Configurer l'authentification externe SSO SAML avec AD FS pour ESA et SMA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Étapes de configuration ADFS IDP pour SAML

- Configurer l'approbation de la partie de confiance
  - Méthode A : Créer l'approbation de la partie de confiance en important les métadonnées SP
- Configurer les terminaux de confiance des parties de confiance (clusters uniquement)
  - Règles de transformation d'émission - Demandes
  - Télécharger les métadonnées IdP et les charger sur ESA
- Vérifier
- Informations connexes

Introduction

Ce document décrit comment configurer les services de fédération Active Directory en tant que fournisseur d'identité SAML pour l'authentification externe sur Cisco ESA et SMA.

Conditions préalables

Ce document fournit une vue de l'application tierce que les ingénieurs ne peuvent pas voir autrement.

- Étapes de configuration de l'authentification externe SAML (Security Assertion Markup Language) avec les services ADFS (Active Directory Federation Services) 2012 et 2016 pour les dernières versions de Cisco Email Security Appliance (ESA) et Security Management Appliance (SMA).
- Étapes de TP de base qui n'incluent pas de configurations spécifiques au déploiement.
- Un exemple pratique d'environnement de laboratoire qui peut différer d'un déploiement en production.

⚠ Mise en garde : Effectuez la configuration du fournisseur de services (SP) avant cette procédure. Reportez-vous à .

Exigences

- Services de fédération Microsoft Active Directory (AD FS) 2012 ou 2016
- Dernière version de Cisco Email Security Appliance (ESA) et Security Management Appliance (SMA).

Composants utilisés

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.

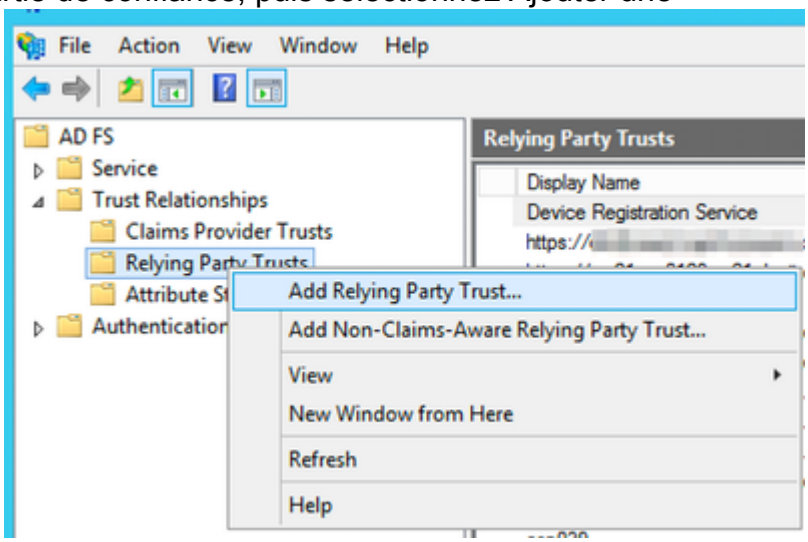
Étapes de configuration ADFS IDP pour SAML

Configurer l'approbation de la partie de confiance

Utilisez l'une des deux options pour créer l'approbation de partie de confiance dans AD FS.

Méthode A : Créer l'approbation de la partie de confiance en important les métadonnées SP

1. Ouvrez la console de gestion AD FS à partir des outils d'administration.
2. Dans la console de gestion AD FS, développez Relations approuvées, cliquez avec le bouton droit sur Approbations de partie de confiance, puis sélectionnez Ajouter une approbation de partie de confiance.



