Unified Contact Center Enterprise (UCCE) simple se connectent les Certificats (SSO) et la configuration

Contenu

Introduction

Ce document décrit les configurations de certificat qui sont exigées pour UCCE SSO. La configuration de cette caractéristique implique plusieurs Certificats pour HTTPS, signature numérique et cryptage.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 11.5 UCCE
- Microsoft Active Directory (AD) - AD installé sur des Windows Server
- Version 2.0/3.0 du service de fédération de Répertoire actif (ADFS)

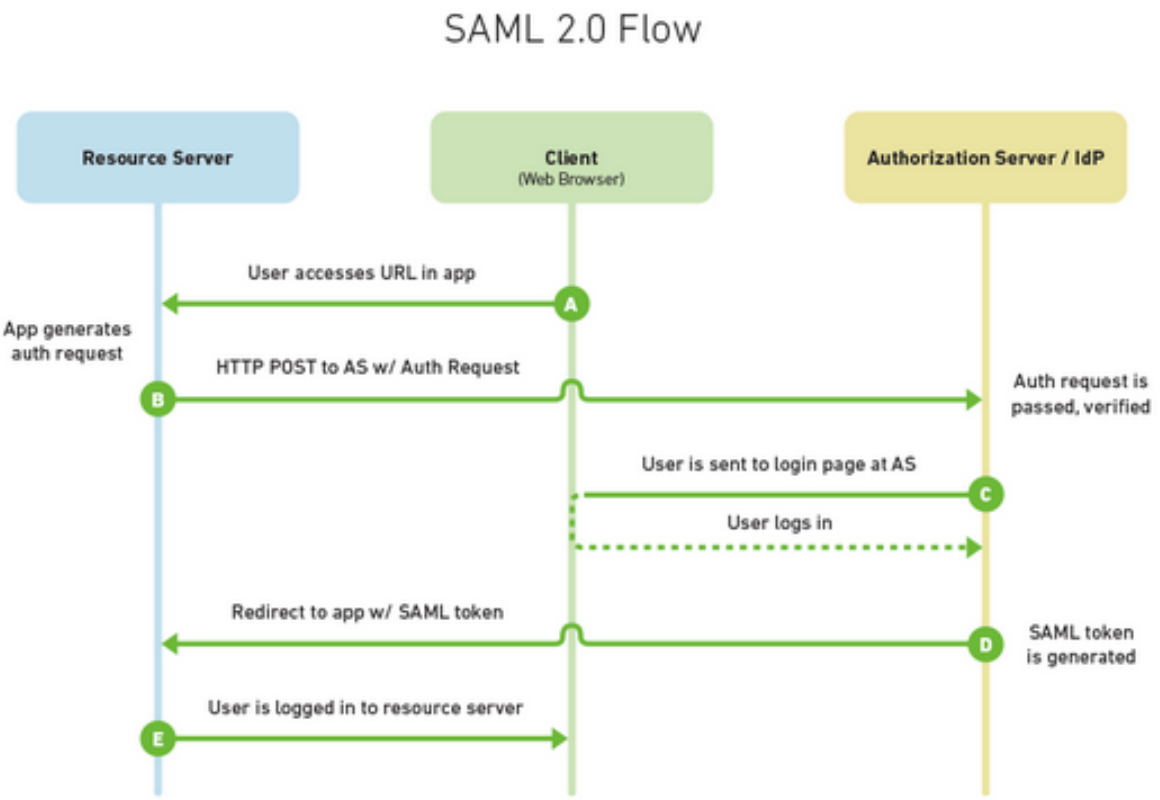
Composants utilisés

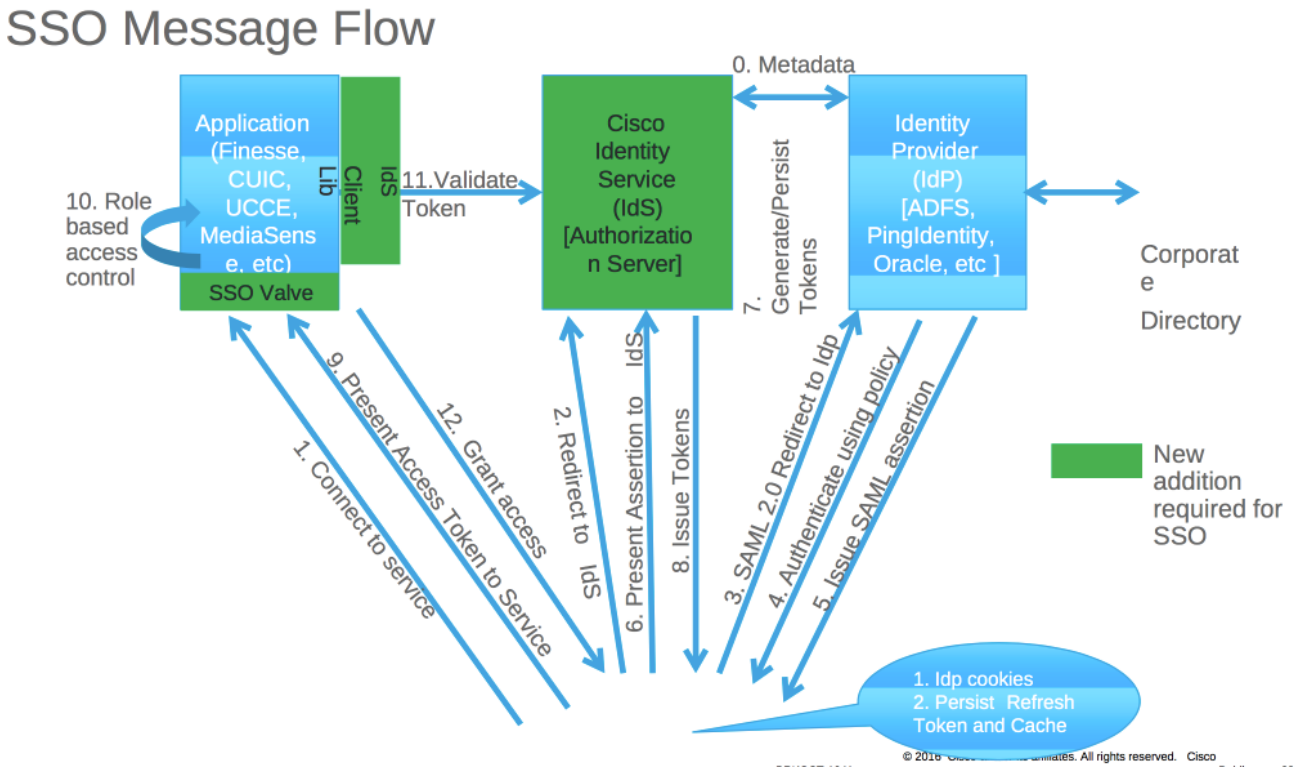
UCCE 11.5

Windows 2012 R2

Partie A. SSO Message Flow

The most common SAML flow is shown below:



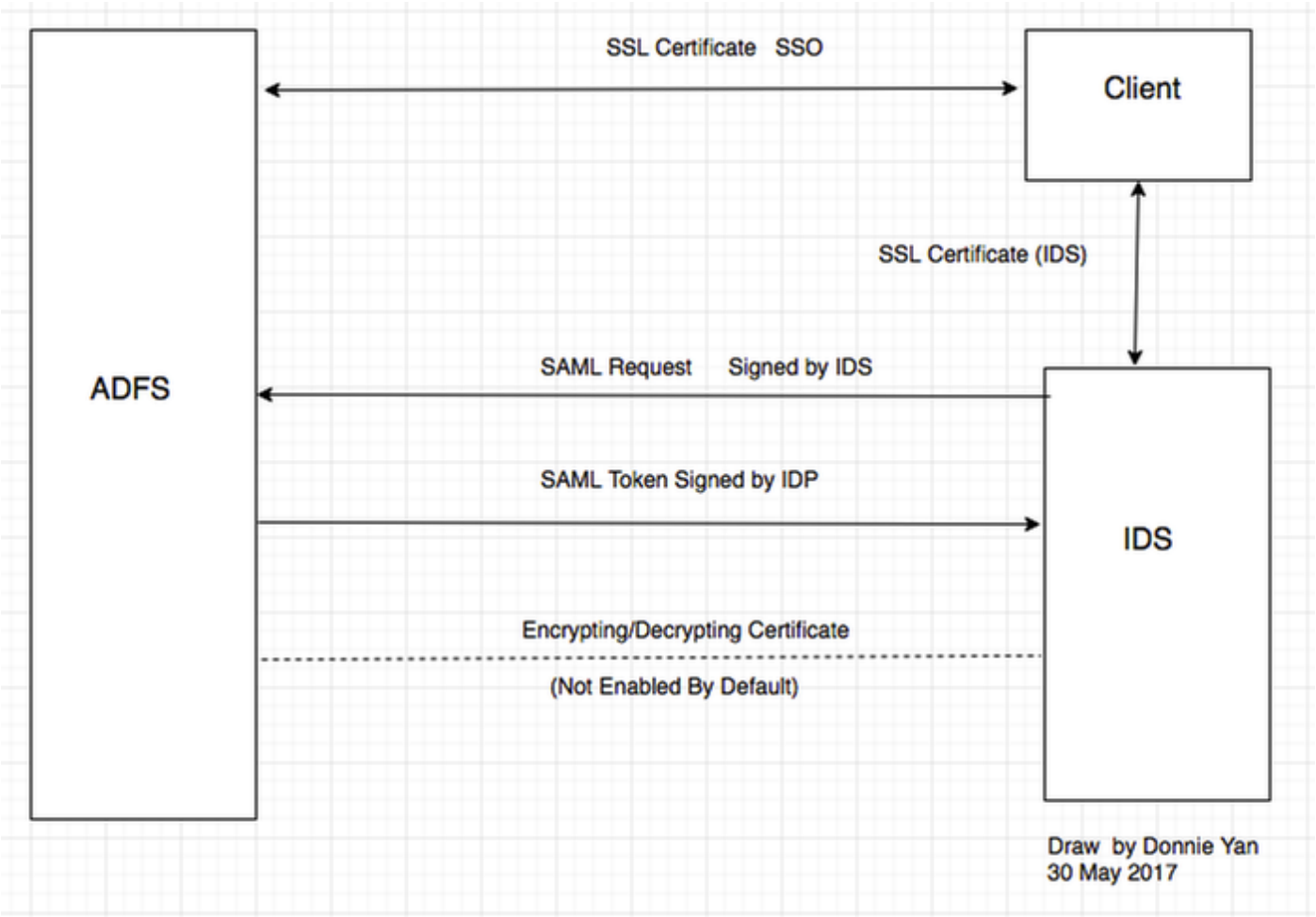


Quand SSO est activé, quand l'agent ouvre une session à l'appareil de bureau de finesse :

- Le serveur de finesse réoriente le navigateur d'agent pour communiquer avec la gestion d'identité (les ID)
- Les ID réoriente le navigateur d'agent au fournisseur d'identité (IDP) avec la demande SAML
- L'IDP génère le jeton SAML et passe aux ID le serveur
- Quand le jeton a été généré, chaque fois que l'agent parcourt au ppplication, il utilise ce jeton

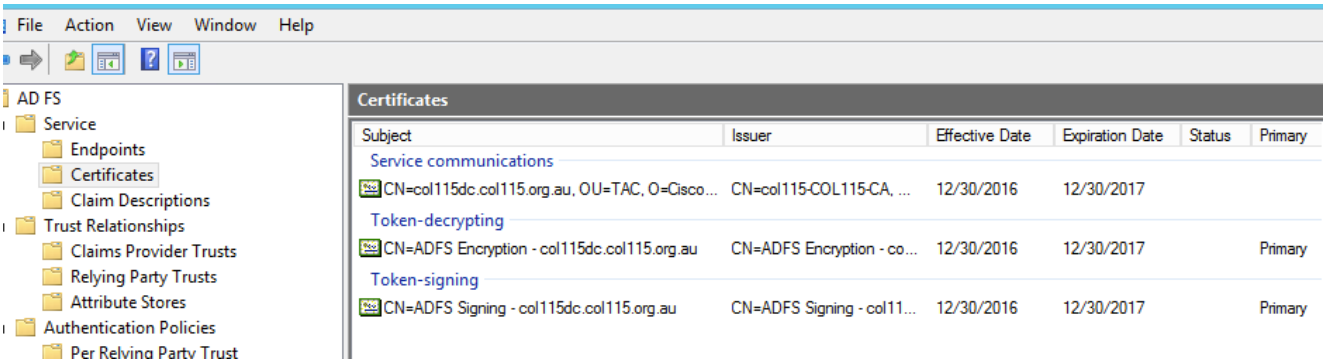
valide pour la procédure de connexion

Partie B. Certificates Used dans l'IDP et les ID



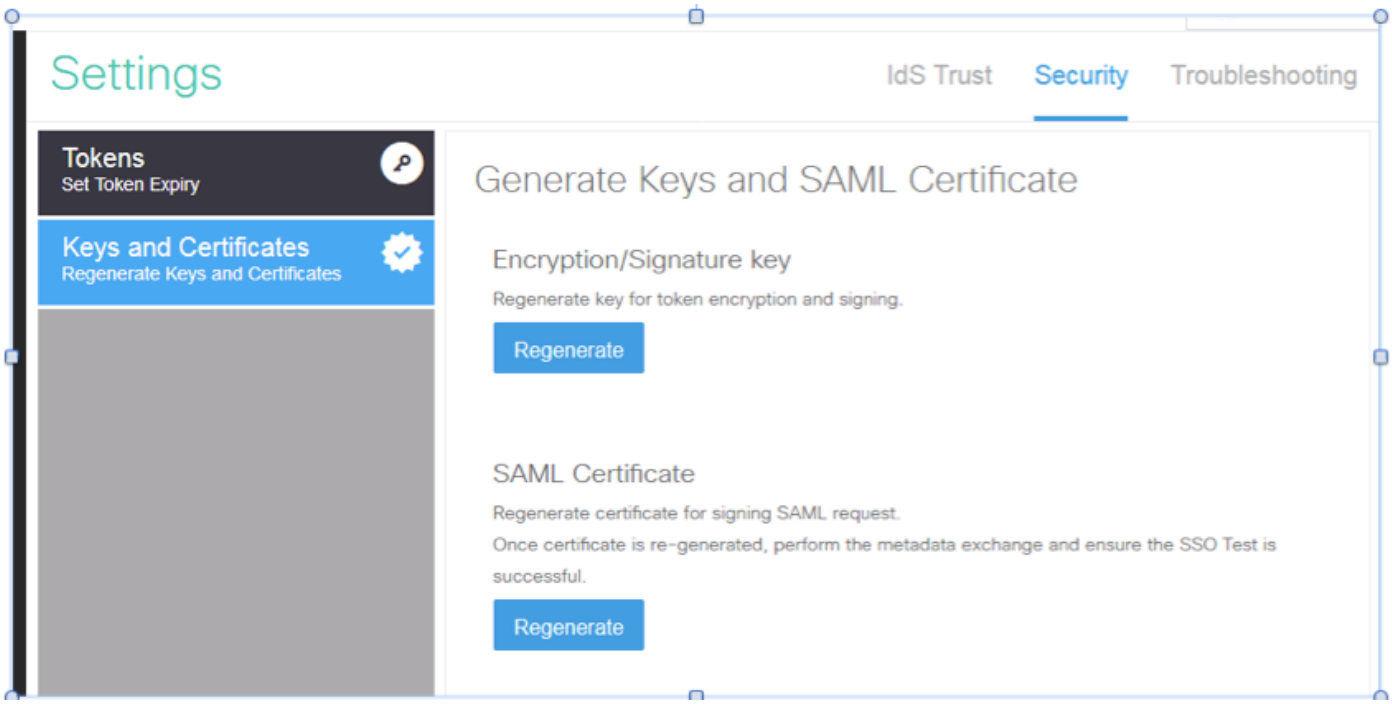
Certificats d'IDP

- Certificat ssl (SSO)
- Certificat de signature symbolique
- Jeton – déchiffrant

1. 

Certificats d'ID

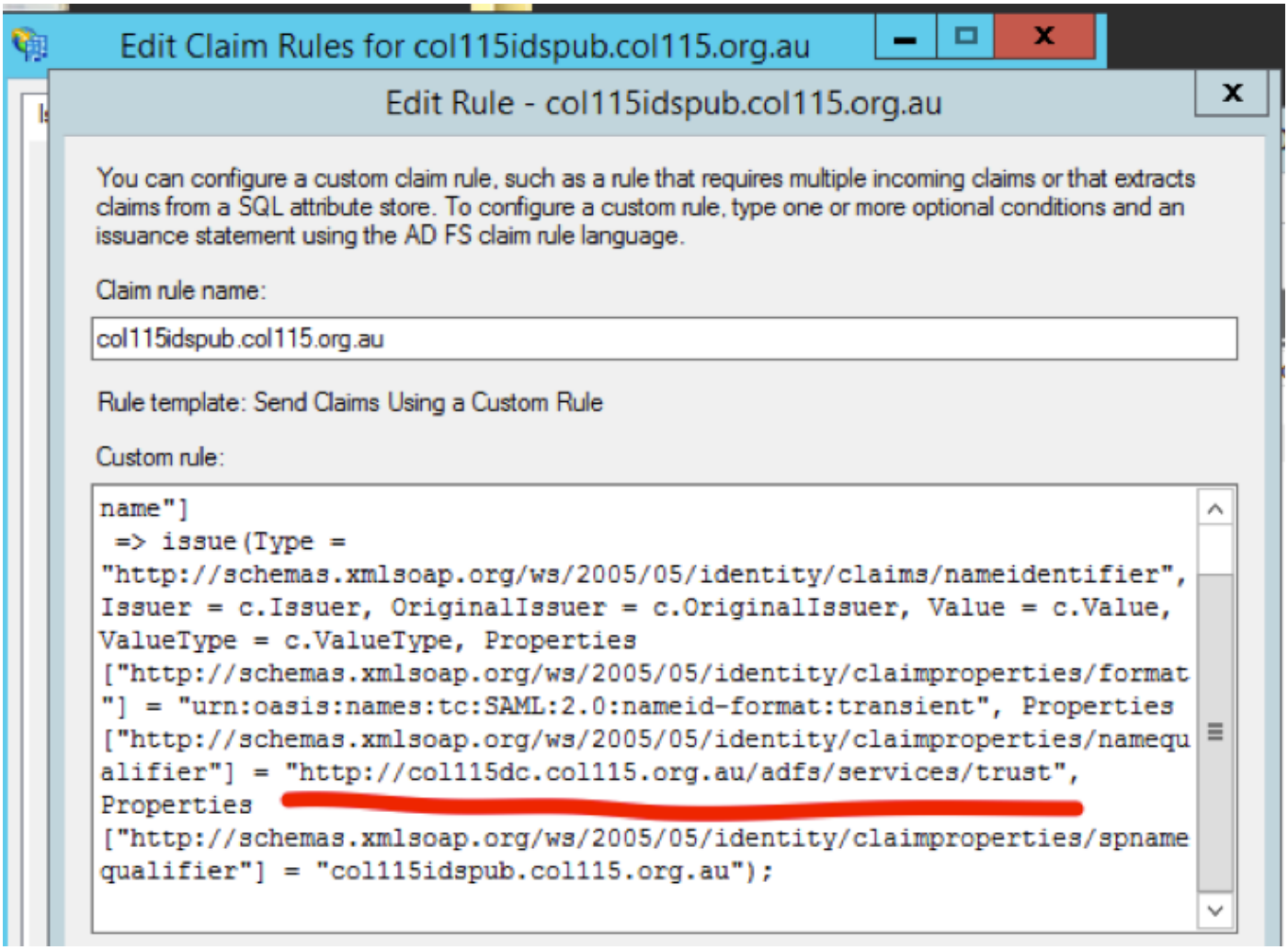
- Certificat SAML
- Clé de signature
- Clé de chiffrement



