Créer et utiliser un certificat tiers sur UCSM

Table des matières

Introduction

Ce document décrit la procédure de création et d'utilisation de certificats tiers sur Unified Computing System (UCS) pour une communication sécurisée.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès à l'autorité CA
- UCSM 3.1

Composants utilisés

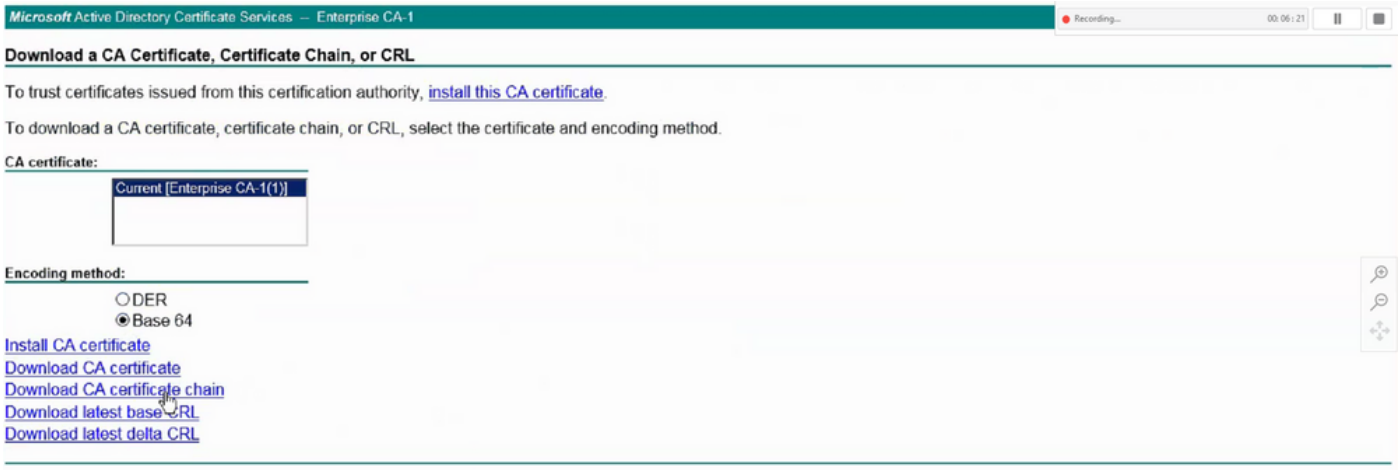
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Étapes de configuration

Configurer le point de confiance

Étape 1

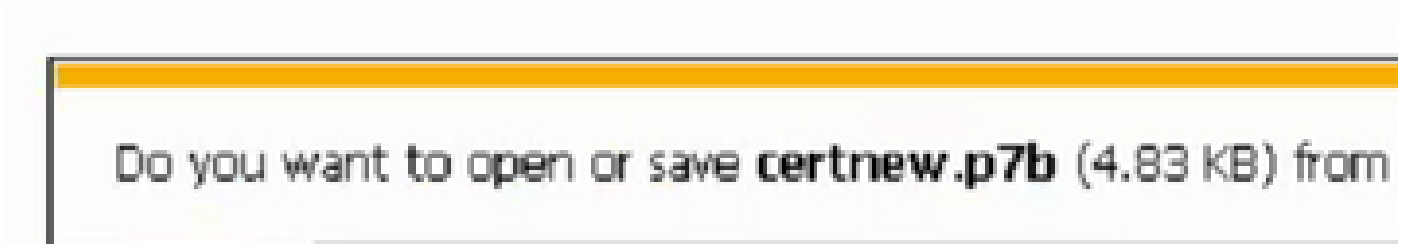
- Téléchargez la chaîne de certificats à partir de l'autorité de certification pour créer Trust-Point. Reportez-vous à http://localhost/certsrv/Default.asp dans le Cert Server.
- Assurez-vous que le codage est défini sur Base 64.



