour correspondre à l'un des noms d'attribut, qui peut être "uid", "<URL>/NameID" ou "<URL>/CommonName". Tant qu'il correspond (exactement) à la valeur attendue configurée sur l'API Callbridge lorsqu'il est passé)

Aucune assertion passée/correspondante dans la validation

Parfois, lors de l'échange de la réponse SAMLResponse à partir du fournisseur d'identité, le Webbridge affiche cette erreur indiquant qu'il y a un échec dans la correspondance de l'assertion et ignore toutes les assertions qui ne correspondent pas à la configuration du serveur :

> client_backend : ERREUR : SamlManager : Aucune assertion n'a réussi la validation
> client_backend : INFO : SamlManager : Ignorer l'affirmation sans nous dans l'audience autorisée

Ce que cette erreur indique est que lors de la révision de la réponse SAMLResponse à partir du fournisseur d'identité, le Webbridge n'a pas trouvé d'assertions correspondantes et a donc ignoré les échecs non correspondants et a finalement abouti à une connexion SSO défaillante.

Afin de localiser ce problème, il est idéal de revoir la réponse SAML du fournisseur d'identité. Si la communication n'est pas chiffrée à l'aide des clés privées de signe et de chiffrement, la réponse SAML peut être extraite de la journalisation réseau des outils de développement via un navigateur Web et décodée à l'aide de base64. Si la réponse est chiffrée, vous pouvez demander la réponse SAML déchiffrée du côté fournisseur d'identité.

Lorsque vous consultez les données SAMLResponse, en consultant la section <AudienceRestriction> de la réponse, vous pouvez trouver tous les publics pour lesquels cette réponse est restreinte :

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

À l'aide de la valeur de la section <Audience> (https://cisco.example.com)), vous pouvez la comparer à l'adresse ssoServiceProviderAddress dans le fichier config.json de la configuration Webbridge et vérifier s'il s'agit d'une correspondance exacte. Pour cet exemple, vous pouvez voir que la raison de l'échec est que l'auditoire ne correspond PAS à l'adresse du fournisseur de

services dans la configuration, car il a l'ajout :443:

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

Cela nécessite une correspondance exacte entre ces éléments pour ne pas entraîner un échec comme celui-ci. Pour cet exemple. la solution serait à l'une de ces deux méthodes :

1. Le :443 peut être supprimé de l'adresse dans la section ssoServiceProviderAddress du fichier config.json, de sorte qu'il corresponde au champ Audience fourni dans SAMLResponse à partir du fournisseur d'identité.
OU

2. Les métadonnées OU la partie d'approbation de confiance pour Webbridge3 dans le fournisseur d'identité peuvent être mises à jour pour que le :443 soit ajouté à l'URL. (Si les métadonnées sont mises à jour, elles doivent être importées à nouveau en tant que partie d'approbation de confiance sur ADFS. Toutefois, si vous modifiez directement la partie de confiance à partir de l'Assistant IdP, il n'est pas nécessaire de la réimporter.)

Faites également attention à la condition NotBefore et NotONOrAfter : <Conditions NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>

Si l'heure du serveur est incorrecte, elle peut entraîner la fin de la période de validité définie dans les conditions. Vous voudrez vérifier les serveurs NTP via l'interface de ligne de commande en utilisant les commandes ntp server list pour examiner les serveurs NTP configurés et ntp status pour vérifier l'état des serveurs NTP configurés. Utilisez la commande date pour vérifier l'heure des serveurs.

Conseil : Si vous utilisez un serveur NTP local/interne, essayez de configurer un serveur NTP public tel que time.google.com (assurez-vous de configurer un serveur DNS public avant).