Partie C. IDP Certification en détail et configuration

Certificat ssl (SSO)

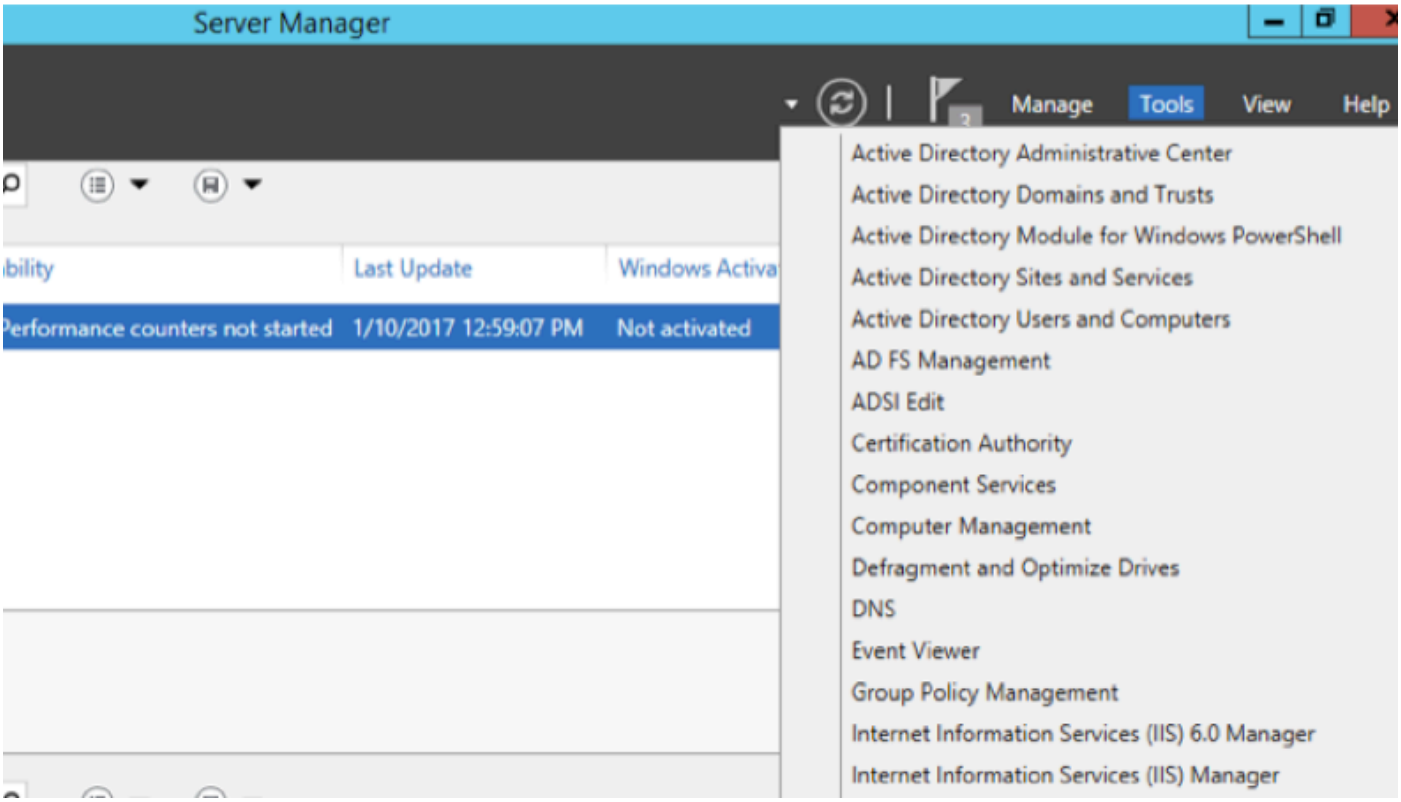
- Ce certificat est utilisé entre l'IDP et le client. Le client doit faire confiance au certificat SSO
- Le certificat ssl est placé pour chiffrer la session entre le client et le serveur d'IDP. Ce certificat n'est pas spécifique à ADFS, mais à particularité à IIS
- Le sujet du certificat ssl doit s'assortir avec le nom utilisé dans la configuration ADFS

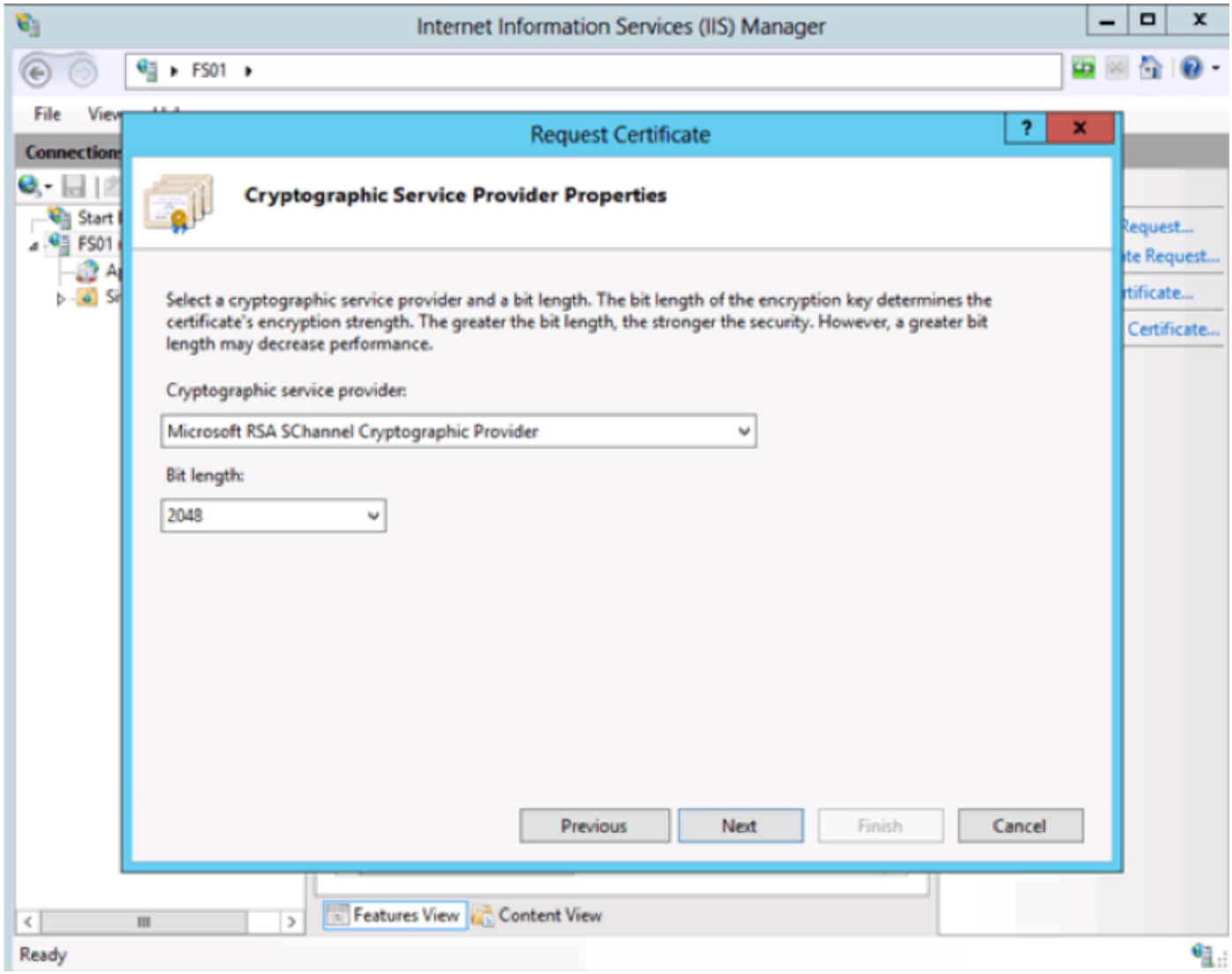


Étapes pour configurer le certificat ssl pour SSO (laboratoire local avec le CA interne signé)

Étape 1. Créez le certificat ssl avec la demande de signature de certificat (CSR) et signez par CA interne pour ADFS.