Télécharger la chaîne de certificats de CA Authority

Étape 2

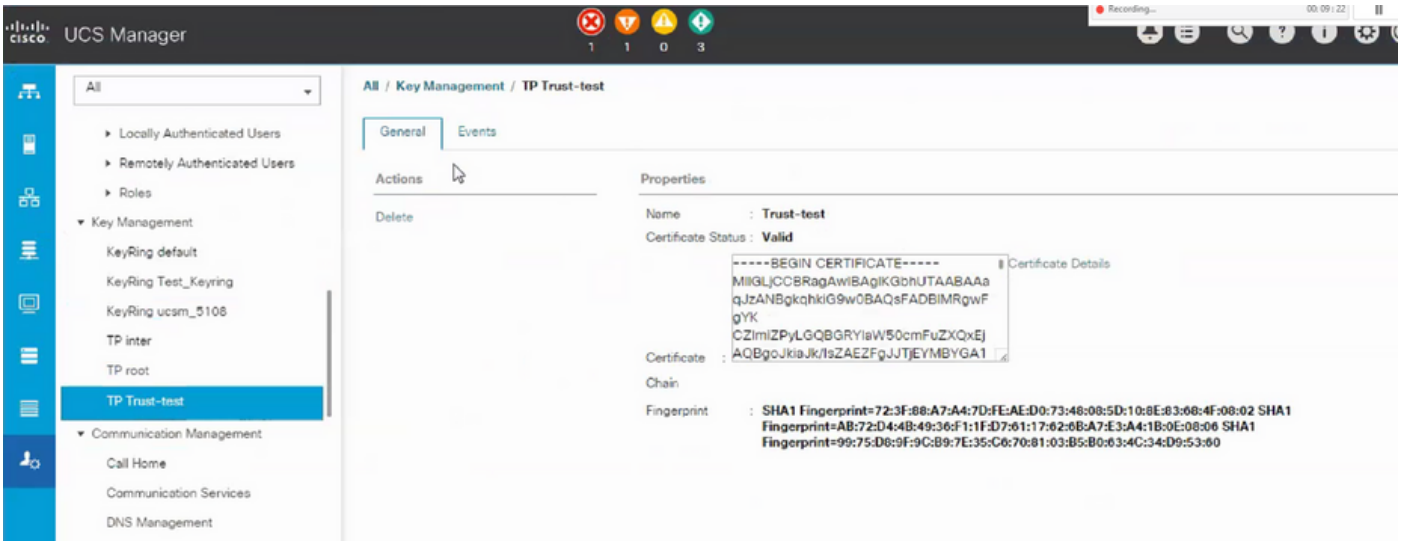
- La chaîne de certificats téléchargée est au format PB7.



- Convertissez le fichier .pb7 au format PEM avec l'outil OpenSSL.
- Par exemple, sous Linux, vous pouvez exécuter cette commande dans terminal pour effectuer la conversion- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

Étape 3

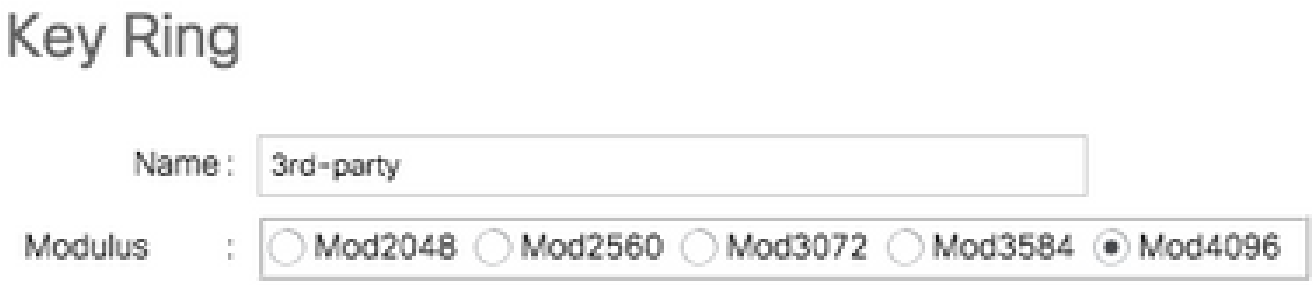
- Créez un point de confiance sur UCSM.
- Accédez à Admin > Key Management > Trustpoint.
- Lorsque vous créez le point de confiance, collez le contenu complet du fichier .PEM créé à l'étape 2 de cette section dans l'espace des détails du certificat.