Échec de la connexion sur Web App :

Home

EN (US)



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign In

Sign in failed

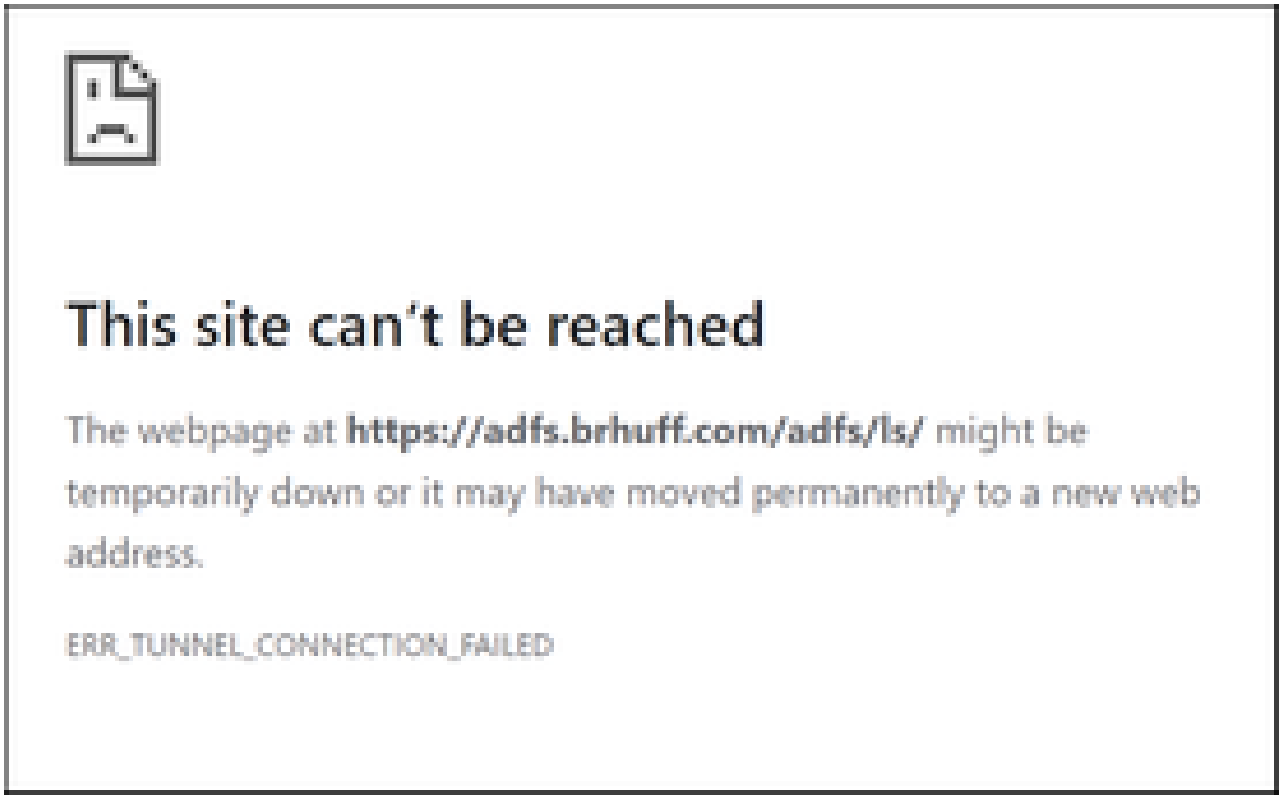
© 2019-2023 Cisco and/or its affiliates. All rights reserved.

CISCO

CMS FAQ

Cisco Website

), webbridge vérifie que le domaine utilisé correspond à un domaine dans le fichier config.json, puis envoie les informations SAML au client, lui indiquant à quel endroit se connecter pour l'authentification. Le client tente de se connecter au fournisseur d'identité qui se trouve dans le jeton SAML. Dans l'exemple, le navigateur affiche cette page car elle ne peut pas atteindre le serveur ADFS.



Erreur sur le navigateur client

Traces Webbridge CMS (alors que ?trace=true est utilisé)

19 mars 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SSO correspondant sso_2024.zip dans la demande de jeton SAML

19 mars 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Tentative de recherche de SSO dans la demande de jeton SAML

19 mars 10:47:07.930 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Génération du jeton SAML réussie

Scénario 2 :

L'utilisateur a tenté de se connecter à l'aide d'un domaine qui ne figure pas dans le fichier zip SSO de la page de connexion du pont Web. Le client envoie une requête tokenRequest avec une charge utile du nom d'utilisateur entré par l'utilisateur. Webbridge arrête immédiatement la tentative de connexion.