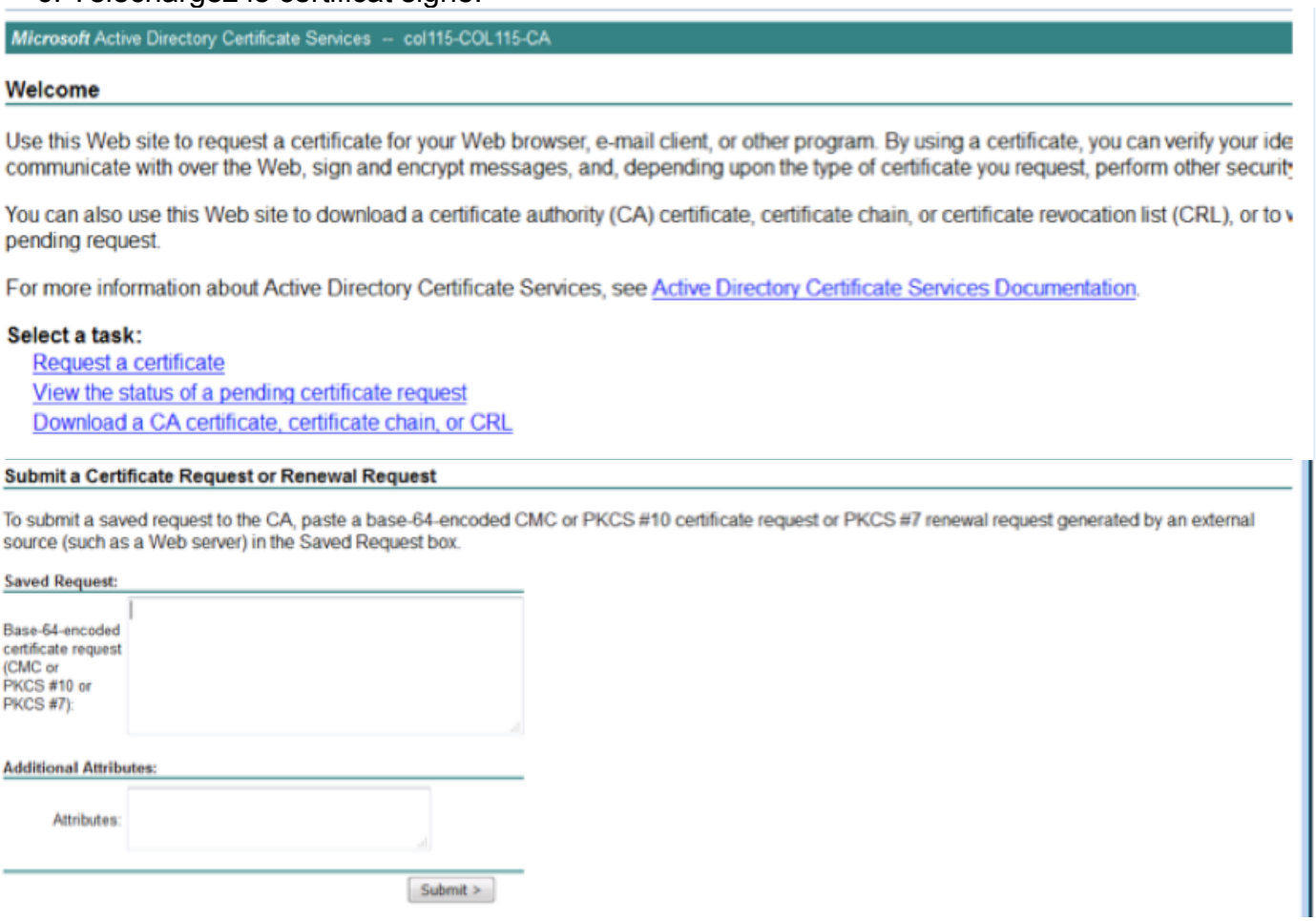
1. Ouvrez le gestionnaire du serveur.
2. Outils de clic.
3. Gestionnaire de l'Internet Information Services de clic (IIS).
4. Sélectionnez le serveur local.
5. Certificats de serveur choisis.
6. Caractéristique ouverte de clic (panneau d'action).
7. Le clic **créent la** demande de certificat.
8. Laissez le fournisseur de services cryptographique au par défaut.
9. Changez la **longueur de bit à 2048**.
10. Cliquez sur **Next** (Suivant).
11. Sélectionnez un emplacement pour sauvegarder le fichier demandé.
12. Cliquez sur **Finish** (Terminer).





Étape 2. Le CA signe le CSR qui a été généré de l'étape 1.

1. **Ouvrez le** serveur CA pour chanter ce **HTTP** CSR **: IP address >/certsrv/de serveur <CA**.
2. Demande de clic un certificat.
3. Demande de certificat avancée par clic.
4. **Copiez le** CSR dans la demande de certificat encodée par Based-64.
5. **Soumettez**.
6. Téléchargez le certificat signé.



Étape 3. Installez le certificat signé de nouveau au serveur ADFS et l'assignez à la caractéristique ADFS.

1. Installez le certificat signé de nouveau au serveur ADFS. Afin de faire ceci, **ouvrez les données Internet Services(IIS) Manager> de manager>Tools>Click de serveur**.

Caractéristique de Server>Server Certificate>Open de gens du pays (panneau d'action).

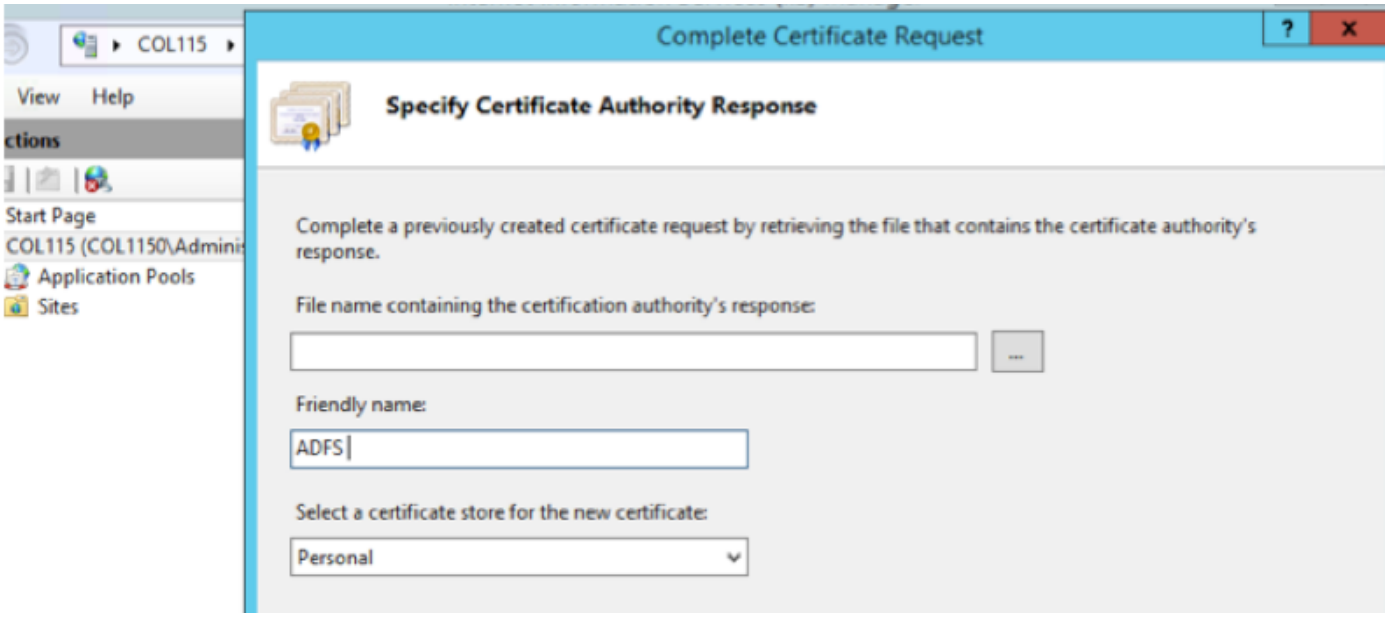
2. Demande complète de certificat de clic.

3. Sélectionnez le chemin au fichier complet CSR que vous vous êtes terminé et avez téléchargé du fournisseur de certificat de tiers.

4. **Écrivez le** nom amical pour le certificat.

5. Personnel choisi comme mémoire de certificat.

6. Cliquez sur **OK**.



7. À ce stade, tout le certificat ont été ajoutés. Maintenant, l'affectation de certificat ssl est exigée.