Ajouter une approbation de partie de confiance

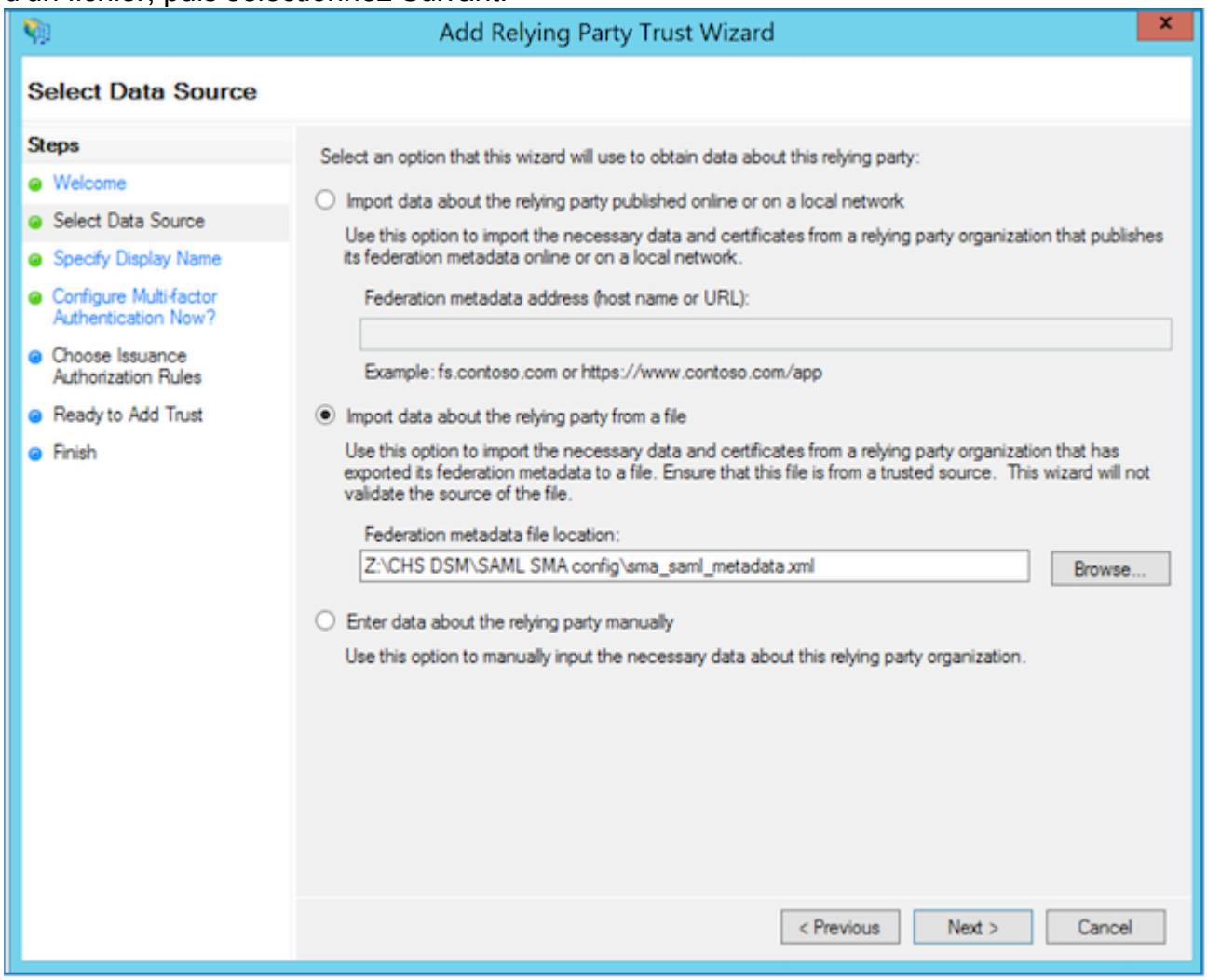
Conseil : Approbations de partie de confiance Microsoft

Utilisez l'une des deux options :

- Option A : Importer des données sur la partie de confiance à partir d'un fichier. Téléchargez le fichier metadata.xml ESA ou SMA Service Provider (SP).
- Option B : Saisissez manuellement les données relatives à la partie de confiance. Cette option vous guide tout au long de la configuration manuelle.

Option A : Importer des données sur la partie de confiance à partir d'un fichier. Téléchargez le fichier metadata.xml ESA ou SMA Service Provider (SP).

1. Sélectionnez l'option permettant d'importer des données sur la partie de confiance à partir d'un fichier, puis sélectionnez Suivant.



Importer le fichier de métadonnées ESA/SMA

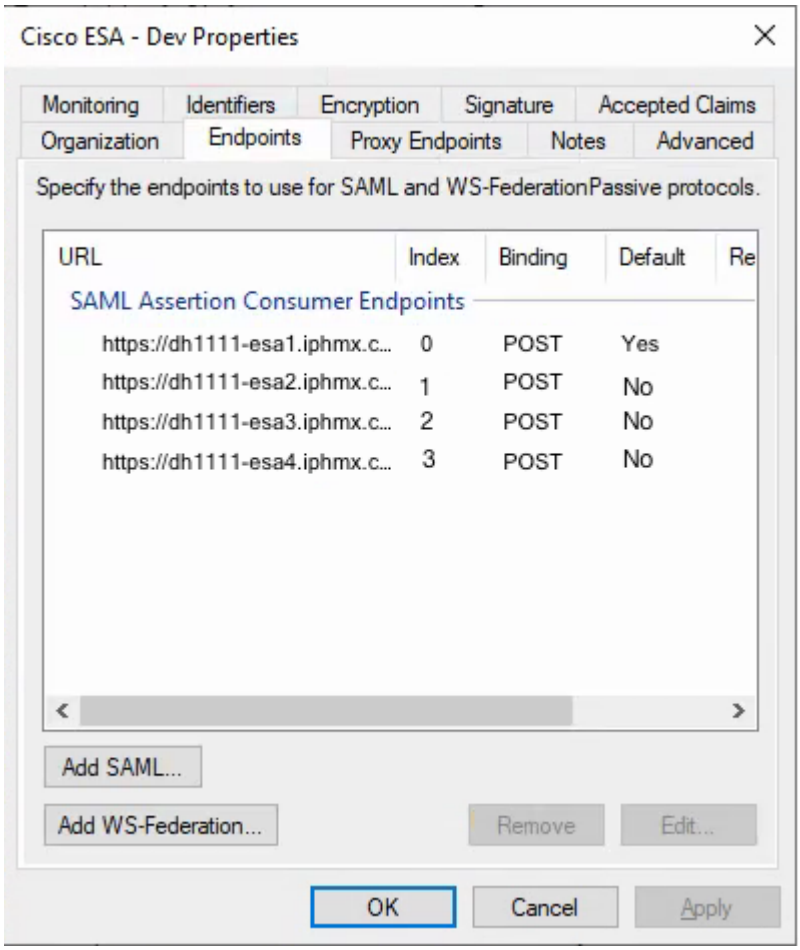
2. Spécifiez un nom complet pour identifier cette approbation de partie de confiance, puis sélectionnez Suivant deux fois.
3. Pour les règles d'autorisation d'émission, sélectionnez Autoriser tous les utilisateurs, puis Suivant.
4. Sur la page Prêt à ajouter un niveau de confiance, acceptez les paramètres par défaut, puis sélectionnez Suivant.

5. Sélectionnez Terminer. La boîte de dialogue Modifier les règles de revendication s'ouvre pour l'approbation de la partie de confiance, qui est traitée dans Règles de transformation d'émission - Revendications.

Propriétés de confiance de la partie de confiance - Terminaux

Effectuez ces étapes uniquement si plusieurs ESA sont présents dans une grappe.

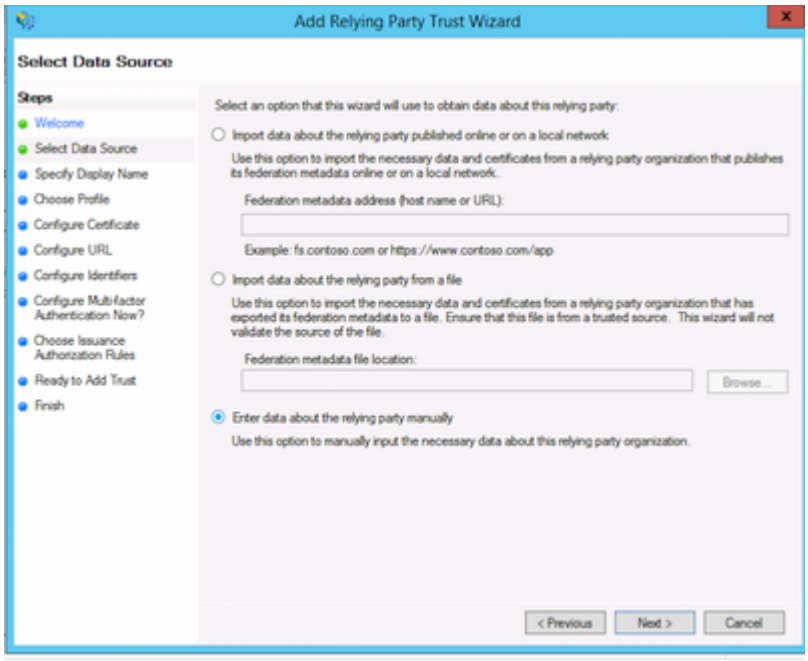
1. Ouvrez Propriétés d'approbation de la partie de confiance > Terminaux.
2. Ajoutez chaque adresse URL d'accès ESA, puis sélectionnez OK.
3. Les valeurs d'index comptent à partir de 0, c'est-à-dire 0, 1, 2 et 3.
4. Définissez une seule entrée sur Default = Yes.
5. Définissez les entrées restantes sur Default = No.



Propriétés de confiance de la partie de confiance - Terminaux

Option B : Saisissez manuellement les données relatives à la partie de confiance. Cette option vous guide tout au long de la configuration manuelle.

1. Sélectionnez Saisir manuellement les données relatives à la partie de confiance.

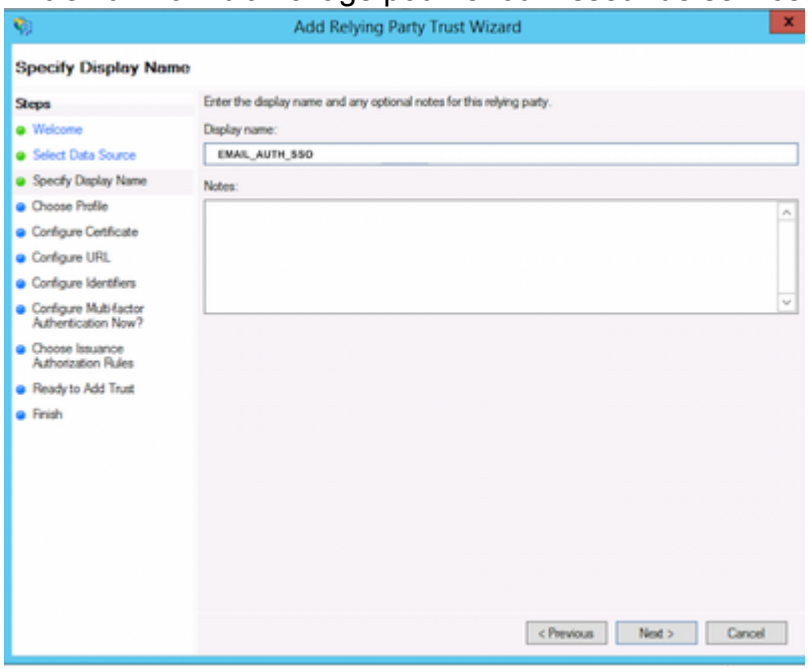


Ajouter manuellement une partie de confiance

Conseil : Nom complet est le nom que vous choisissez pour identifier l'approbation de partie de confiance pour ESA ou SMA SAML.

---

2. Entrez un nom d'affichage pour le fournisseur de services, par exemple ESA_SP.

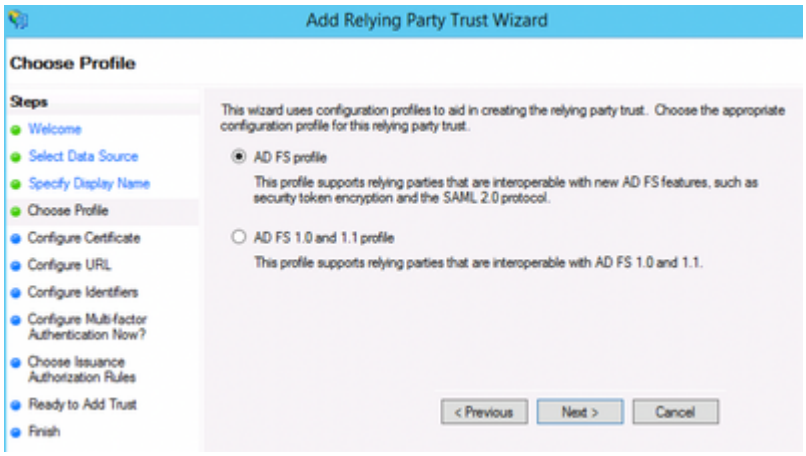


Créer un nom pour le profil de fournisseur de services

Conseil : [Rôle des règles de réclamation et des règles de transformation d'émission]

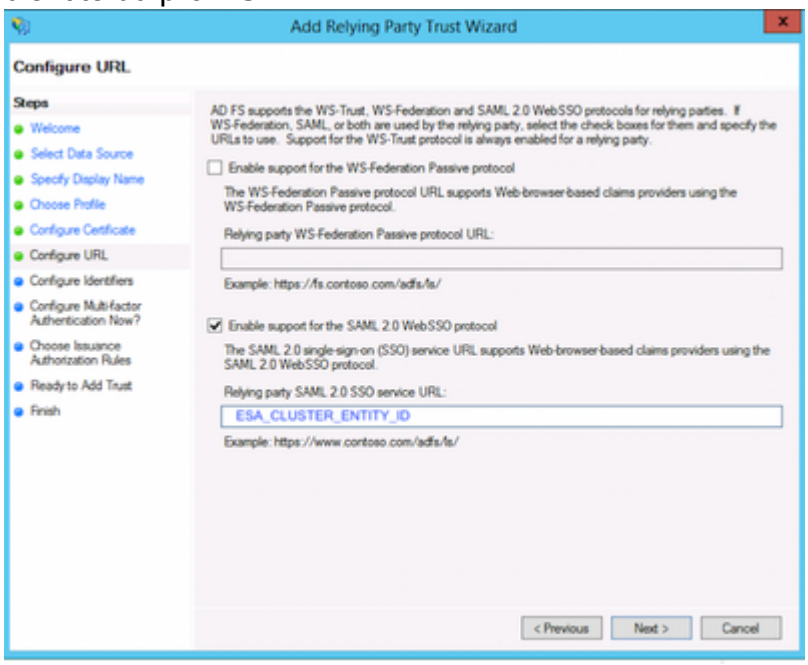
---

3. Sélectionnez l'option de profil Profil AD FS.



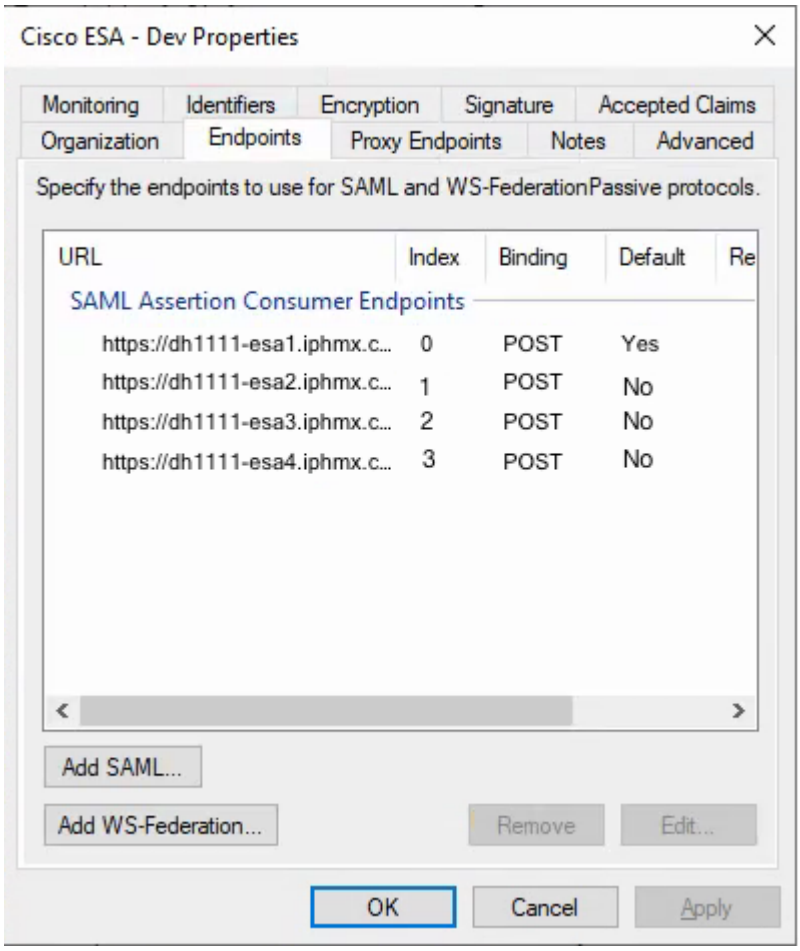
Option de profil AD FS pour utiliser SAML 2.0

4. Chargez le certificat public à partir de la configuration du fournisseur de services ESA.
5. Pour Configurer l'URL, sélectionnez Activer la prise en charge de l'authentification unique (SSO) SAML 2.0.
6. Saisissez l'URL du service SSO SAML 2.0 de la partie de confiance avec la valeur de l'ID d'entité du profil SP.



Règles d'autorisation d'émission - -Autoriser tous les utilisateurs

7. Pour les règles d'autorisation d'émission, sélectionnez Autoriser tous les utilisateurs à accéder à cette partie de confiance.



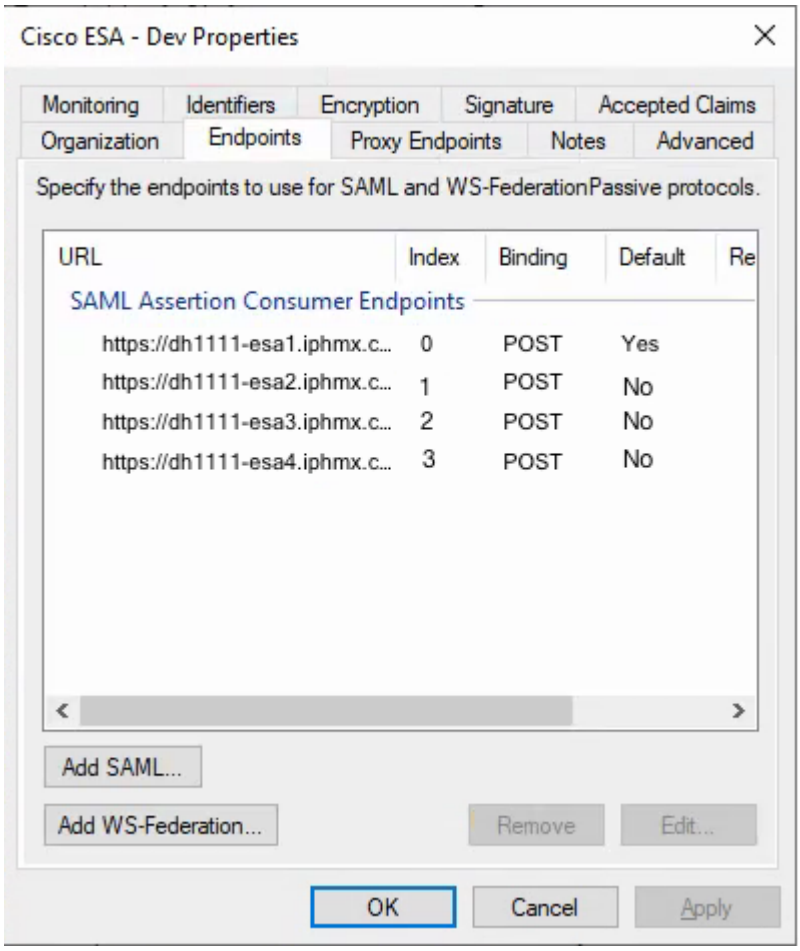
Choisir des règles d'autorisation d'émission

8. Sélectionnez Next pour passer à la page Finish.

Configurer les terminaux de confiance des parties de confiance (clusters uniquement)

Effectuez cette étape uniquement si plusieurs ESA sont présents dans une grappe.

1. Ouvrez Propriétés d'approbation de la partie de confiance > Terminaux.
2. Ajoutez chaque adresse URL accessible ESA, puis cliquez sur OK.
3. Définissez des valeurs d'index de point de terminaison commençant à 0 (par exemple, 0, 1, 2, 3).
4. Définissez un seul point de terminaison sur Default = Yes. Définissez les points d'extrémité restants sur Default = No.

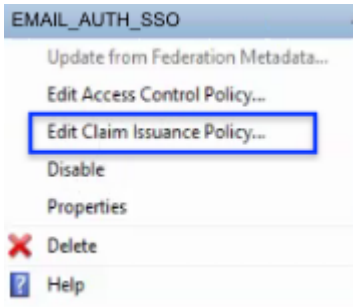


Règles d'autorisation d'émission - Autoriser tous les utilisateurs

L'étape finale lance la boîte de dialogue Modifier les règles de revendication pour l'approbation de partie de confiance, traitée dans les règles de transformation d'émission.

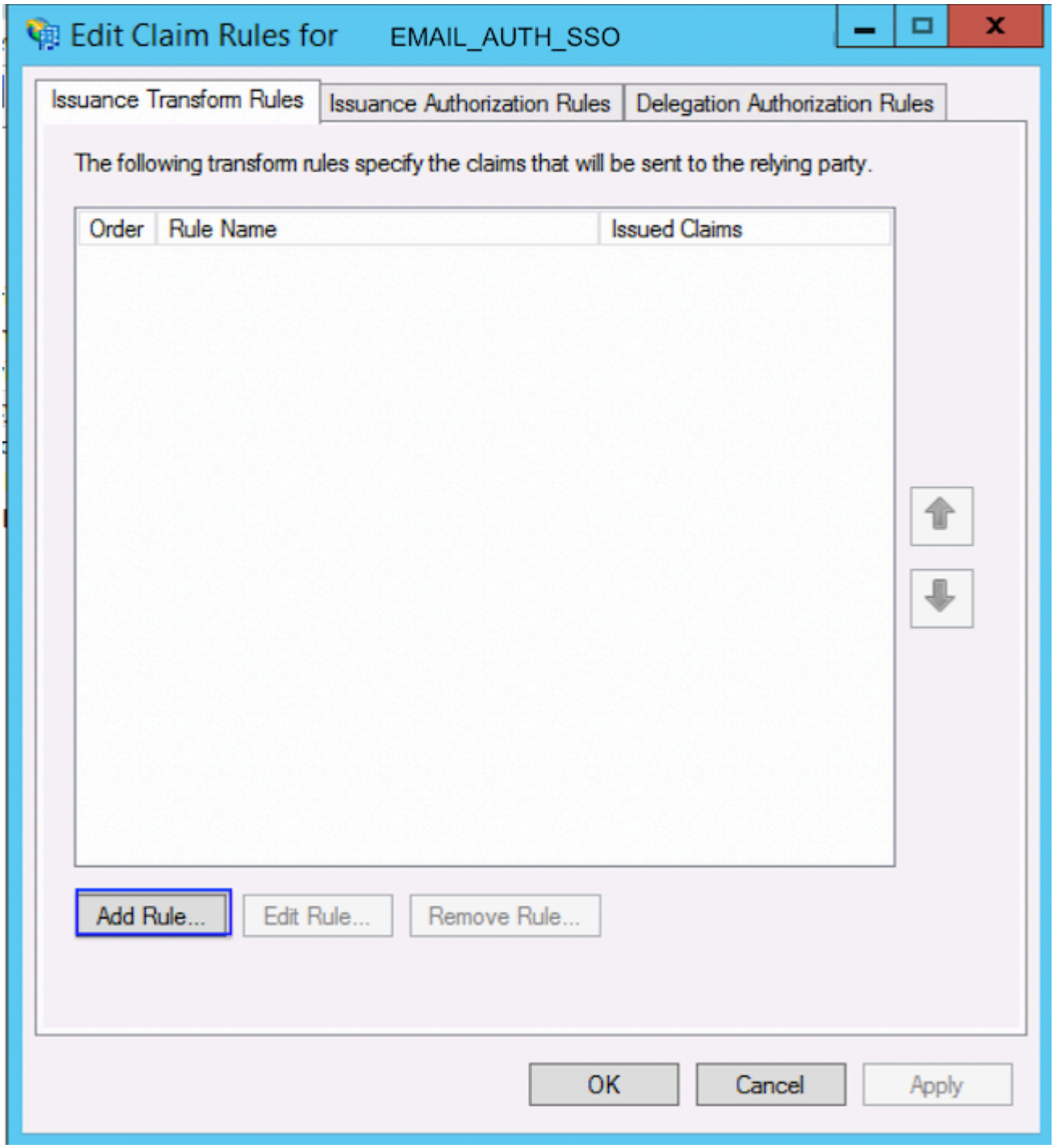
Règles de transformation d'émission - Demandes

1. Sélectionnez Modifier la stratégie d'émission des revendications.



Modifier la stratégie d'émission des demandes

2. Sélectionnez Ajouter une règle.



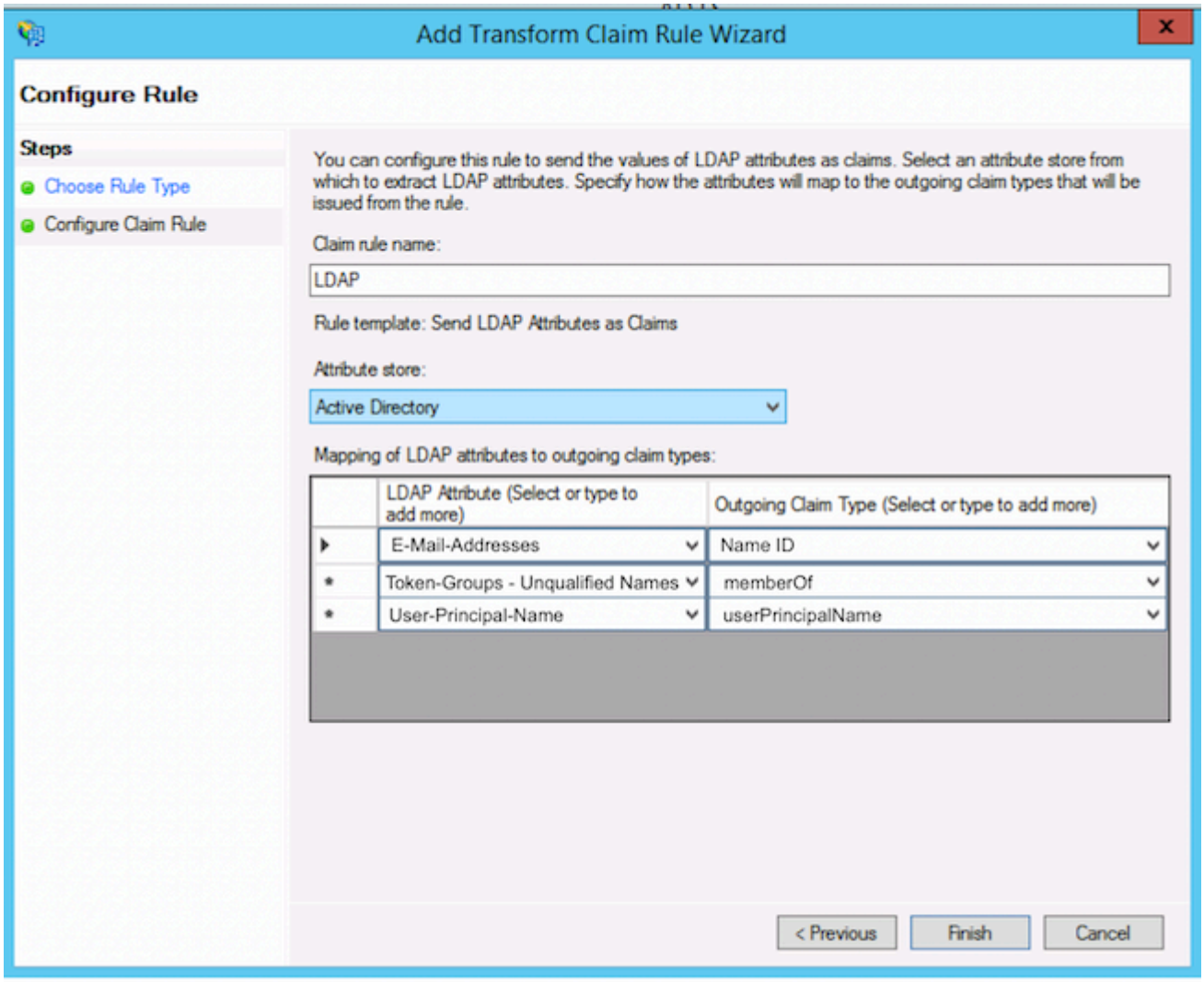
Ajouter une règle de transformation d'émission

Les valeurs présentées ici sont des valeurs courantes qui permettent à ESA de renseigner les noms de groupe dans les paramètres d'authentification externe.

Conseil : Les valeurs du mappage peuvent varier en fonction des préférences de l'administrateur.

Conseil : Dans l'exemple répertorié, entrez manuellement les types de revendications sortantes memberOf et userPrincipalName. Sélectionnez Name ID dans la liste déroulante.

3. Sélectionnez Terminer.



Transformer la règle de revendication

Télécharger les métadonnées IdP et les charger sur ESA

Une fois que vous avez terminé la configuration de la règle d'approbation et de revendication de partie de confiance, exportez les métadonnées de fournisseur d'identité (IdP) et téléchargez-les vers ESA.

⚠ Mise en garde : Le redémarrage du service AD FS peut interrompre les sessions d'authentification actives. Effectuez cette étape au cours d'une fenêtre de maintenance, si nécessaire.

---

1. Redémarrez le service AD FS si nécessaire.
2. Exécutez ces commandes :

```
net stop adfssrv
net start adfssrv
```

3. Terminez et revenez au cluster ESA.

Vérifier

1. Dans ESA ou SMA, vérifiez que l'importation des métadonnées IdP s'est correctement effectuée.
2. Testez une connexion administrative à l'aide de l'authentification unique (SSO) SAML.
3. Vérifiez que les revendications de groupe attendues sont reçues et que le mappage de rôle est renseigné comme prévu dans la configuration de l'authentification externe.

Informations connexes

-

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Cisco Content Security Management Appliance - Guides d'utilisation

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.