Traces Webbridge CMS (alors que ?trace=true est utilisé)

18 mars 14:54:52.698 user.err cmscb3-1 client_backend : ERREUR : SamlManager : Tentative de connexion SSO non valide

18 mars 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Impossible de trouver une SSO dans la demande de jeton SAML

18 mars 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Tentative de recherche de SSO dans la demande de jeton SAML

Scénario 3 :

L'utilisateur a entré le nom d'utilisateur correct et la page de connexion SSO s'affiche. L'utilisateur saisit également ici le nom d'utilisateur et le mot de passe corrects, mais obtient toujours Échec de la connexion

Traces Webbridge CMS (alors que ?trace=true est utilisé)

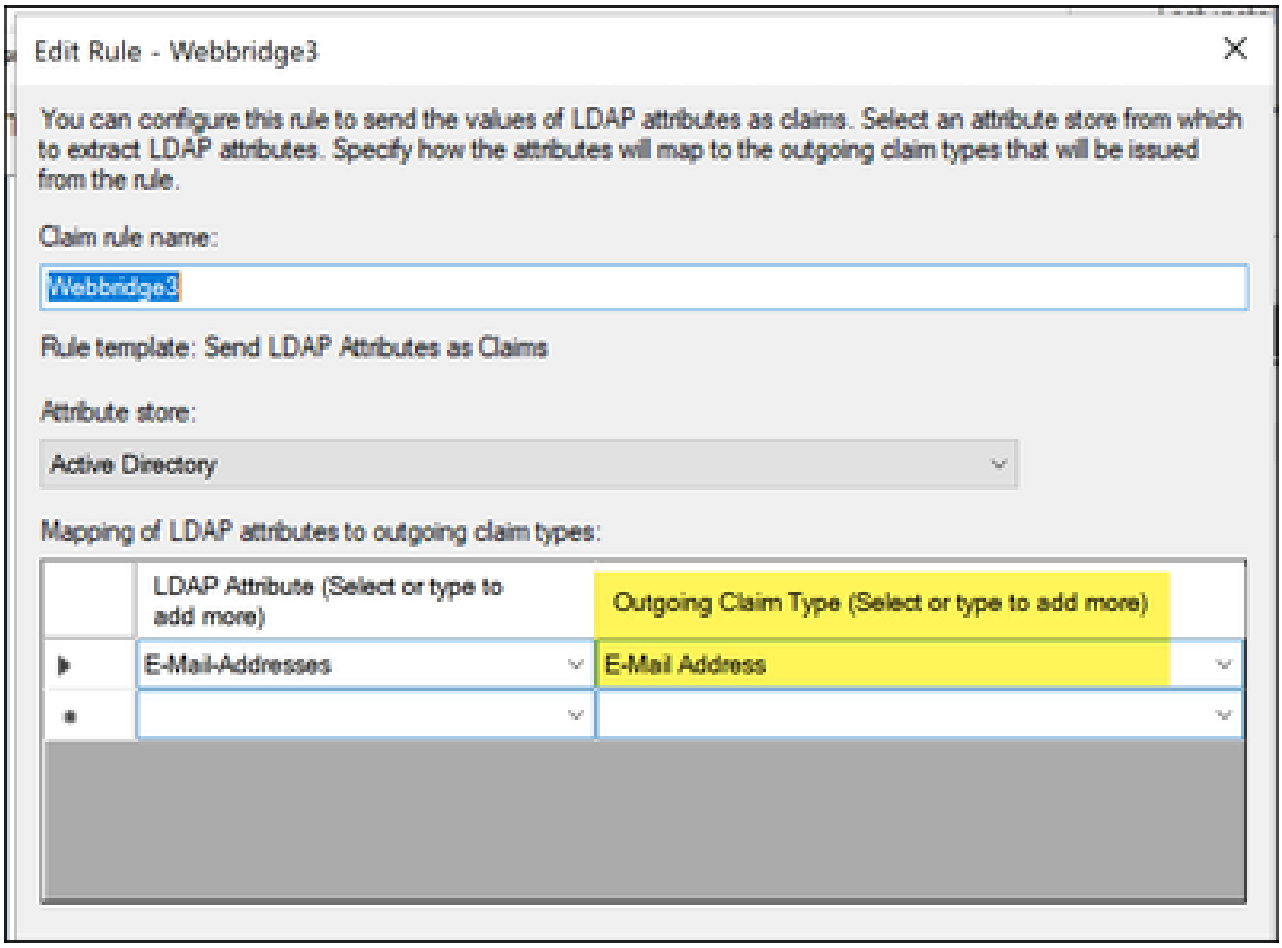
19 mars 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] SSO correspondant sso_2024.zip dans la demande de jeton SAML