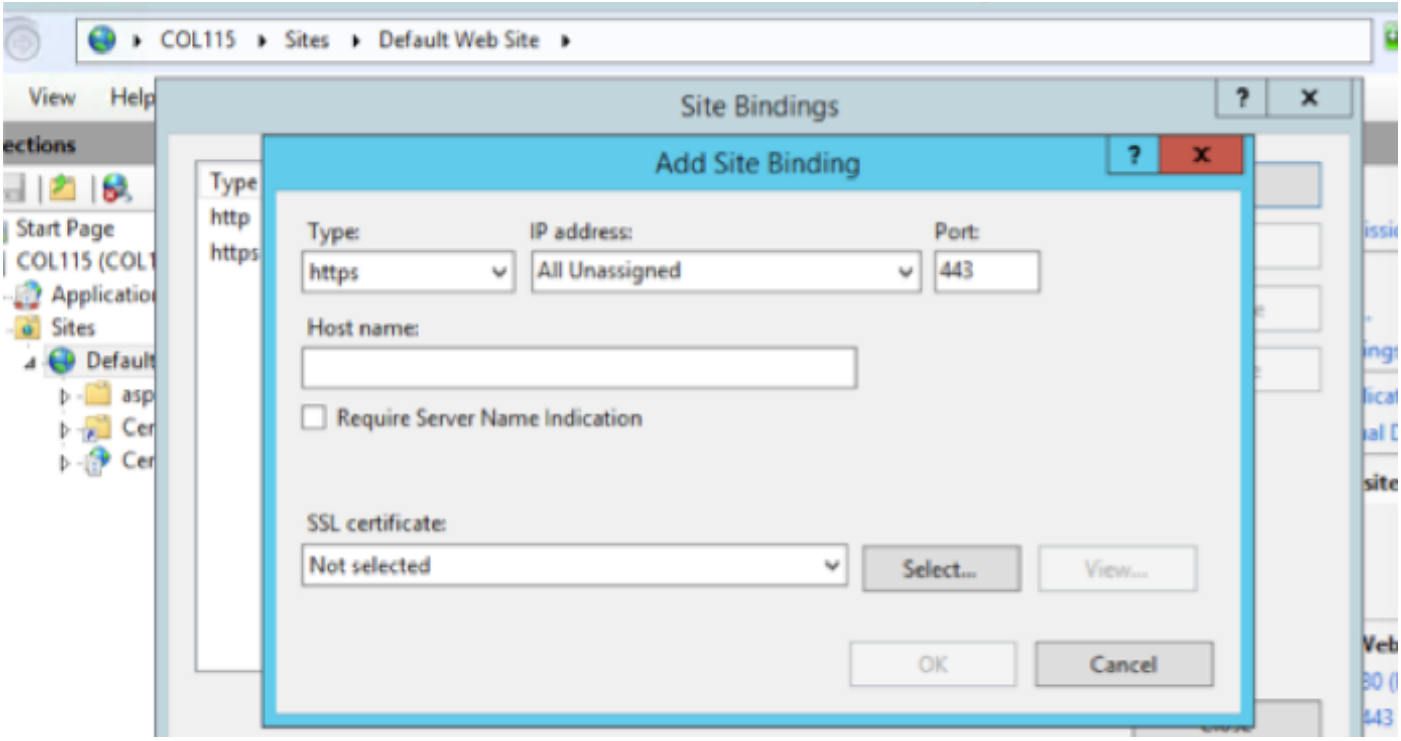
8. **Développez les attaches locales de >Click de site Web de par défaut de Sites>Select de server>Expand** (volet d'actions).

9.Click **ajoutent**.

10. **Changez le** type à HTTPS.

11. Sélectionnez votre certificat du menu de baisse vers le bas.

12. Cliquez sur **OK**.



Maintenant, le certificat ssl pour le serveur ADFS a été assigné.

Note: Pendant l'installation de la caractéristique ADFS, le certificat ssl précédent doit être

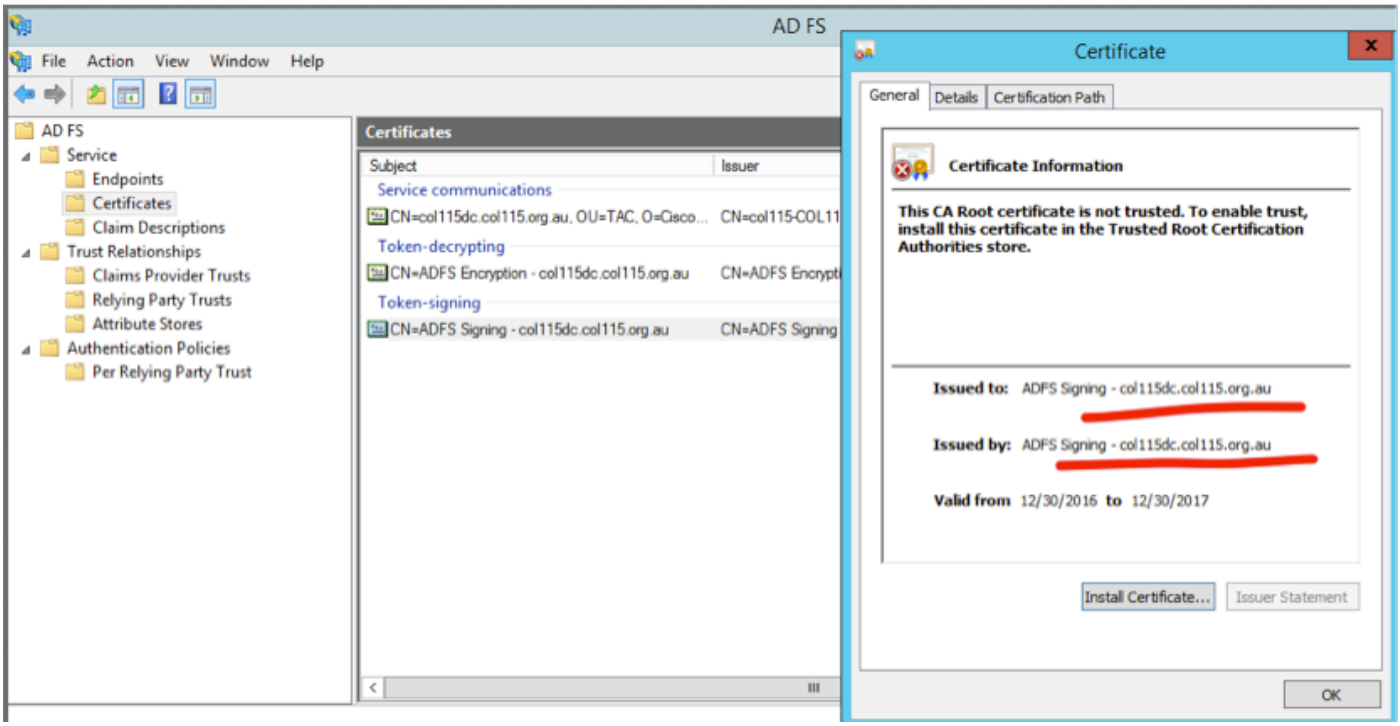
utilisé.

Certificat de signature symbolique

ADFS génère le certificat auto-signé pour le certificat de signature symbolique. Par défaut il est valable une année.

On brûle légèrement le jeton SAML généré par IDP par clé privée ADFS (pièce privée de signature symbolique de certificat). Puis, les ID emploie la clé publique ADFS pour vérifier. Ceci garantit que le jeton signé n'est pas d'obtenir modifié.

Le certificat de signature de jeton est utilisé chaque fois qui les besoins de l'utilisateur d'accéder à une application comptante d'interlocuteur (ID de Cisco).

