Dépannage de l'authentification unique CCE avec la gestion des certificats Identity Service (IdS)

Table des matières

Introduction

Ce document décrit les étapes détaillées pour la régénération et l'échange de certificats SAML dans UCCE/PCCE, assurant des processus sécurisés et clairs.

Contribution de Nagarajan Paramasivam, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

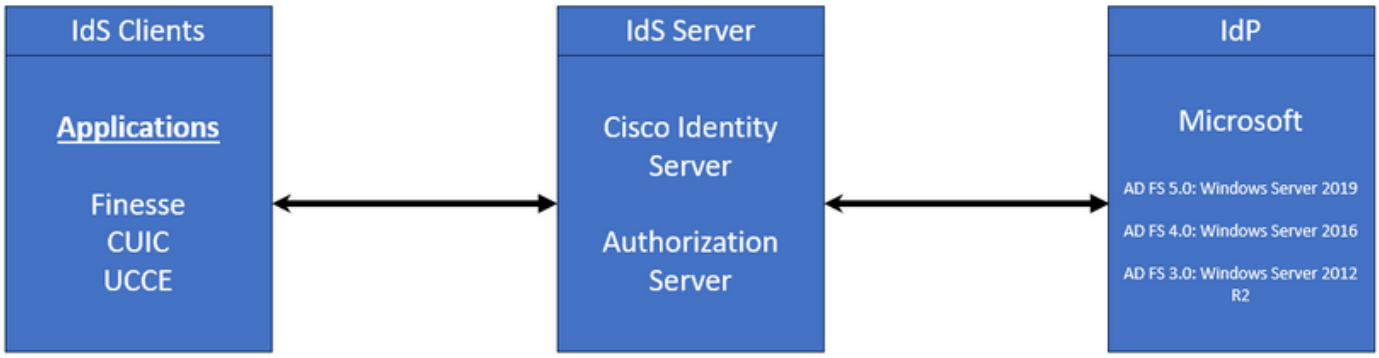
Cisco vous recommande de connaître les sujets suivants :

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Plate-forme VOS (Voice Operating System)
- Gestion des certificats
- SAML (Security Assertion Markup Language)
- Secure Socket Layer (SSL)
- Services de fédération Active Directory (AD FS)
- Authentification unique (SSO)

Composants utilisés

Les informations contenues dans ce document sont basées sur les composants suivants :

- Cisco Identity Service (ID Cisco)
- Fournisseur d'identités (IdP) - ADFS Microsoft Windows



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.

Informations générales

Dans UCCE/PCCE, Cisco Identity Service (Cisco IdS) fournit une autorisation entre le fournisseur d'identité (Identity Provider, IdP) et les applications.

Lorsque vous configurez les ID Cisco, vous configurez un échange de métadonnées entre les ID Cisco et le fournisseur d'ID. Cet échange établit une relation de confiance qui permet ensuite aux

applications d'utiliser les ID Cisco pour SSO. Vous établissez la relation d'approbation en téléchargeant un fichier de métadonnées à partir des ID Cisco et en le téléchargeant vers le fournisseur d'ID.

Le certificat SAML est similaire à un certificat SSL et, comme lui, doit être mis à jour ou modifié lorsque certaines situations se présentent. Lorsque vous régénérez ou permutez le certificat SAML sur le serveur Cisco Identity Services (IdS), il peut provoquer une interruption de la connexion approuvée avec le fournisseur d'identité (IdP). Cette interruption peut entraîner des problèmes lorsque les clients ou les utilisateurs qui dépendent de l'authentification unique ne peuvent pas obtenir l'autorisation dont ils ont besoin pour accéder au système.

Ce document vise à couvrir un large éventail de situations courantes dans lesquelles vous devez créer un nouveau certificat SAML sur le serveur Cisco IdS. Il explique également comment donner ce nouveau certificat au fournisseur d'identité (IdP) afin que l'approbation puisse être reconstruite. Ainsi, les clients et les utilisateurs peuvent continuer à utiliser l'authentification unique sans aucun problème. L'objectif est de vous assurer que vous disposez de toutes les informations dont vous avez besoin pour gérer le processus de mise à jour des certificats en douceur et sans confusion.

Points importants à retenir :

1. Le certificat SAML est généré par défaut lors de l'installation du serveur Cisco IdS avec une validité de 3 ans

2. Le certificat SAML est un certificat auto-signé

3. Le certificat SAML est un certificat SSL qui réside sur l’éditeur et l’abonné Cisco IDS

4. La régénération du certificat SAML n'a pu être effectuée que dans le noeud Cisco IDS Publisher

5. Les types disponibles d’algorithme de hachage sécurisé pour le certificat SAML sont SHA-1 et SHA-256

6. L'algorithme SHA-1 est utilisé sur IdS 11.6 et dans les versions précédentes, l'algorithme SHA-256 est utilisé sur IdS 12.0 et dans les versions ultérieures

7. Le fournisseur d'identité (IdP) et le service d'identité (IdS) doivent utiliser le même type d'algorithme.

8. Le certificat Cisco IdS SAML n'a pu être téléchargé qu'à partir du noeud Cisco IdS Publisher (sp-<Cisco IdS_FQDN>.xml)

9. Consultez ce lien pour comprendre la configuration de l'authentification unique UCCE/PCCE. Guide des fonctionnalités d'UCCE 12.6.1

Certificat SAML expiré

Le certificat SAML est généré avec 3 ans (1095 jours) de validité et il est nécessaire de renouveler

le certificat SAML avant l'expiration. Le certificat SSL expiré est considéré comme non valide et rompt la chaîne de certificats entre Cisco Identity Service (IdS) et le fournisseur d'identité (IdP).