19 mars 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Tentative de recherche de SSO dans la réponse IDP SAML

19 mars 16:39:17.720 user.err cmscb3-1 client_backend : ERREUR : SamlManager : Aucun élément mappé authenticationId trouvé dans les assertions SAML signées

19 mars 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Échec de l'obtention d'un authenticationID

La cause du scénario 3 était que la règle de revendication dans le fournisseur d'identité utilisait un type de revendication qui ne correspondait pas à authenticationIdMapping dans le fichier config.json utilisé dans le fichier zip SSO qui a été téléchargé sur webbridge. Webbridge examine la réponse SAML et s'attend à ce que le nom d'attribut corresponde à ce qui est configuré dans le fichier config.json.



Règle de revendication dans ADFS

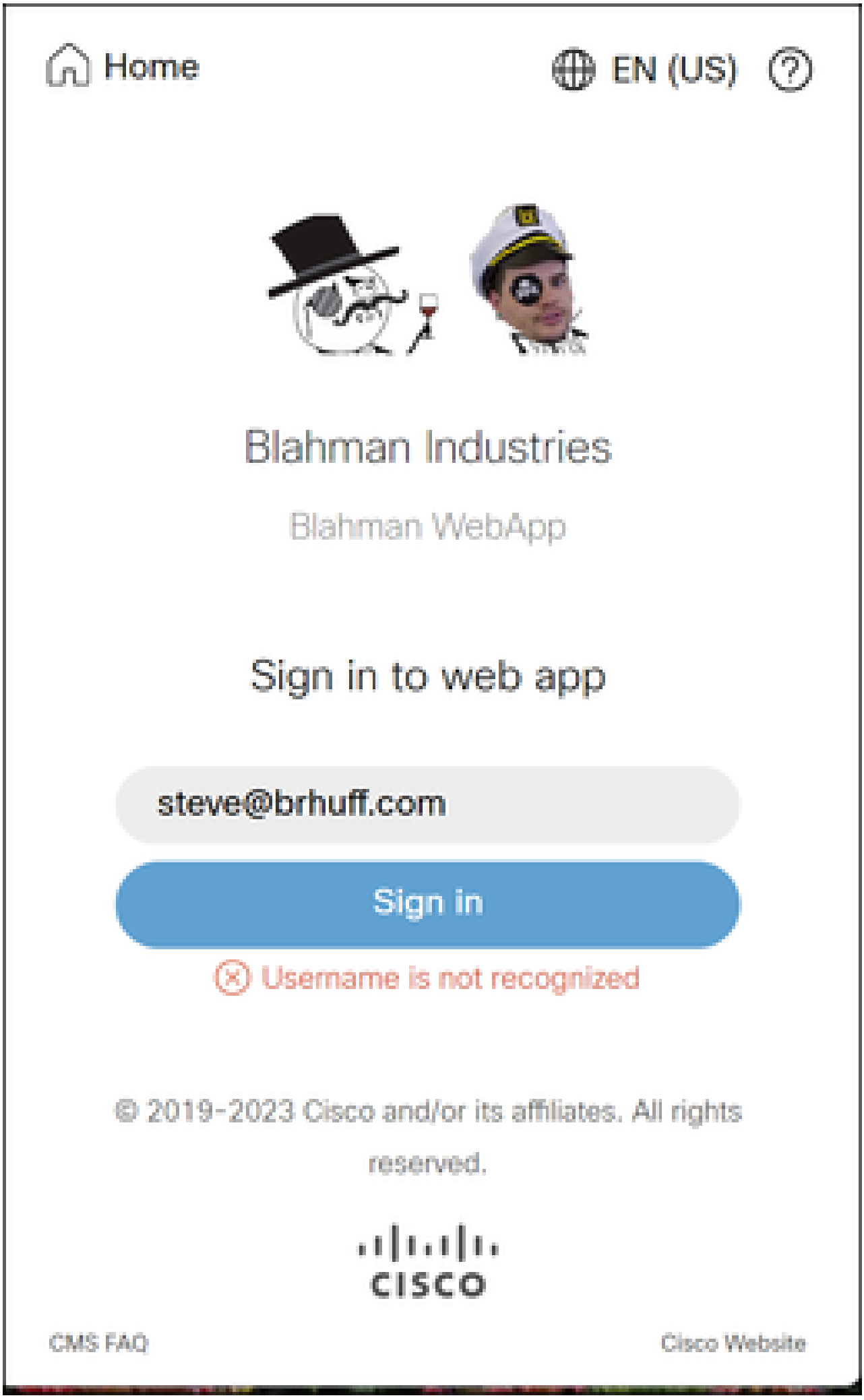


config.json, exemple

Nom d'utilisateur non reconnu

Scénario 1 :

Utilisateur connecté avec un nom d'utilisateur incorrect (le domaine correspond à ce qui se trouve dans le fichier zip SSO qui a été téléchargé sur webbridge3, mais l'utilisateur n'existe pas)