Créer un porte-clés et une CSR

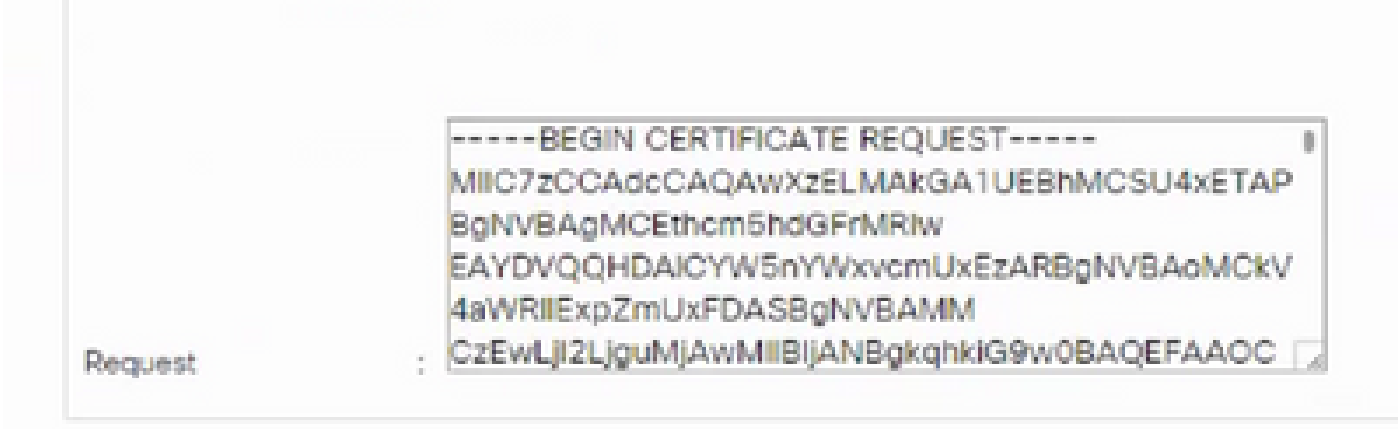
Étape 1

- Accédez à UCSM > Admin > Key Management > Keyring.
- Sélectionnez le module nécessaire pour le certificat tiers.