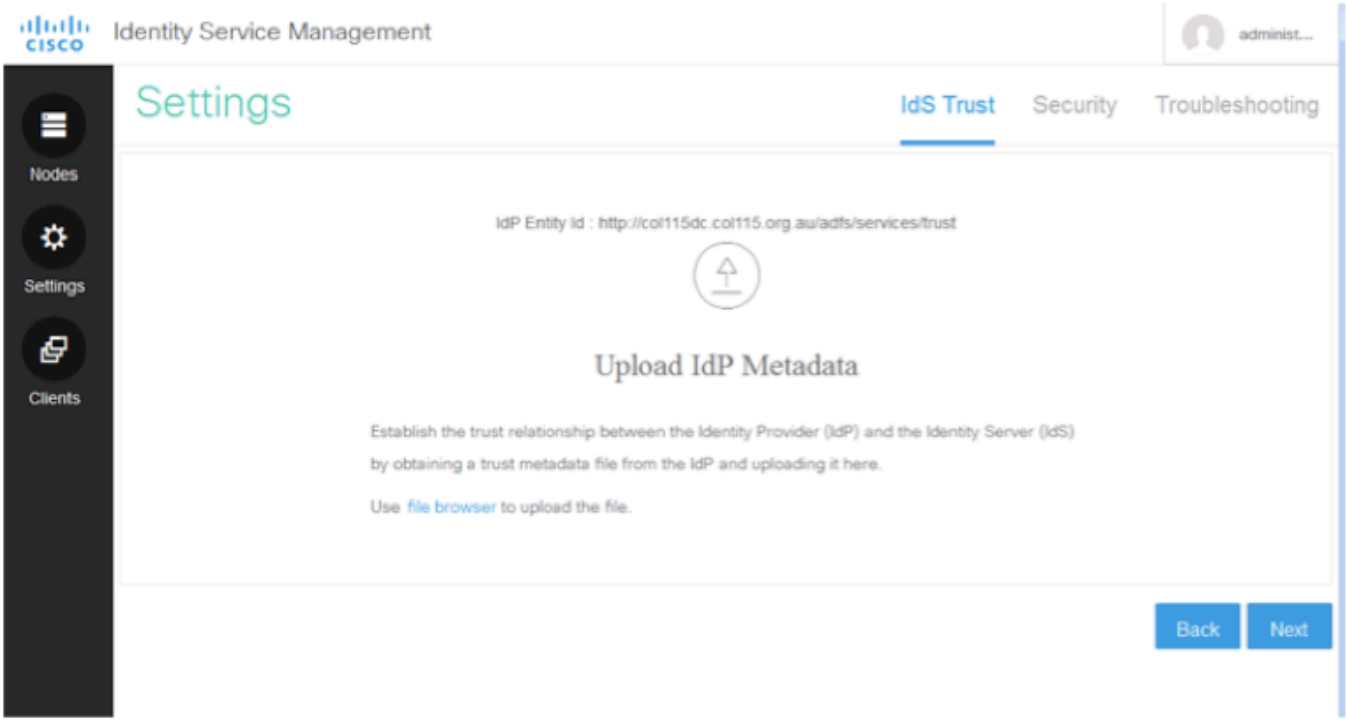


Comment le serveur d'ID de Cisco obtient-il la clé publique du certificat symbolique de chant ?

Ceci est fait en téléchargeant des métadonnées ADFS au serveur d'ID, et puis en passant la clé publique d'ADFS au serveur d'ID. De cette façon, les ID gagne la clé publique du serveur ADFS.

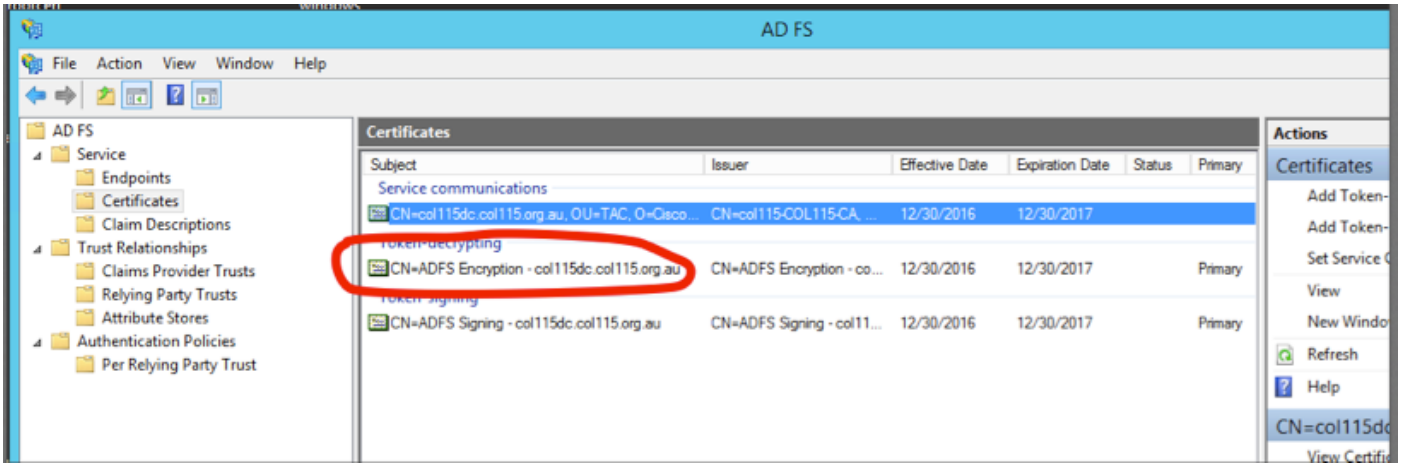
Vous devez **télécharger des** métadonnées d'IDP d'ADFS. Afin de télécharger des métadonnées d'IDP, référez-vous au lien **https:// <FQDN d'ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

D'ADFS les
métadonnées



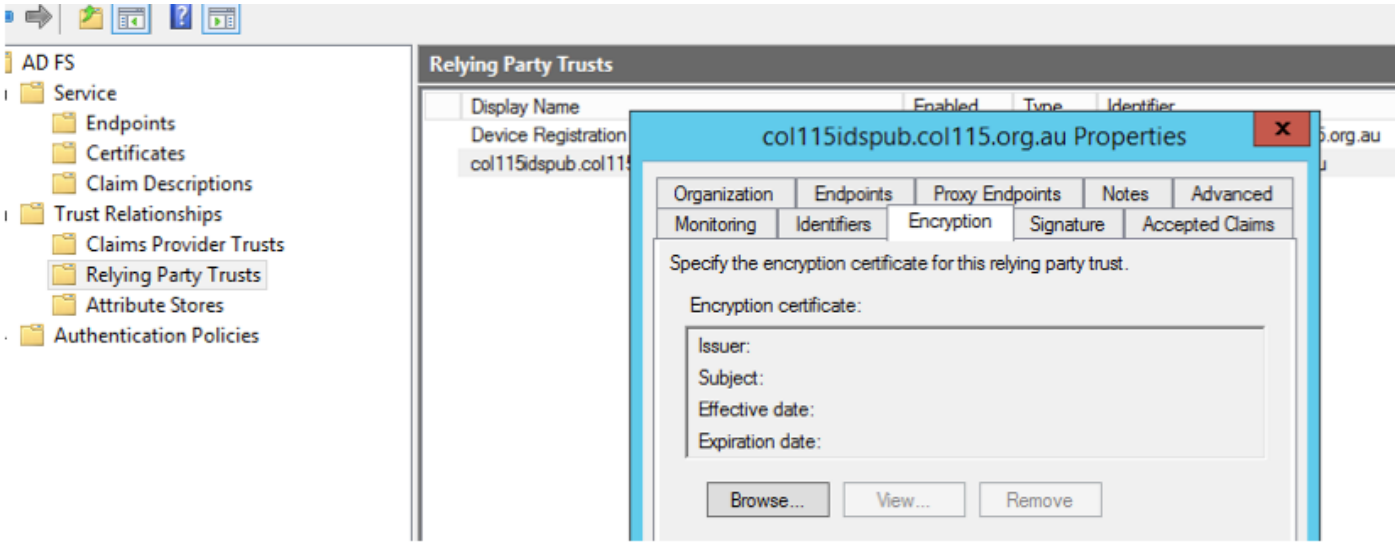
téléchargent des métadonnées ADFS aux ID
Déchiffrement symbolique

Ce certificat se produit automatiquement par le serveur ADFS (auto-signé). Si le jeton a besoin de cryptage, ADFS emploie la clé publique d'ID pour la déchiffrer. Mais, quand vous voyez le jeton-dcrypting ADFS, il ne signifie pas que le jeton est chiffré.



Si vous voulez voir si le cryptage symbolique a été activé pour une application comptante spécifique d'interlocuteur, vous devez vérifier l'onglet de cryptage sur une application comptante spécifique d'interlocuteur.

Cette image affiche, le cryptage symbolique n'a pas été activée.