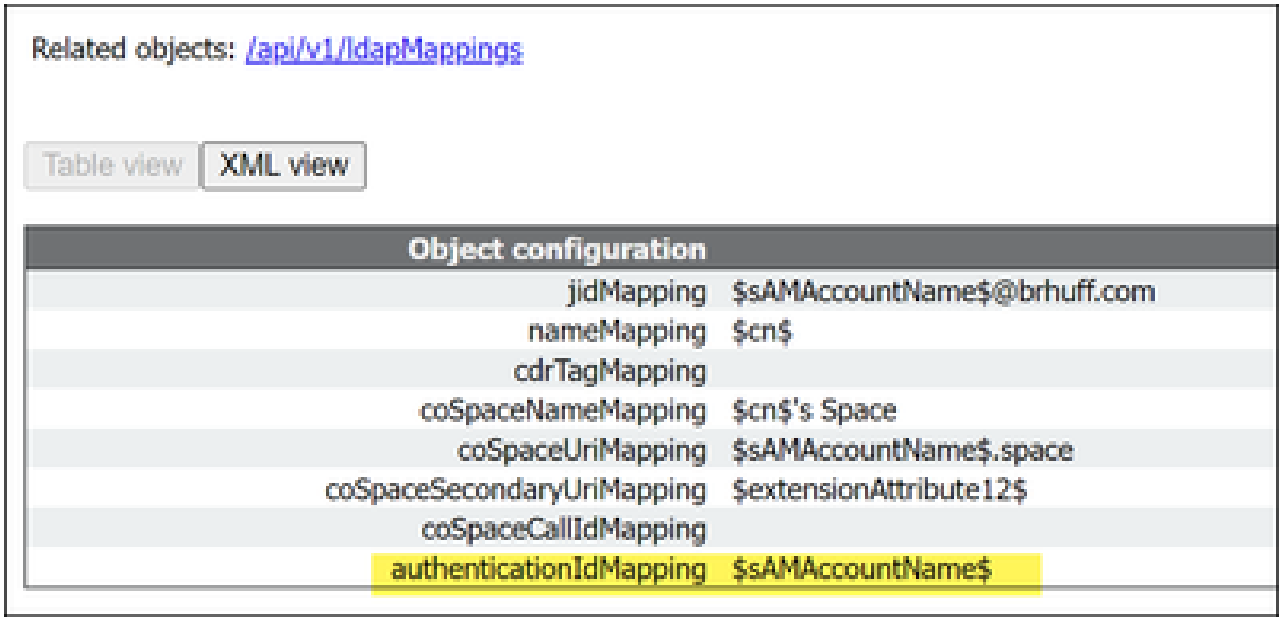
Nom d'utilisateur non reconnu

dans CMS ldapmapping ne correspond pas à l'attribut LDAP configuré utilisé pour la règle de revendication dans ADFS. La ligne indiquant "Successfully got authenticationID:darmckin@brhuff.com" indique qu'ADFS a configuré une règle de revendication avec un attribut qui obtient darmckin@brhuff.com à partir d'Active Directory, mais que AuthenticationID dans CMS API > Users indique qu'il attend le darmckin. Dans CMS ldapMappings, AuthenticationID est configuré comme $sAMAccountName$, mais la règle de revendication