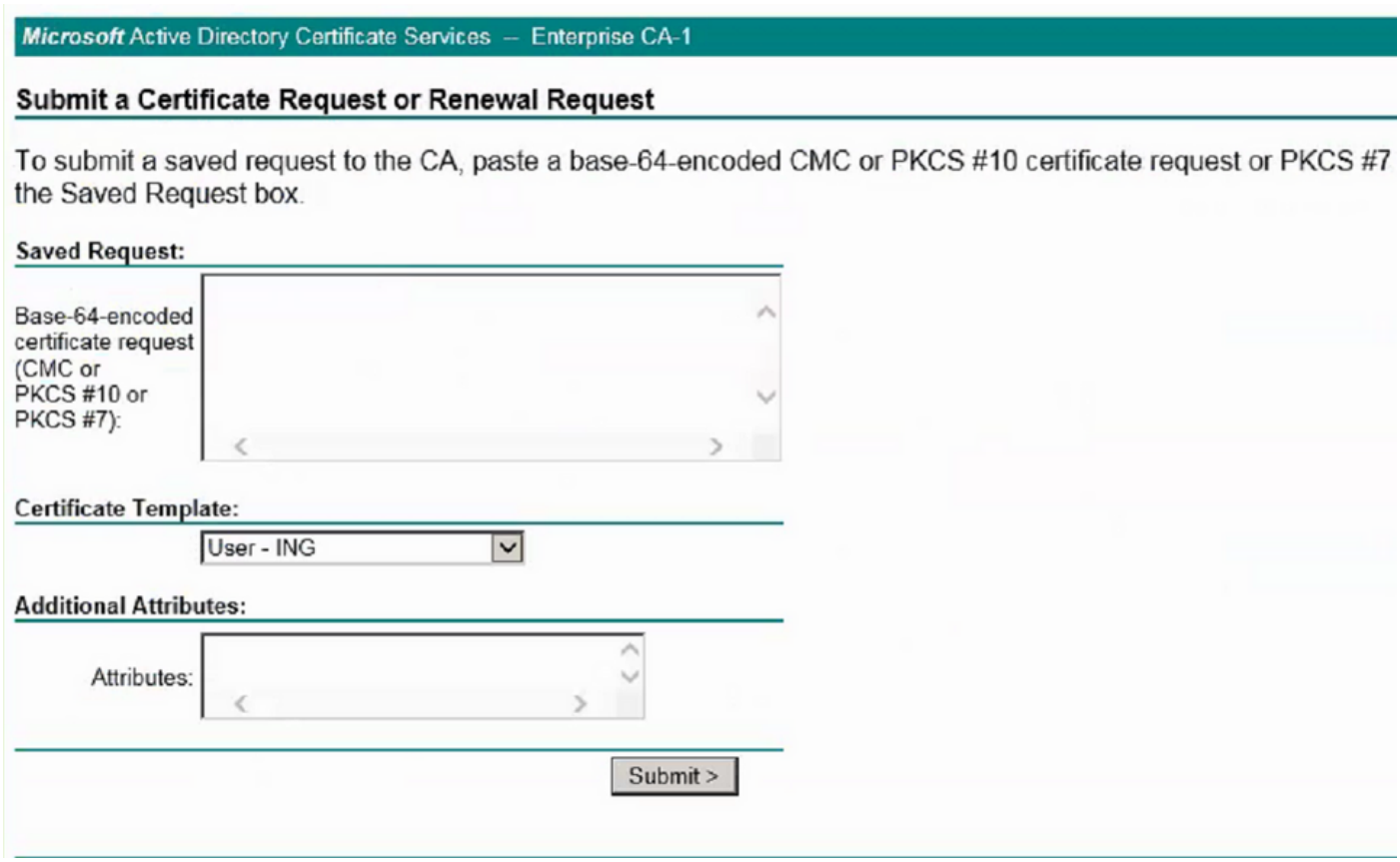
Étape 2

- Cliquez sur créer une demande de certificat et complétez les détails demandés.
- Copiez le contenu du champ de demande.



Étape 3

Pour générer le certificat, collez la demande copiée de l'étape 2 dans l'espace ci-dessous :