Solution

1. Vérifiez la date d'expiration du certificat SAML

2. Régénérer le certificat SAML

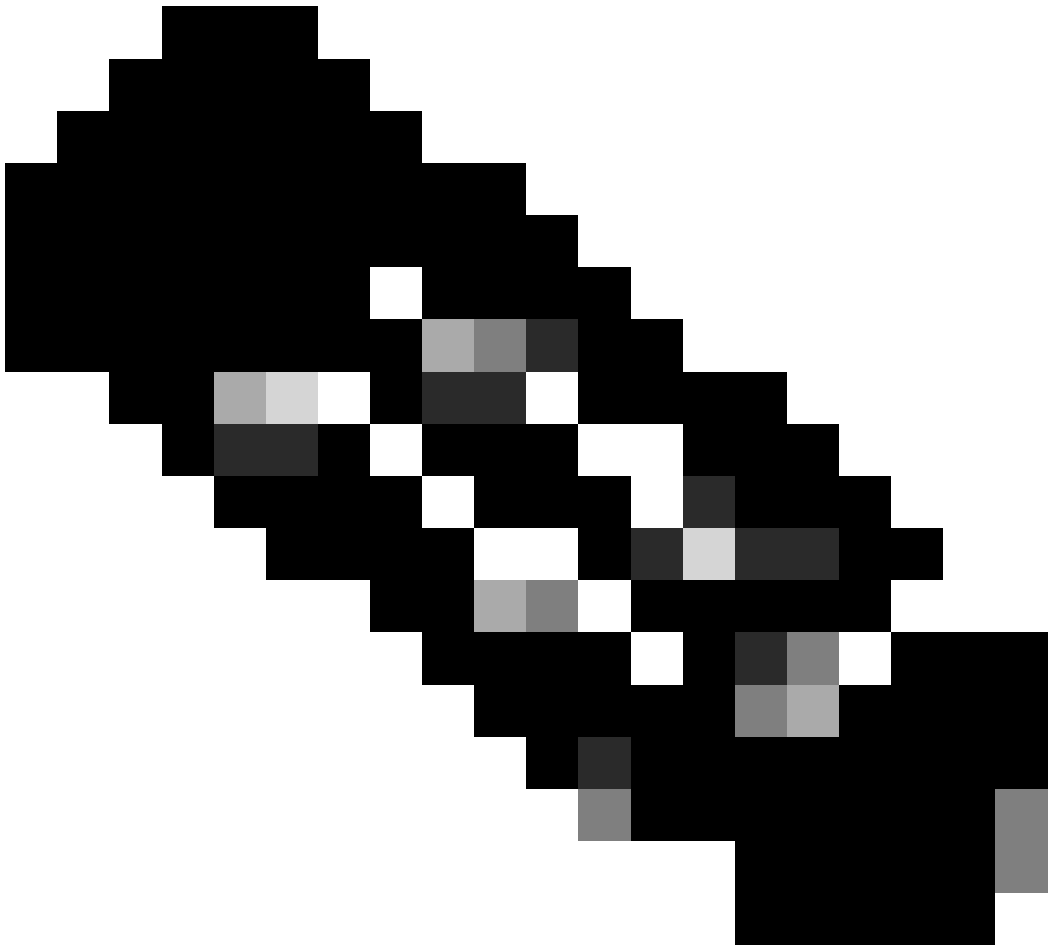
3. Téléchargez le fichier sp.xml

4. Récupérez le certificat SAML du fichier sp.xml

5. Remplacez l'ancien certificat SAML par le nouveau certificat SAML dans l'IdP

6. Reportez-vous à la section Référence pour connaître les étapes détaillées

---



(Remarque : {étant donné que seul le certificat SAML a changé, l'échange de

---

métadonnées IdS vers IdP n'est pas requis})

Modification de l'algorithme de hachage sécurisé dans le fournisseur d'identités (IdP)

Supposons que vous travaillez dans un environnement PCCE/UCCE existant avec l'authentification unique. IdP et le serveur Cisco IdS ont été configurés avec l'algorithme de hachage sécurisé SHA-1. Compte tenu de la faiblesse du SHA-1 nécessaire pour changer l'algorithme de hachage sécurisé en SHA-256.

Solution

1. Modifiez l'algorithme de hachage sécurisé dans la partie de confiance de confiance AD FS (SHA-1 à SHA-256)

2. Modifiez l'algorithme de hachage sécurisé dans l'éditeur IdS sous Clés et certificat (SHA-1 à SHA-256)

3. Régénérez le certificat SAML dans l'éditeur IdS

4. Téléchargez le fichier sp.xml

5. Récupérez le certificat SAML du fichier sp.xml

6. Remplacez l'ancien certificat SAML par le nouveau certificat SAML dans l'IdP

7. Reportez-vous à la section Référence pour connaître les étapes détaillées

Modification de l'adresse IP ou du nom d'hôte du serveur Cisco IdS - Serveur de publication CUIC/LiveData/IdS co-résident ou Serveur de publication IdS autonome reconstruit - Abonné CUIC/LiveData/IdS co-résident ou Abonné IdS autonome reconstruit

Ces situations sont rares et il est vivement recommandé de recommencer avec la configuration SSO (Single Sign-On) pour garantir que la fonctionnalité SSO dans l'environnement de production est restaurée rapidement et efficacement. Il est essentiel de hiérarchiser cette reconfiguration afin de minimiser toute interruption des services SSO dont dépendent les utilisateurs.

Solution

1. Supprimez la partie de confiance de confiance existante des services ADFS (Active Directory Federation Services)

2. Téléchargez le certificat SSL AD FS dans le serveur Cisco IdS pour faire confiance à

3. Téléchargez le fichier sp.xml

4. Reportez-vous à la section Référence et au Guide des fonctionnalités pour connaître les étapes détaillées

5. Configurer la partie de confiance dans AD FS

6. Ajouter les règles de réclamation

7. Activer l'assertion SAML signée

8. Télécharger les métadonnées de fédération AD FS

9. Téléchargez les métadonnées de fédération sur le serveur Cisco IdS

10. Exécution du test SSO

Référence

Comment ajouter une partie d'approbation de confiance dans ADFS ou

Comment activer l'assertion SAML signée

Consultez ce document pour connaître les étapes détaillées : Guide des fonctionnalités d'UCCE 12.6.1

Comment télécharger le certificat SSL AD FS vers l'approbation Cisco IdS tomcat

1. Téléchargez ou récupérez le certificat SSL AD FS

2. Accédez à la page Cisco IdS Publisher OS Administration

3. Connectez-vous avec les informations d'identification de l'administrateur OS

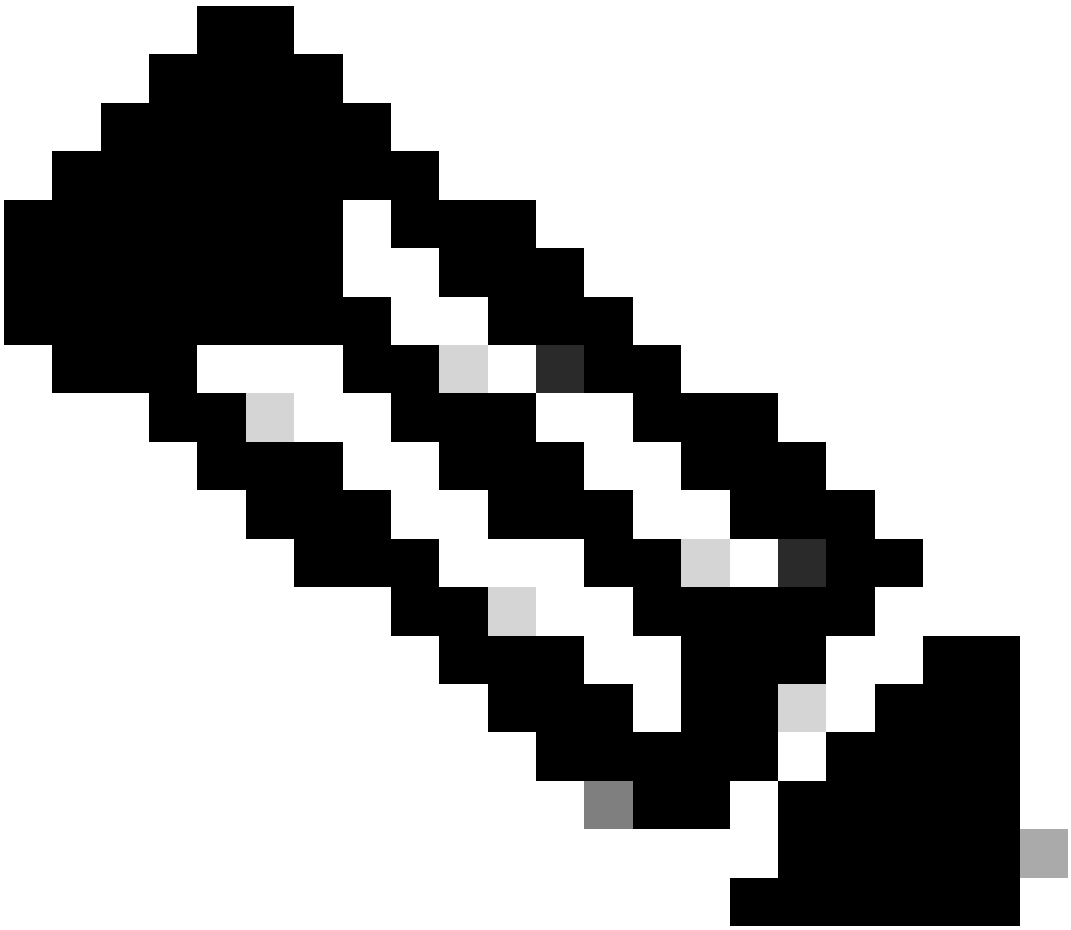
4. Accédez à Security > Certificate Management

5. Cliquez sur Upload Certificate/Certificate Chain et une fenêtre contextuelle s'ouvre

6. Cliquez sur le menu déroulant et sélectionnez tomcat-trust on Certificate Purpose

7. Cliquez sur Parcourir et sélectionnez le certificat SSL AD FS

8. Cliquez sur Télécharger



(Remarque : {Les certificats de confiance sont répliqués sur les noeuds Abonné. Vous n'avez pas besoin de télécharger sur le noeud Abonné.})

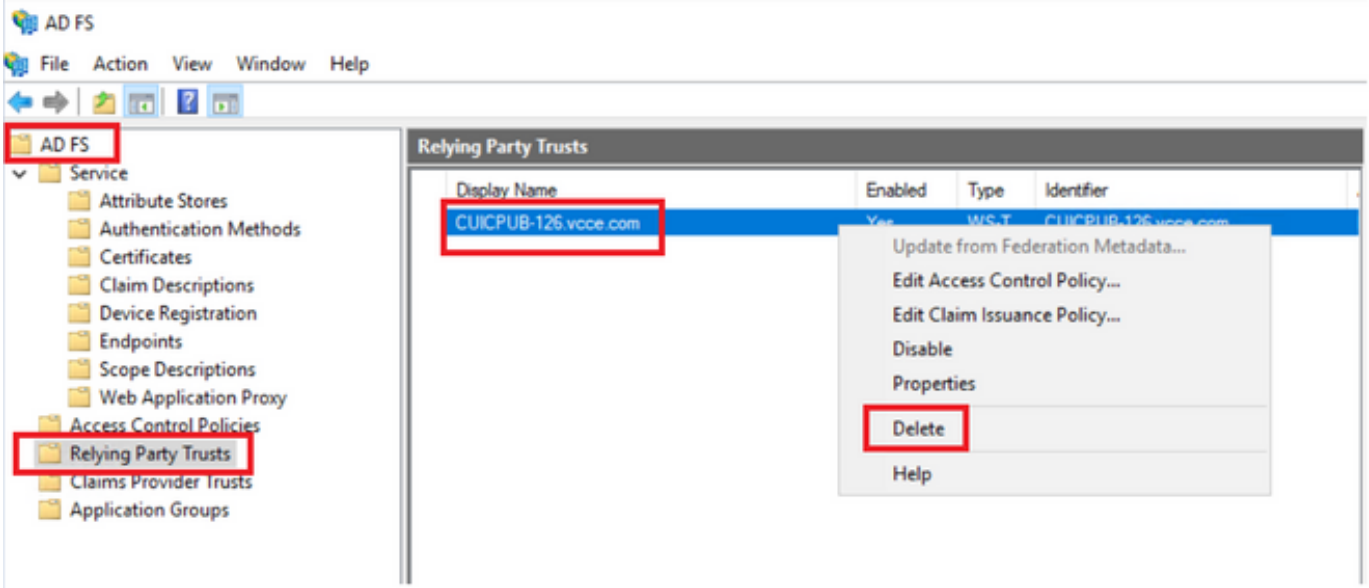
Suppression de la partie d'approbation de confiance dans AD FS

1. Connectez-vous au serveur du fournisseur d'identités (IdP) avec les informations d'identification d'administrateur

2. Ouvrez le Gestionnaire de serveur et choisissez AD FS >Outils > Gestion AD FS

3. Dans l'arborescence de gauche, sélectionnez les approbations de partie de confiance sous AD FS

4. Cliquez avec le bouton droit sur le serveur Cisco IdS et sélectionnez Supprimer



Comment vérifier ou modifier l'algorithme de hachage sécurisé configuré dans le fournisseur d'identité (IdP)

1. Connectez-vous au serveur du fournisseur d'identités (IdP) avec les informations d'identification d'administrateur

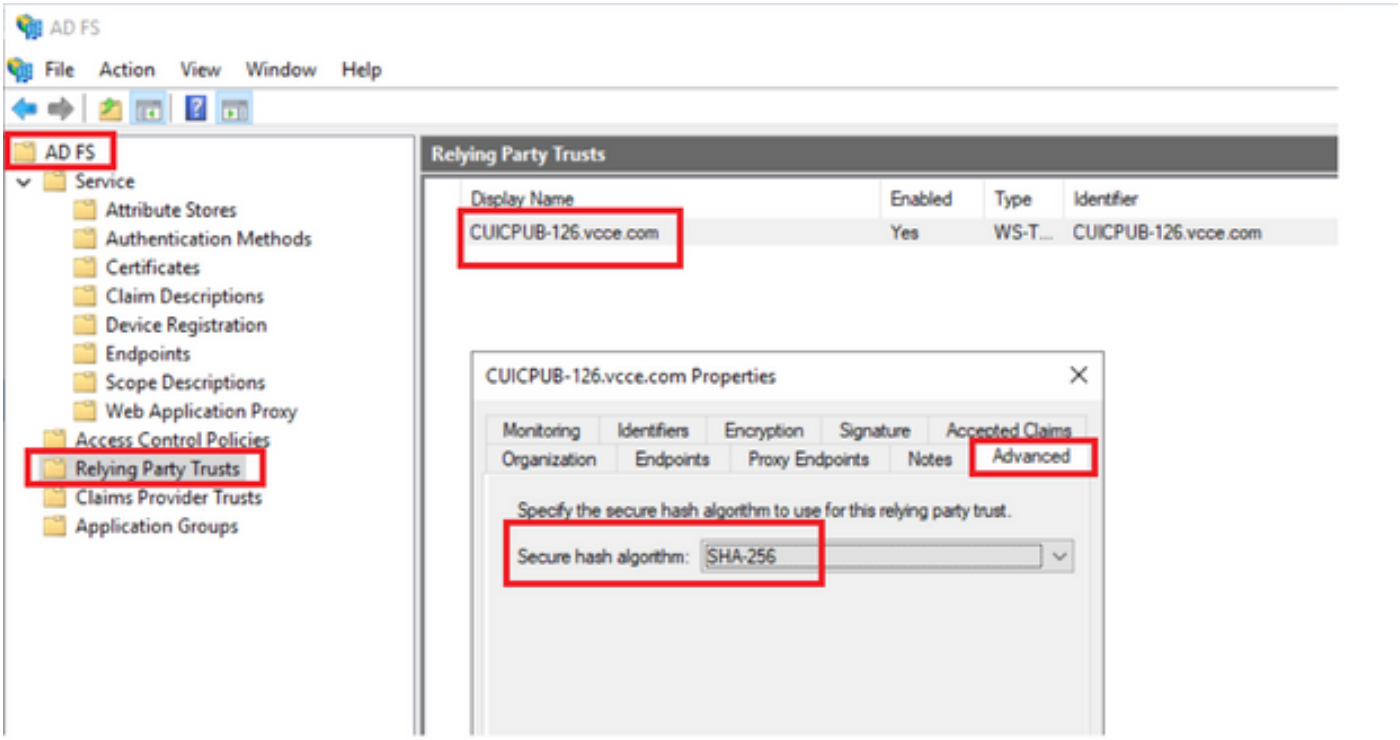
2. Ouvrez le Gestionnaire de serveur et choisissez AD FS >Outils > Gestion AD FS

3. Dans l'arborescence de gauche, sélectionnez les approbations de partie de confiance sous AD FS

4. Cliquez avec le bouton droit sur le serveur Cisco IdS et sélectionnez Propriétés

5. Accédez à l'onglet Avancé

6. L'option Secure Hash Algorithm affiche l'algorithme de hachage sécurisé configuré sur le serveur AD FS.



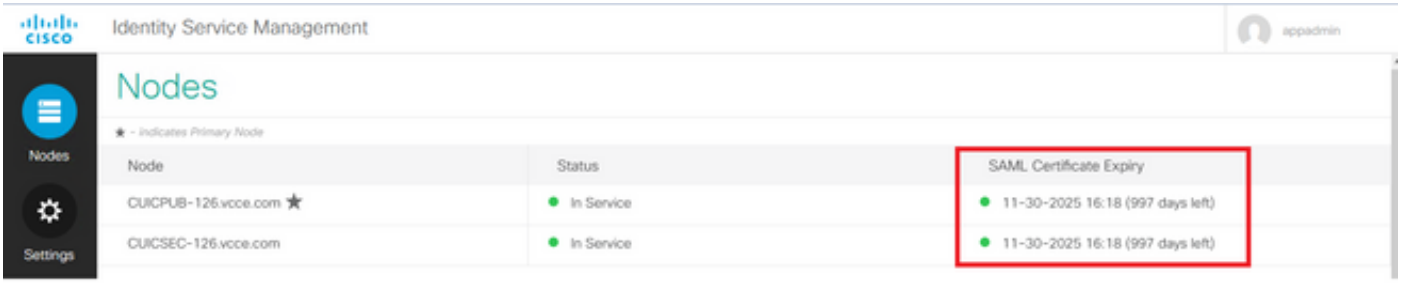
7. Cliquez sur le menu déroulant et sélectionnez l'algorithme de hachage sécurisé souhaité.

Vérification du certificat SAML du serveur Cisco IdS Date d'expiration

1. Connectez-vous au noeud Éditeur ou Abonné du serveur Cisco IdS avec les informations d'identification de l'utilisateur de l'application

2. Une fois la connexion réussie, la page atterrit sur Identity Service Management > Nodes

3. Affiche le noeud Éditeur et abonné Cisco IdS, l'état et l'expiration du certificat SAML



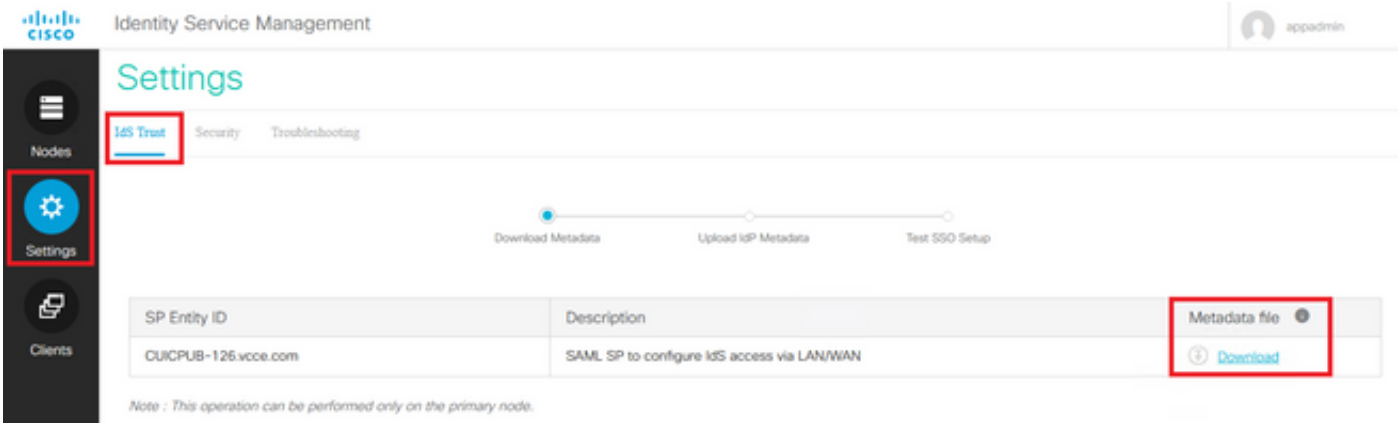
Comment télécharger les métadonnées du serveur Cisco IdS

1. Connectez-vous au noeud Cisco IdS Publisher avec les informations d'identification de l'utilisateur de l'application

2. Cliquez sur l'icône Paramètres

3. Accédez à l'onglet Confiance IDS

4. Cliquez sur le lien Download (Télécharger) pour télécharger les métadonnées du cluster Cisco IdS



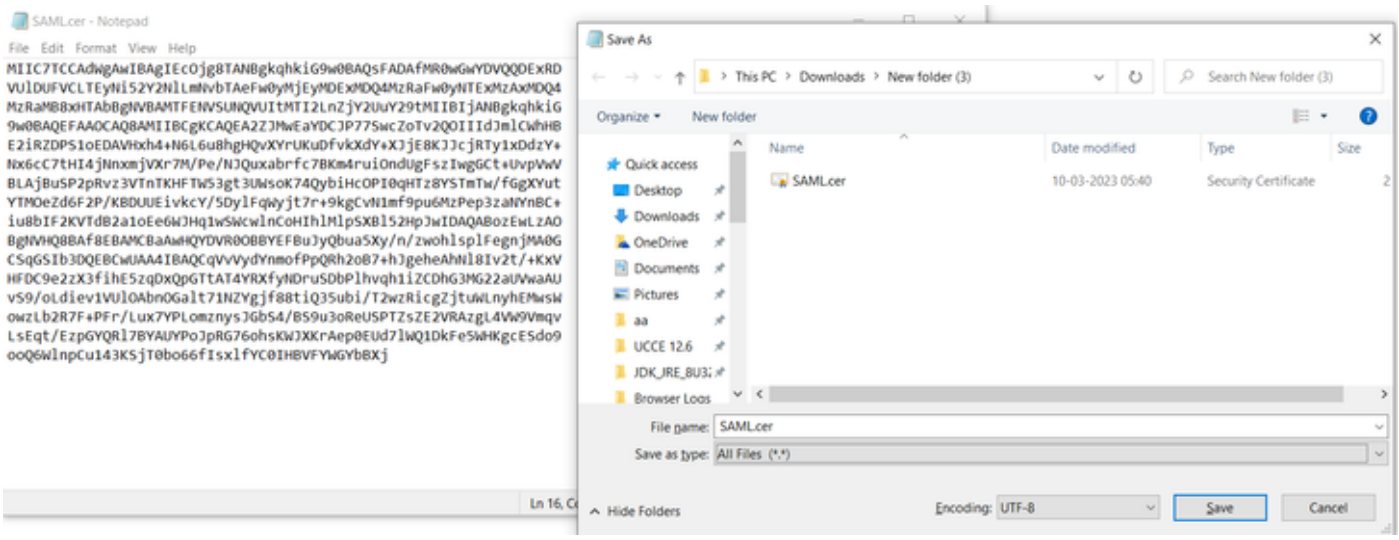
Comment récupérer le certificat SAML du fichier sp.xml

1. Ouvrez le fichier sp.xml avec un éditeur de texte

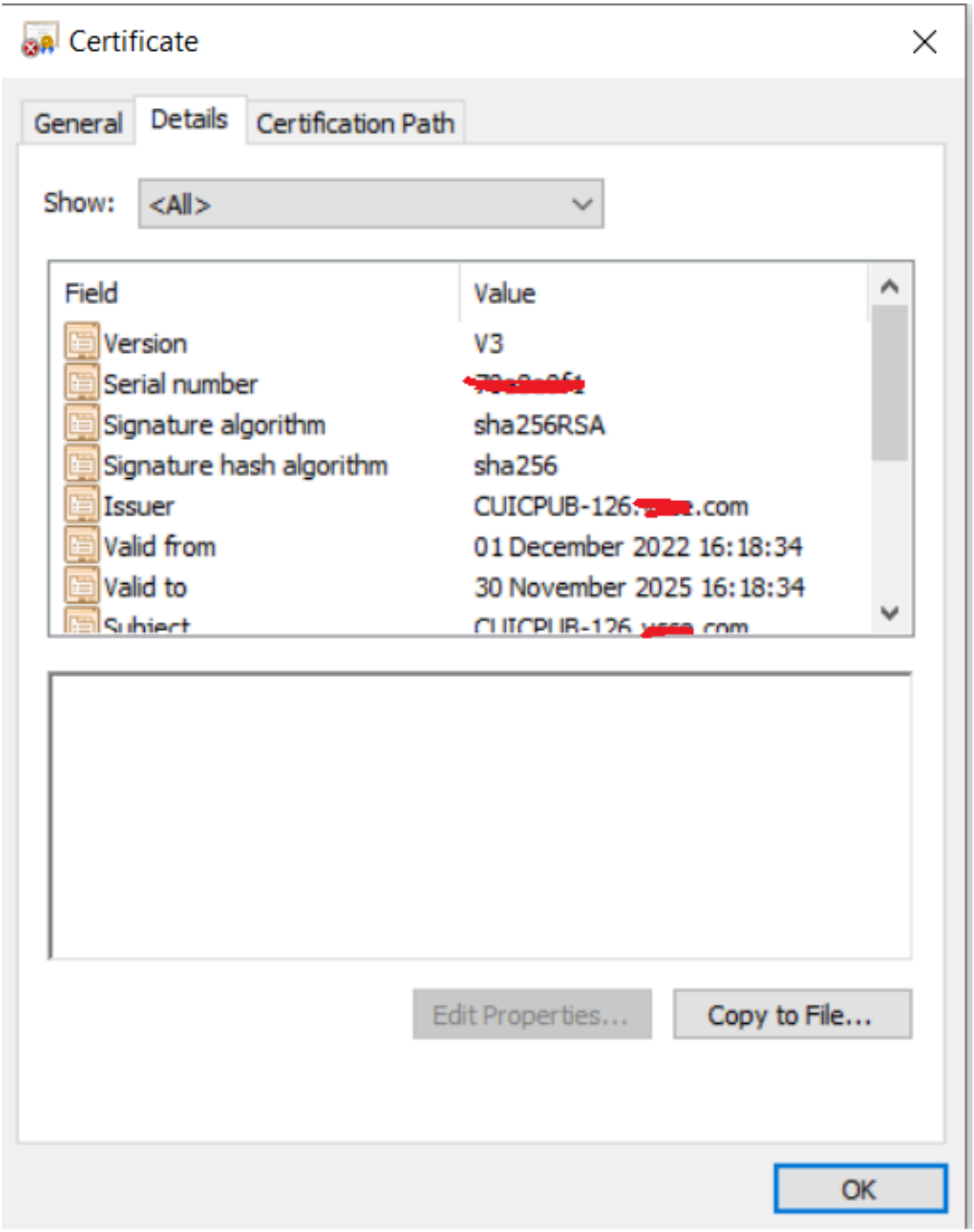
2. Copiez les données brutes entre l'en-tête <ds : X509Certificate></ds : X509Certificate>

3. Ouvrez un autre éditeur de texte et collez les données copiées

4. enregistrez le fichier au format .CER



5. Ouvrez le certificat pour vérifier les informations du certificat



Comment remplacer le certificat SAML dans AD FS

1. Copiez le fichier de certificat SAML sur le serveur AD FS qui est récupéré à partir du fichier sp.xml

2. Ouvrez le Gestionnaire de serveur et choisissez AD FS >Outils > Gestion AD FS

3. Dans l'arborescence de gauche, sélectionnez les approbations de partie de confiance sous AD FS

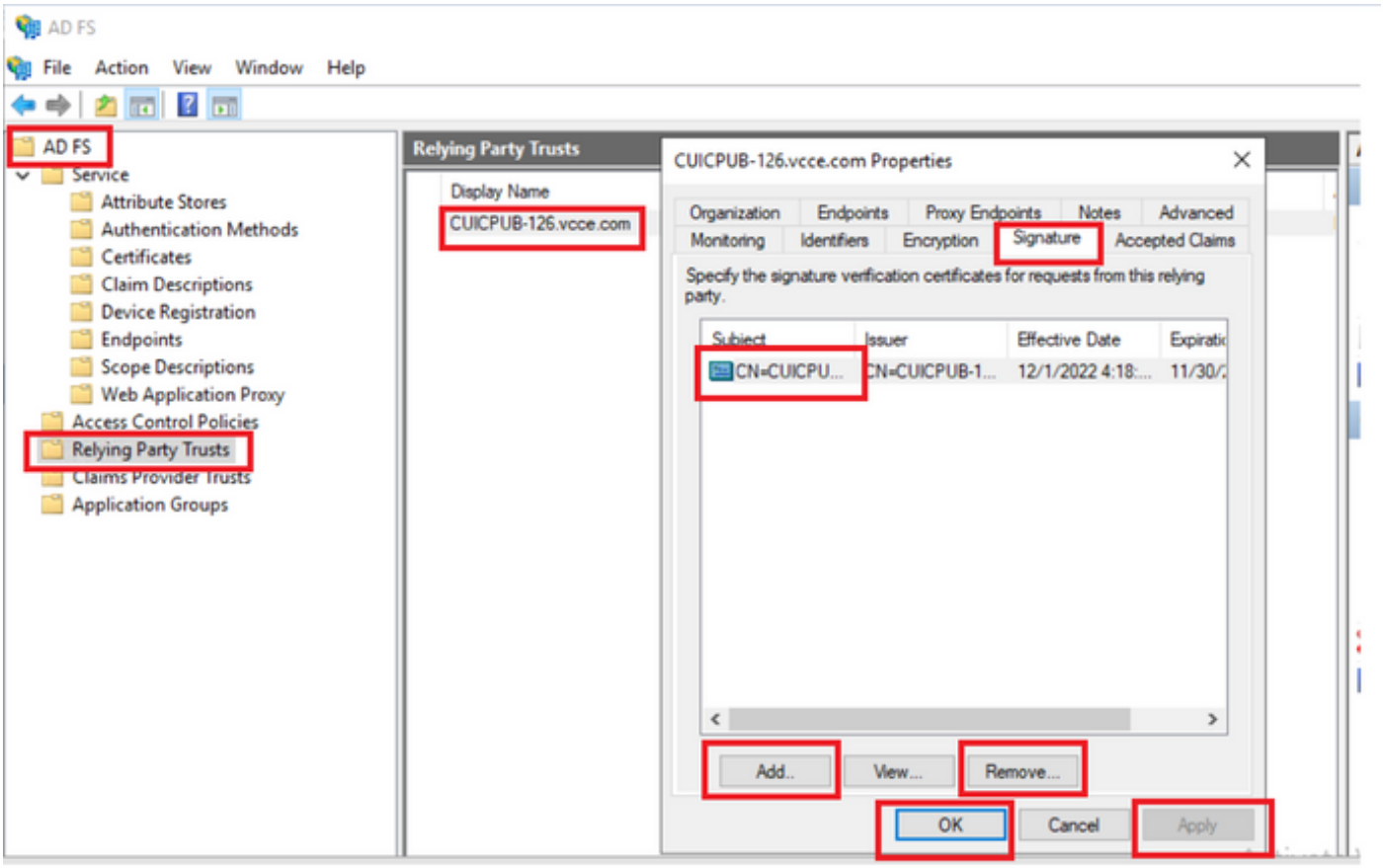
4. Cliquez avec le bouton droit sur le serveur Cisco IdS et sélectionnez Propriétés

5. Accédez à l'onglet Signature

6. Cliquez sur Ajouter et choisissez le certificat SAML nouvellement généré

7. Sélectionnez l'ancien certificat SAML et cliquez sur Supprimer

8. Appliquer et enregistrer



Comment régénérer le certificat SAML dans le serveur Cisco IdS

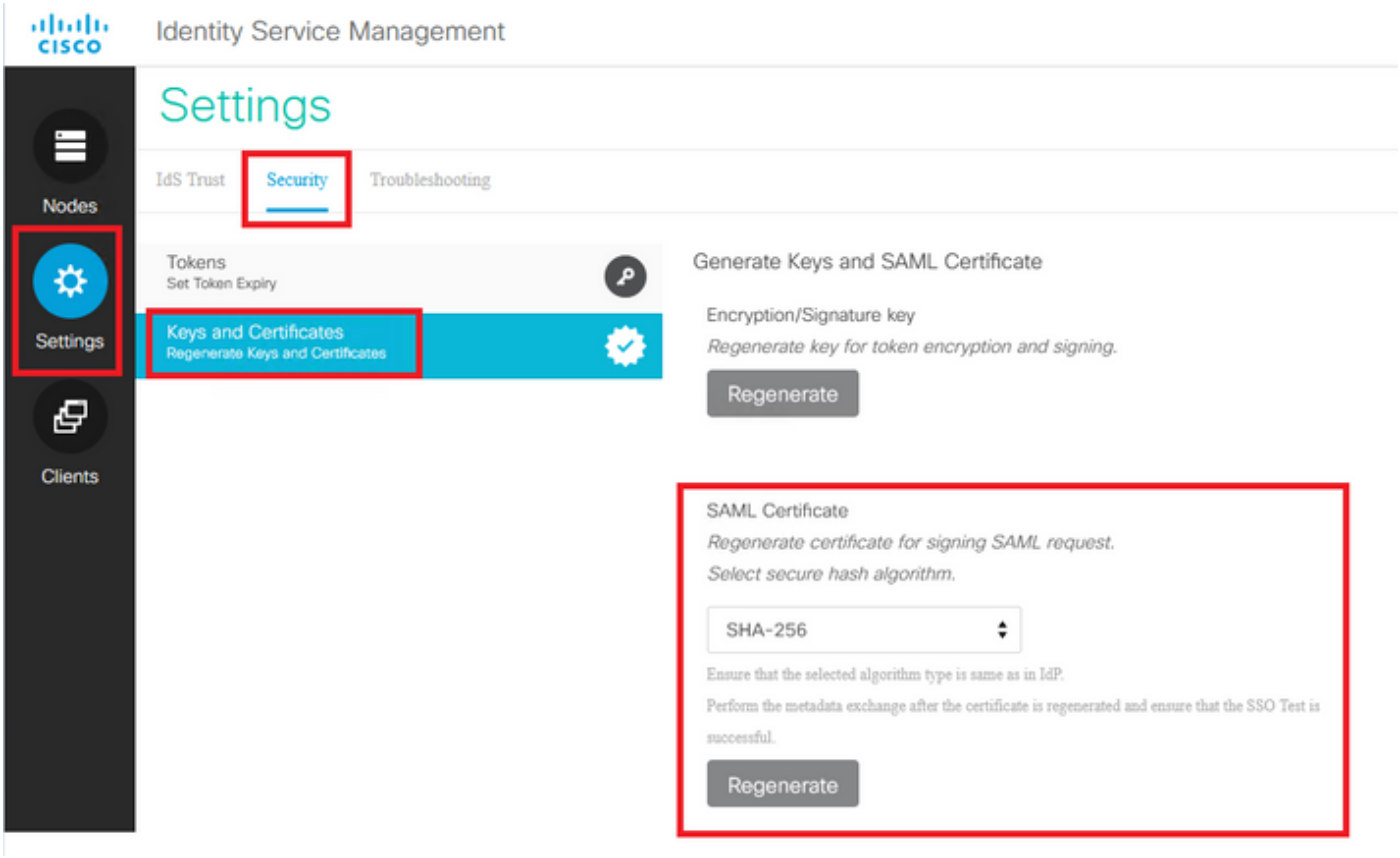
1. Connectez-vous au noeud Cisco IdS Publisher avec les informations d'identification de l'utilisateur de l'application

2. Cliquez sur l'icône Paramètres

3. Accédez à l'onglet Sécurité

4. Sélectionnez l'option Clés et certificats

5. cliquez sur le bouton Régénérer sous la section Certificat SAML (mis en surbrillance)



Test SSO

En cas de modification du certificat SAML, assurez-vous que TEST SSO a réussi sur le serveur Cisco IdS et réenregistrez toutes les applications à partir de la page CCEAdmin.

1. Accédez à la page CCEAdmin à partir du serveur AW principal

2. Connectez-vous au portail CCEAdmin avec les privilèges de niveau admin

3. Accédez à Overview > Features > Single-Sign-On

4. Cliquez sur le bouton Register sous Register with Cisco Identity Service

5. Exécution du test SSO

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.