dans ADFS est configurée pour envoyer les adresses de messagerie, donc cela ne correspond pas.

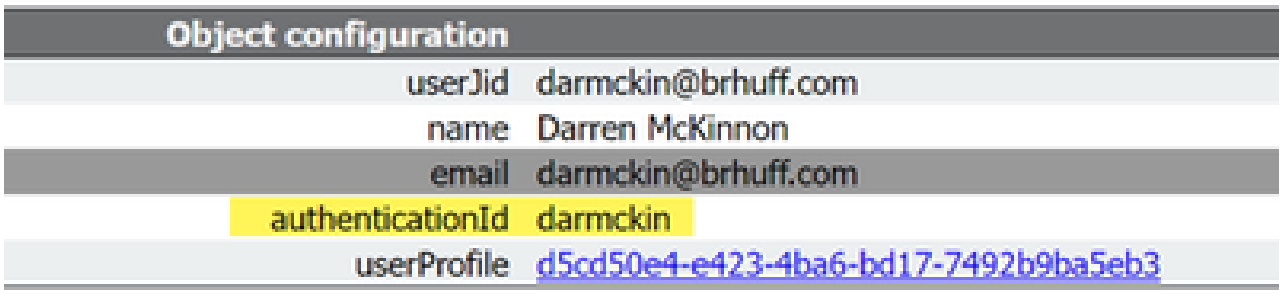
Comment résoudre ce problème :

Faites l'une ou l'autre option pour atténuer :

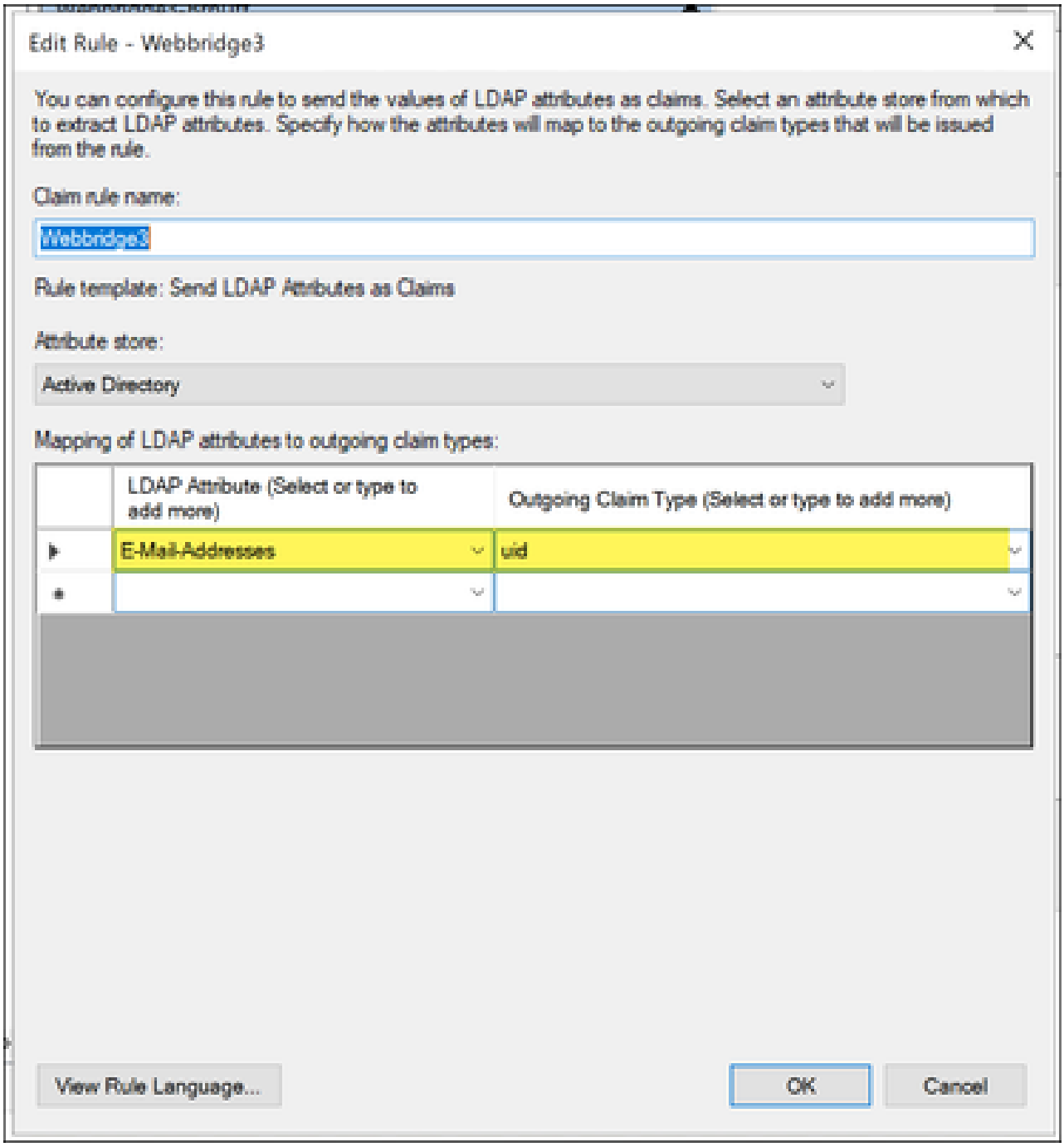
1. Modifiez l'AuthenticationID dans le ldapmapping CMS pour qu'il corresponde à ce qui est utilisé dans la règle de revendication sur ADFS et effectuez une nouvelle synchronisation
2. Modifier l'attribut LDAP utilisé dans la règle de revendication ADFS pour correspondre à ce qui est configuré dans CMS ldapmapping