Étape 4

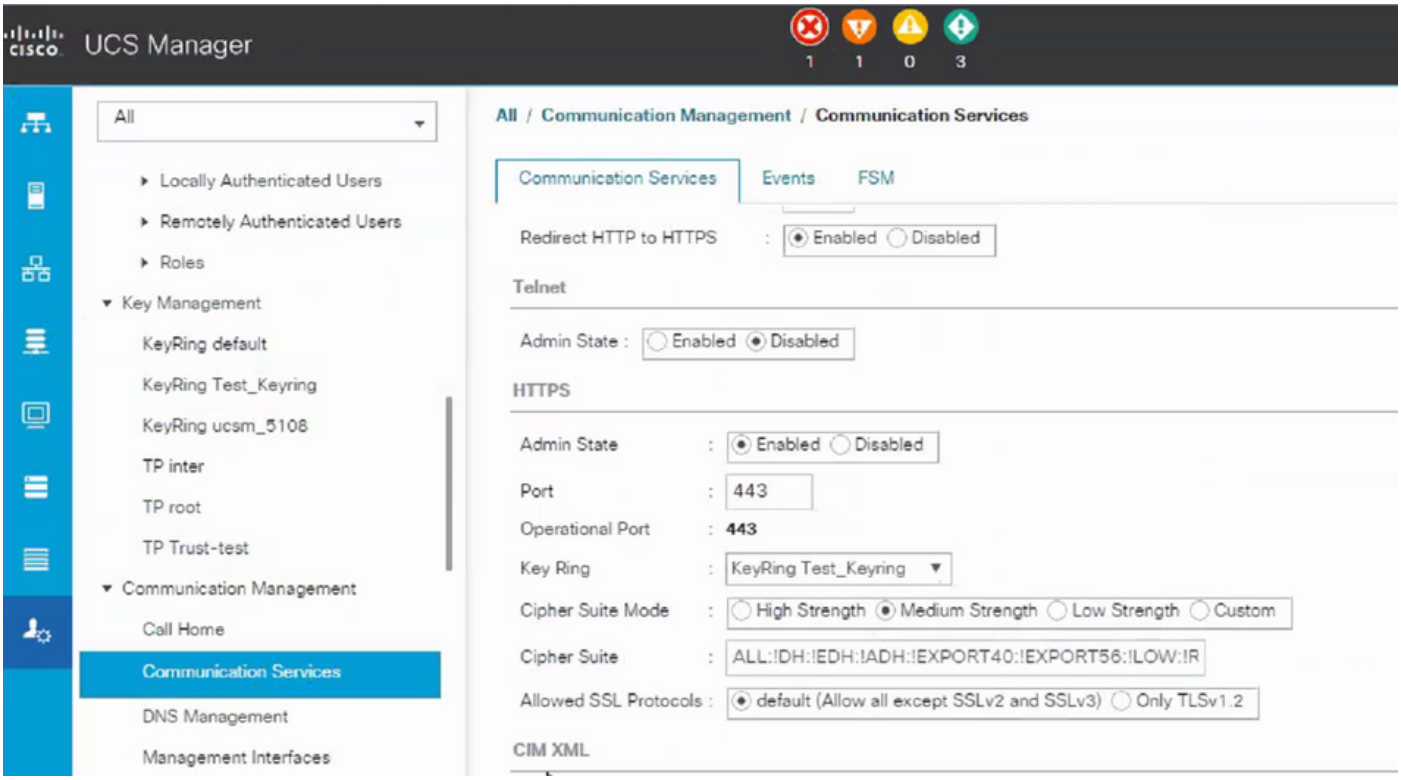
- Une fois soumis, un nouveau certificat est généré. Ouvrez le fichier et copiez tout le contenu du certificat nouvellement généré dans le champ de certificat sur le porte-clés créé à l'étape 1 de cette section.

- Choisissez le point de confiance dans la liste déroulante créée à l'étape 3 de Créer un porte-clés et un CSR.

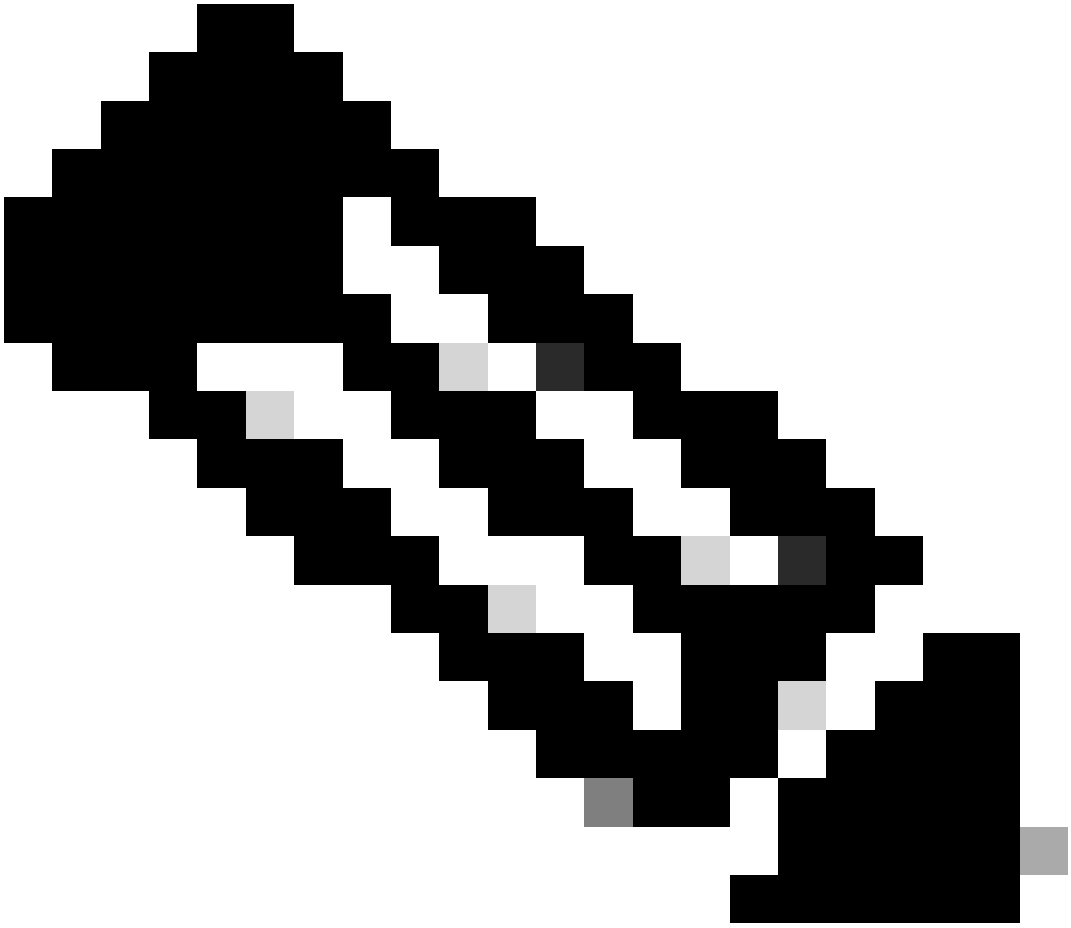
Appliquer le porte-clés

Étape 1

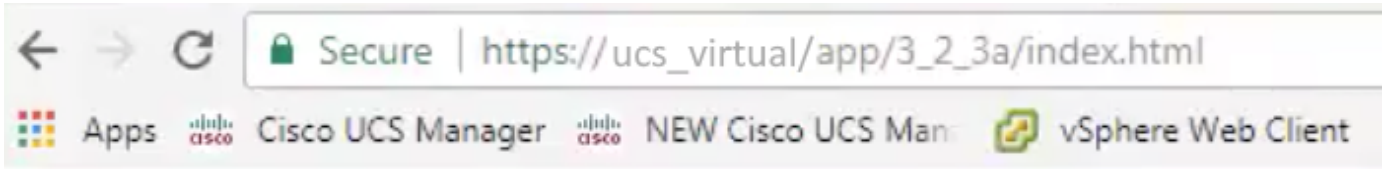
Choisissez le porte-clés créé dans les services de communication comme indiqué ci-dessous :



Après le changement de porte-clés, la connexion HTTPS à l'UCSM apparaît comme sécurisée dans votre navigateur Web.



Remarque : le bureau local doit également utiliser le certificat de la même autorité de certification que l'UCSM.



Informations connexes

- [Assistance et documentation techniques - Cisco Systems]

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.