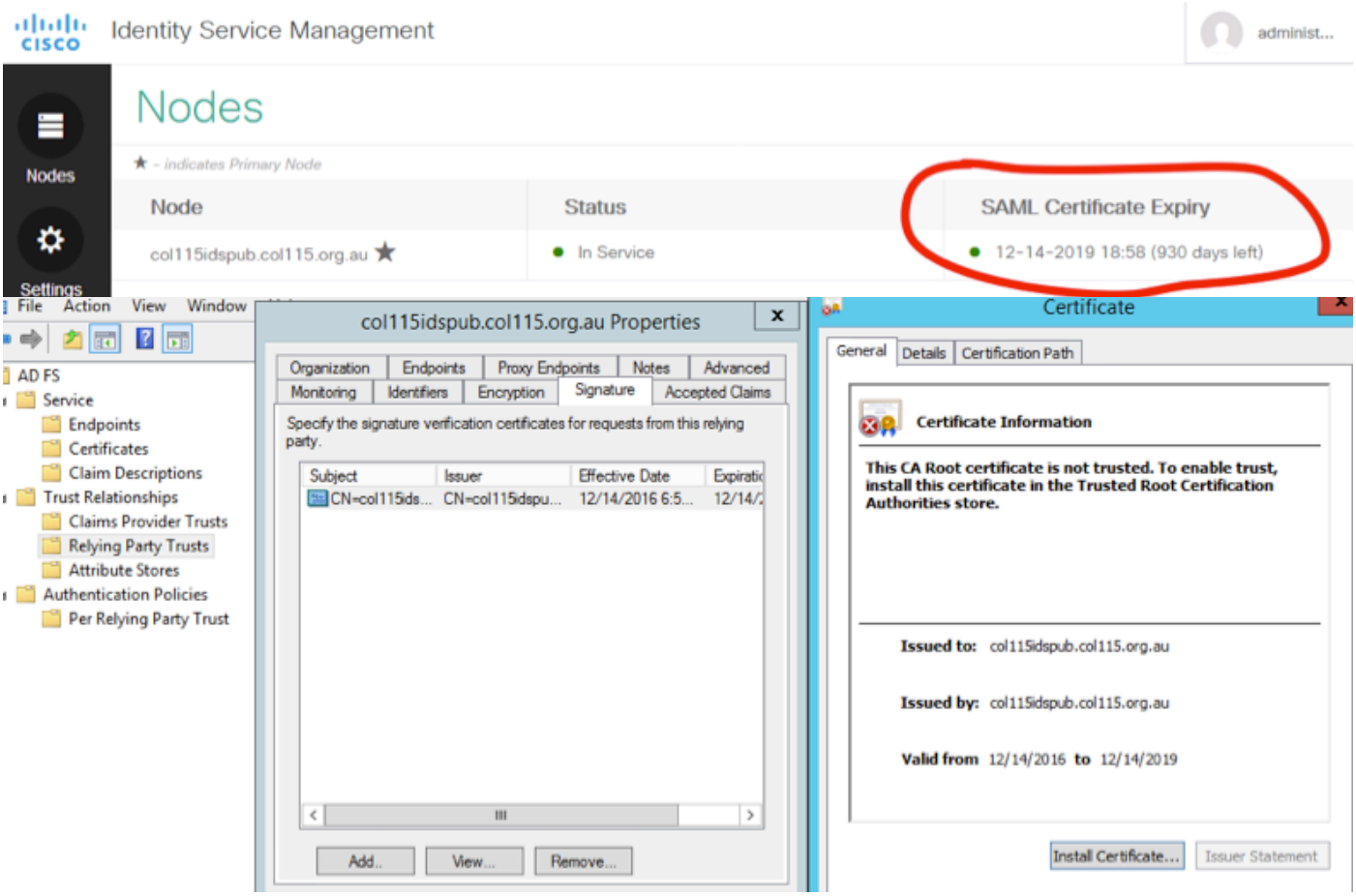
Le cryptage n'est pas activé

Certificat de côté de D. Cisco IDS de partie

- Certificat SAML
- Clé de chiffrement
- Clé de signature

Certificat SAML

Ce certificat est généré par le serveur d'ID (auto-signé). Par défaut il est valable 3 années.

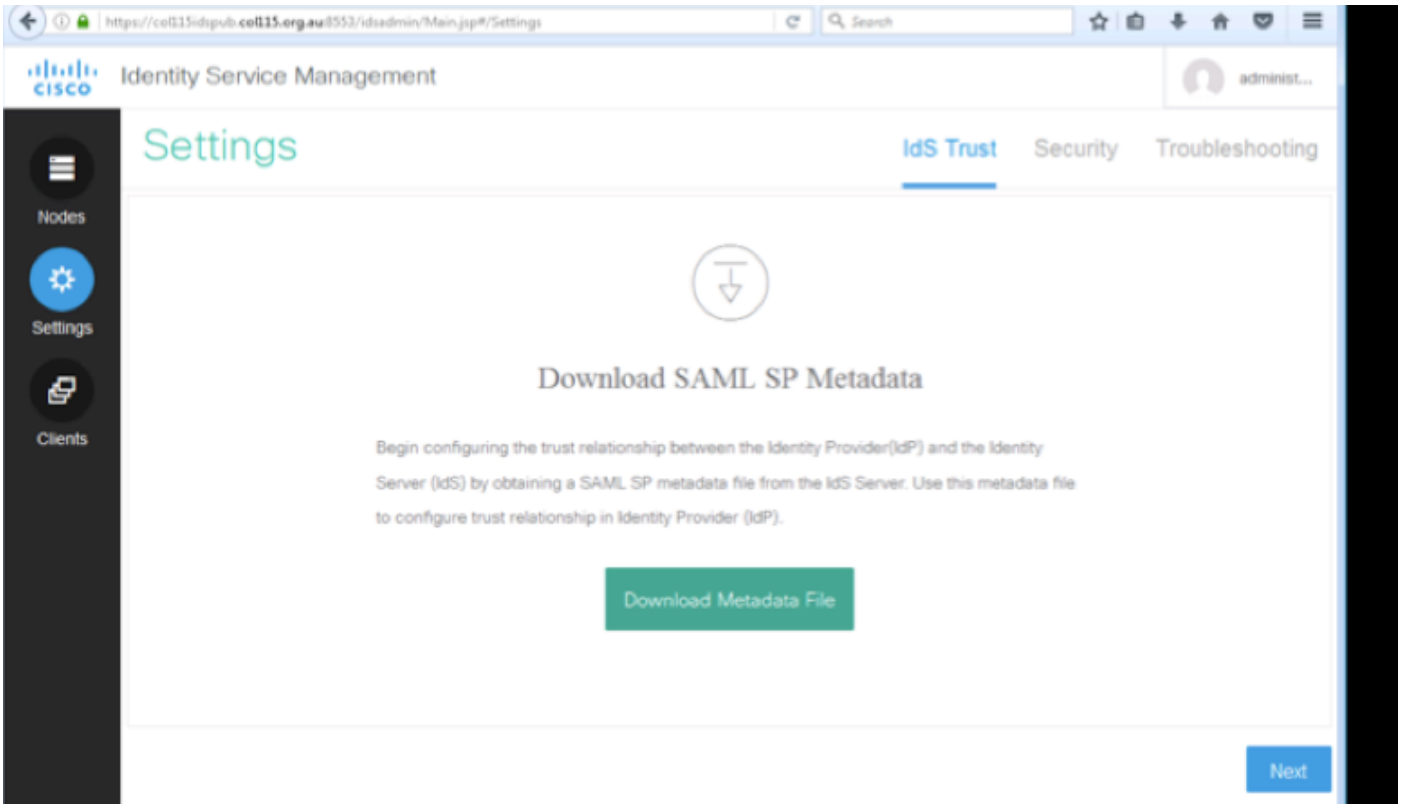


Ce certificat est utilisé pour signer la demande SAML, et envoie à l'IDP (ADFS). Cette clé publique est dans les métadonnées d'ID, et doit être importée au serveur ADFS.

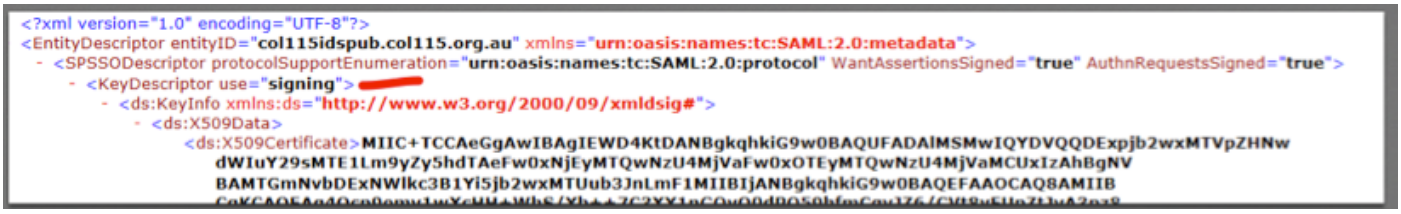
métadonnées de fournisseur de services 1.Download SAML de serveur d'ID.

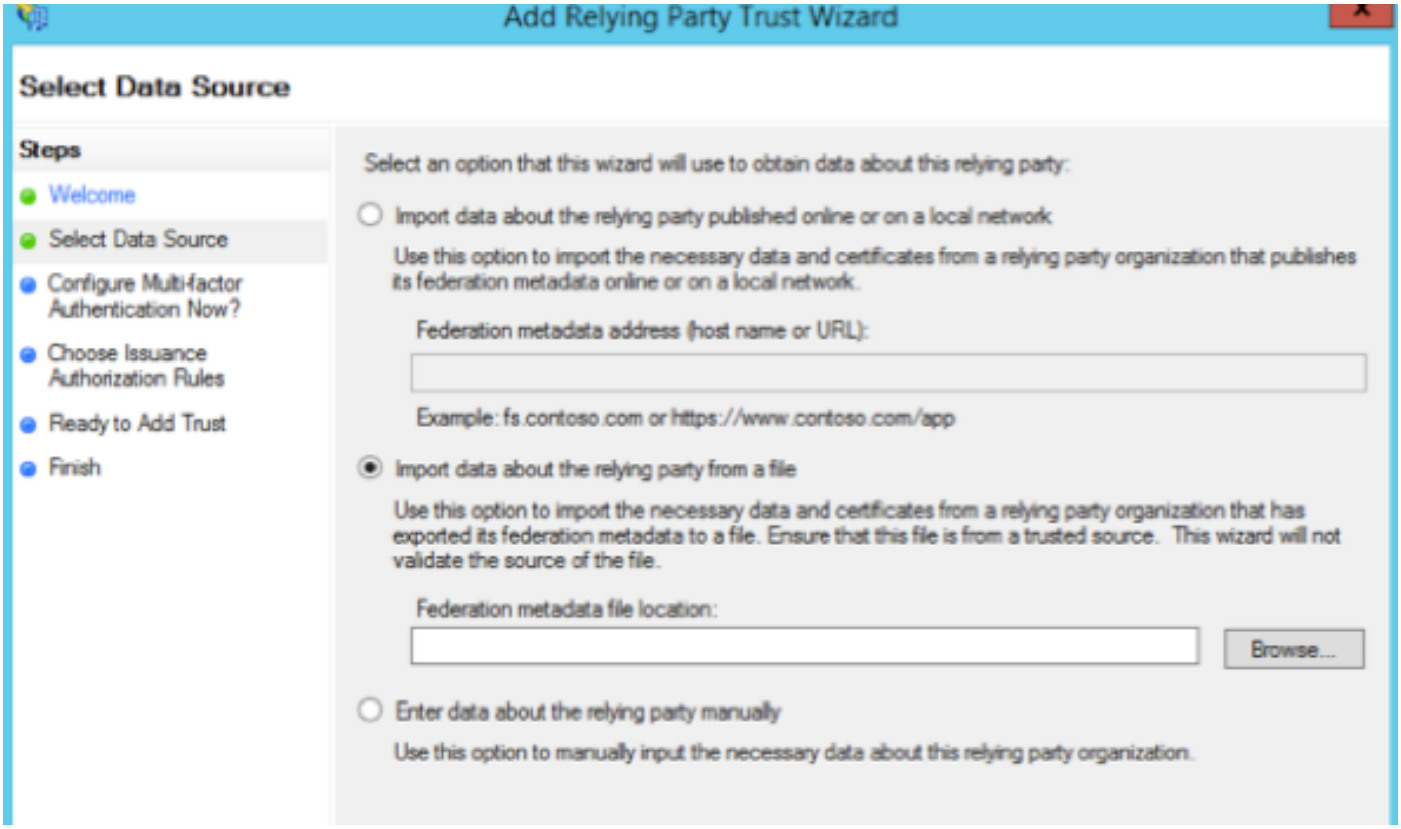
2. Broswer au **serveur FQDN>:8553/idsadmin/ de <ids de https://**.