API LDAPMapping



Exemple d'utilisateur API



Règle de demande d'ADFS

Journal Webbridge affichant l'exemple de connexion en cours. Exemple généré à l'aide de ?trace=true dans l'URL de jointure :

> 18 mars 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] SSO correspondant sso_2024.zip dans la demande de jeton SAML
>
> 18 mars 14:24:01.096 user.info cmscb3-1 client_backend: INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Tentative de recherche de SSO dans la réponse d'IDP SAML
>
> 18 mars 14:24:01.101 user.info cmscb3-1 client_backend: INFO : SamlManager :

[7979f13c-d490-4f8b-899c-0c82853369ba] AuthentificationID obtenue : darmckin@brhuff.com

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

18 mars 14:24:01.130 user.info cmscb3-1 hôte:serveur: INFO : demande de connexion réussie depuis darmckin@brhuff.com

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

18 mars 14:24:01.132 user.info cmscb3-1 hôte:serveur: INFO : WB3Cmgr : [7979f13c-d490-4f8b-899c-0c82853369ba] envoi d'une réponse d'authentification (longueur jwt=1064, connexion=64004556-faea-479f-aabe-691e17783aa5)

18 mars 14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 10.10.10.8 - - [18/Mar/2024:18:24:01 +0000] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "https://adfs.brhuff.com/" http_user_agent "Mozilla/5.0 (Windows NT 10.0 ; Win64 ; x64) AppleWebKit/537.36 (KHTML, comme Gecko) Chrome/122.0.0. Safari/537.36" vers l'amont 192.0.2.2:9000 : upstream_response_time 0.038 request_time 0.039 ms 1710786241.133 upstream_response_length 24 200

Foire aux questions (FAQ)

Cette section présente les questions fréquemment posées ou les sujets relatifs à WebApp SSO sur le serveur de réunion Cisco.

Le WebApp SSO JWT peut-il être étendu ?

Le JSON Web Token (JWT) est le jeton fourni par Callbridge à un client Webapp authentifié (authentifié avec succès auprès du fournisseur d'identité), lui accordant l'accès aux services WebApp. Dans le JWT est une valeur de temporisateur d'expiration qui indique combien de temps le JWT est valide, qui une fois le délai d'expiration du JWT est atteint - l'utilisateur WebApp est redirigé vers la page de connexion Webbridge, nécessitant une nouvelle authentification pour obtenir l'accès de retour.

L'expiration JWT est configurable à l'aide de la commande 'callbridge wc3jwt expiry <1-24>' (ajoutée dans la version 3.8 et ultérieure - plus de détails peuvent être trouvés dans les notes de version de CMS 3.8 ou dans le guide MMP de CMS) dans laquelle la valeur numérique correspond au nombre d'heures que vous souhaitez définir le délai d'expiration pour le JWT fourni aux clients WebApp. Cependant, comme on le voit dans la commande, la valeur max peut être définie est 24 heures, ce qui signifie que la durée la plus longue pendant laquelle le JWT peut

rester valide et l'utilisateur WebApp peut se connecter est de 24 heures. Lorsque le délai d'expiration de JWT est atteint, le navigateur vide le jeton expiré et l'utilisateur WebApp est forcé de revenir à la page de connexion WebApp.

Dans certains environnements, en fonction de l'IdP et de la configuration de l'environnement, une SSO persistante/fonction « Me garder connecté » peut être implémentée sur l'IdP, ce qui fournirait au navigateur un cookie persistant à partir de l'IdP, où même en fermant le navigateur, le cookie serait conservé (sauf s'il est effacé par d'autres moyens). Quelle que soit la configuration SSO/IdP, lorsque le JWT expire (max 24 heures), l'utilisateur WebApp est forcé de revenir à la page de connexion WebApp. Cependant, dans ce scénario où l'SSO persistante est activée sur l'IdP, l'utilisateur n'utilisateur aurait juste besoin d'entrer son <user@domain> sur la page Page de connexion WebApp et pas besoin de se réauthentifier auprès de leur fournisseur d'identité.

Une amélioration est disponible pour la mise en oeuvre d'un mécanisme de jeton d'actualisation permettant une autorisation étendue à WebApp - ID de bogue Cisco CSCwm28758.

Dois-je m'authentifier à nouveau sur WebApp si je ferme mon navigateur ?

Le flux de ce scénario serait le suivant :

1. Un utilisateur se connecte à WebApp (en utilisant la méthode d'authentification SSO).
2. L'utilisateur ferme le navigateur à un moment donné.
3. L'utilisateur ouvre à nouveau le navigateur et accède au site WebApp. (immédiatement ou ultérieurement).

Que se passerait-il dans ce scénario ?

Pour cette réponse, cela dépend ! Cela dépend entièrement de l'expiration du JWT fourni par Callbridge au moment de l'accès à la page WebApp. Tant que le JWT est toujours valide et présent dans le stockage, vous pouvez naviguer jusqu'à la page WebApp (même si vous avez fermé le navigateur). Gardez à l'esprit que la durée maximale de validité du JWT est de 24 heures.

- Si le JWT est toujours VALIDE (NON EXPIRÉ) et présent, l'utilisateur peut naviguer jusqu'à la page WebApp avec ses espaces et ainsi de suite sans avoir besoin de se réauthentifier.
- Si le JWT est INVALID (EXPIRED), l'utilisateur est redirigé vers la page de connexion WebApp, nécessitant une nouvelle connexion à WebApp. L'utilisateur peut également devoir s'authentifier à nouveau auprès de son fournisseur d'identité en fonction de sa méthode d'authentification (par exemple, si le fournisseur d'identité utilise l'authentification unique de session ou l'authentification unique permanente).

Comment plusieurs domaines sont-ils pris en charge dans WebApp SSO ?

WebApp SSO est capable de prendre en charge des environnements qui ont plusieurs domaines et même des environnements où ces différents domaines pointent vers différents fournisseurs d'identité (IdP). Consultez les guides de déploiement de Cisco Meeting Server ou contactez le TAC Cisco pour obtenir de l'aide sur l'utilisation de plusieurs domaines.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.