3. Les configurations et les métadonnées choisies de fournisseur de services du téléchargement SAML et **le sauvegardent**.

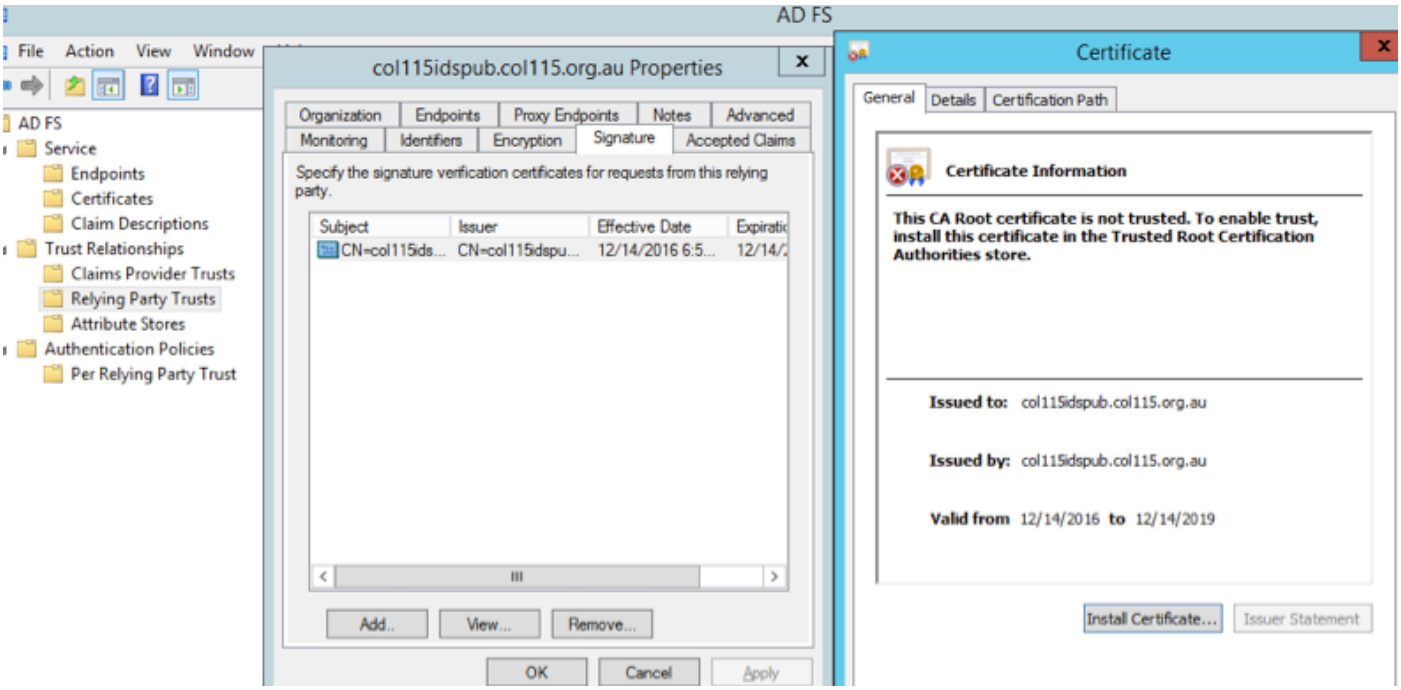


Les métadonnées de l'importation de serveur





d'ID vers le serveur ADFS

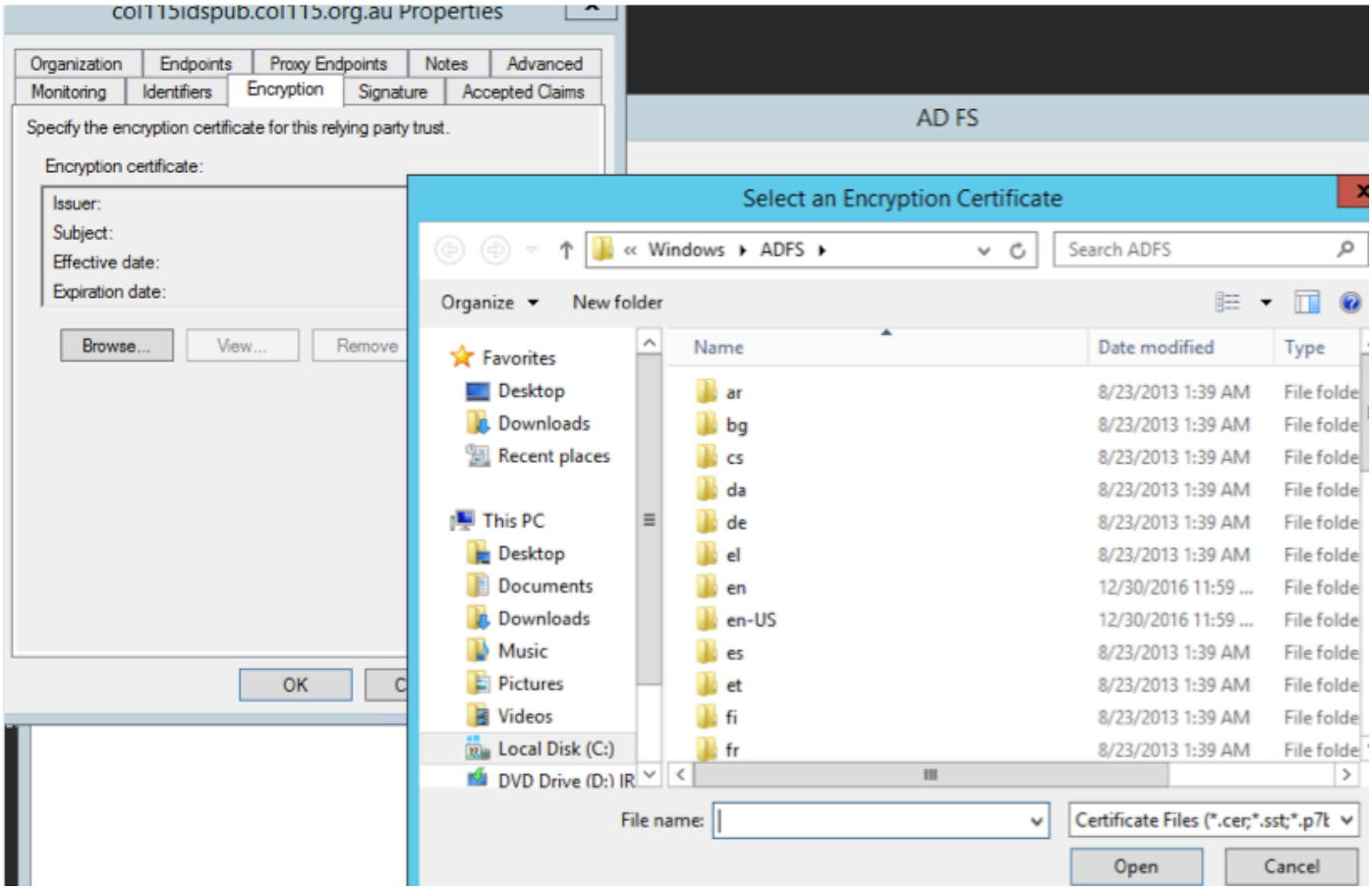


vérifient du côté ADFS

Quand les ID régénère le certificat-le un SAML est utilisé pour signer la demande SAML qu'il exécute l'échange de métadonnées.

Cryptage/clé de signature

Le cryptage n'est pas activé par défaut. Si le cryptage est activé, il doit être téléchargé à ADFS.



Referecne :

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf