Importation d'un certificat sur les commutateurs des gammes Sx350 et Sx550X

Objectif

L'objectif de ce document est de fournir les étapes permettant d'importer avec succès un certificat sur les commutateurs des gammes Sx350 et Sx550X à l'aide de l'interface graphique utilisateur (GUI) et de l'interface de ligne de commande (CLI).

Table des matières

- Introduction
- Périphériques et version du logiciel applicables
- Conditions préalables
- Importer via une interface utilisateur graphique
- Erreurs possibles
    - Erreur d'en-tête de clé manquante
    - Erreur de chargement de la clé publique impossible
- Importer avec CLI
- Conclusion

Introduction

L'un des problèmes rencontrés lors de l'importation d'un certificat sur les commutateurs Sx350 et Sx550X est que l'en-tête de clé de l'utilisateur est manquant et/ou n'a pas pu charger les erreurs de clé publique. Ce document explique comment surmonter ces erreurs pour importer un certificat avec succès. Un certificat est un document électronique qui identifie un individu, un serveur, une société ou une autre entité et associe cette entité à une clé publique. Les certificats sont utilisés dans un réseau pour fournir un accès sécurisé. Les certificats peuvent être auto-signés ou signés numériquement par une autorité de certification externe. Un certificat auto-signé, comme son nom l'indique, est signé par son propre créateur. Les autorités de certification gèrent les demandes de certificats et délivrent des certificats aux entités participantes telles que les hôtes, les périphériques réseau ou les utilisateurs. Un certificat numérique signé par une autorité de certification est considéré comme la norme de l'industrie et plus sûr.

Périphériques et version du logiciel applicables

- SG350 version 2.5.0.83

- SG350X version 2.5.0.83
- SG350XG version 2.5.0.83
- SF350 version 2.5.0.83
- SG550X version 2.5.0.83
- SF550X version 2.5.0.83
- SG550XG version 2.5.0.83
- SX550X version 2.5.0.83

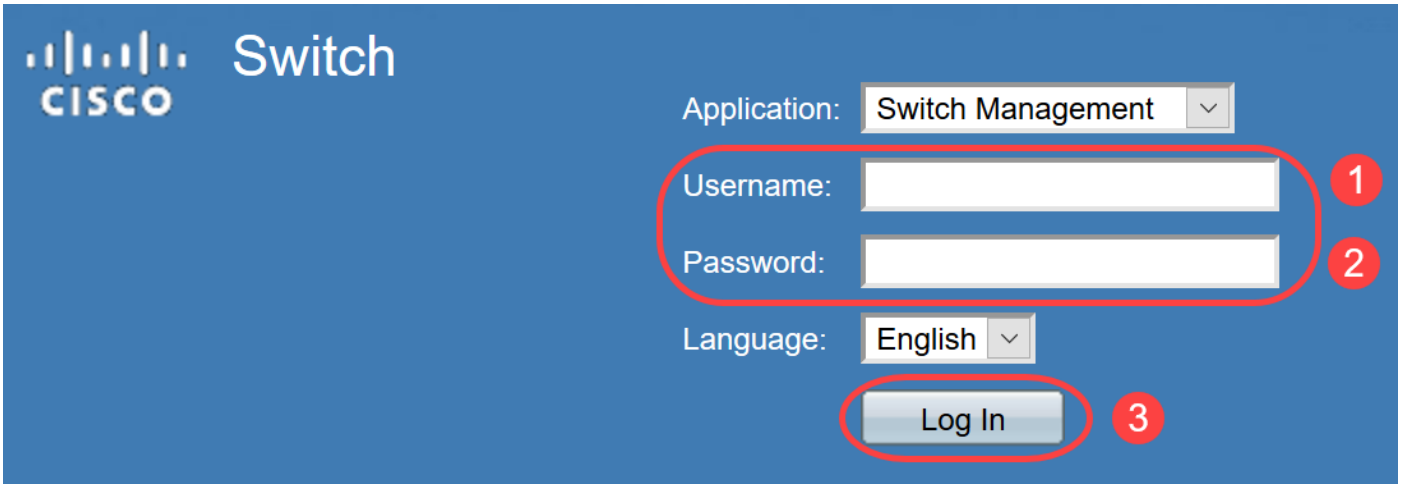
Conditions préalables

Vous devez disposer d'un certificat auto-signé ou d'une autorité de certification (CA). Les étapes d'obtention d'un certificat auto-signé sont incluses dans cet article. Pour en savoir plus sur les certificats CA, cliquez ici.

Importer via une interface utilisateur graphique

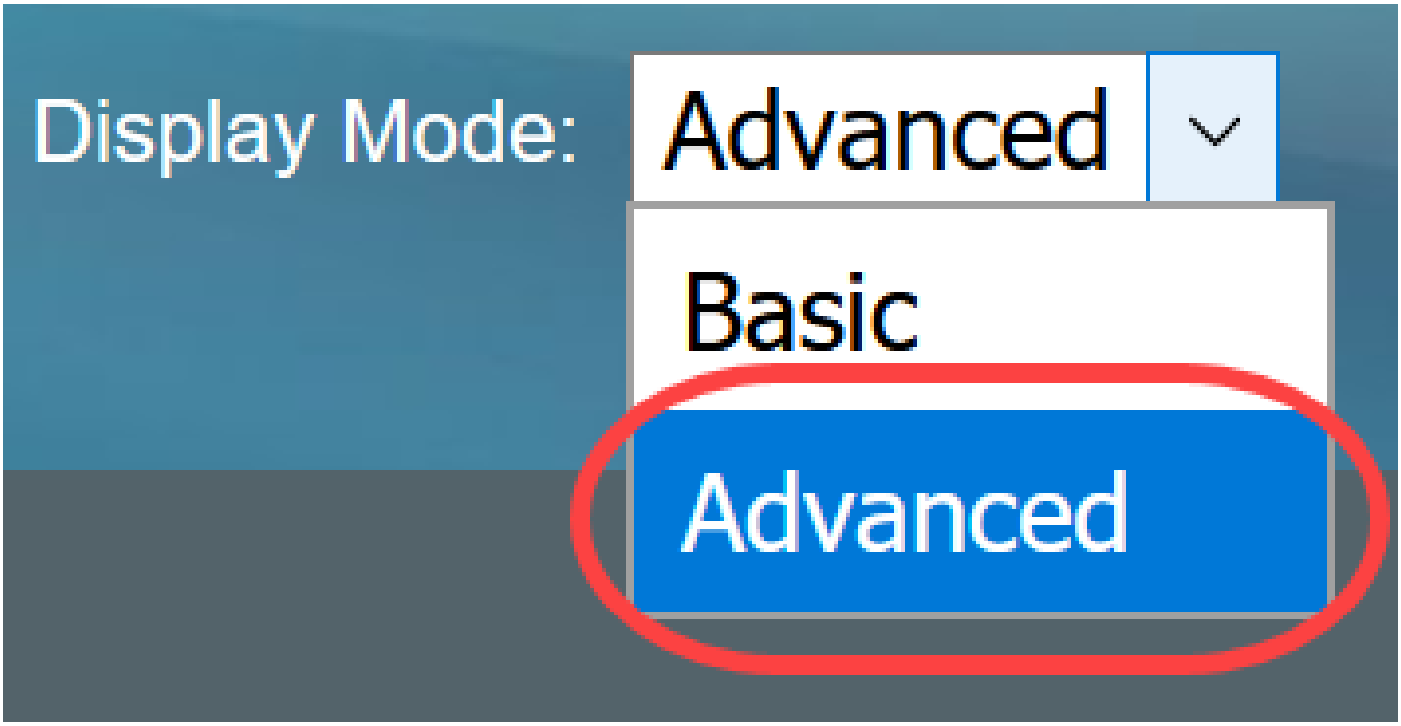
Étape 1

Connectez-vous à l'interface utilisateur graphique du commutateur en entrant votre nom d'utilisateur et votre mot de passe. Cliquez sur Log In.



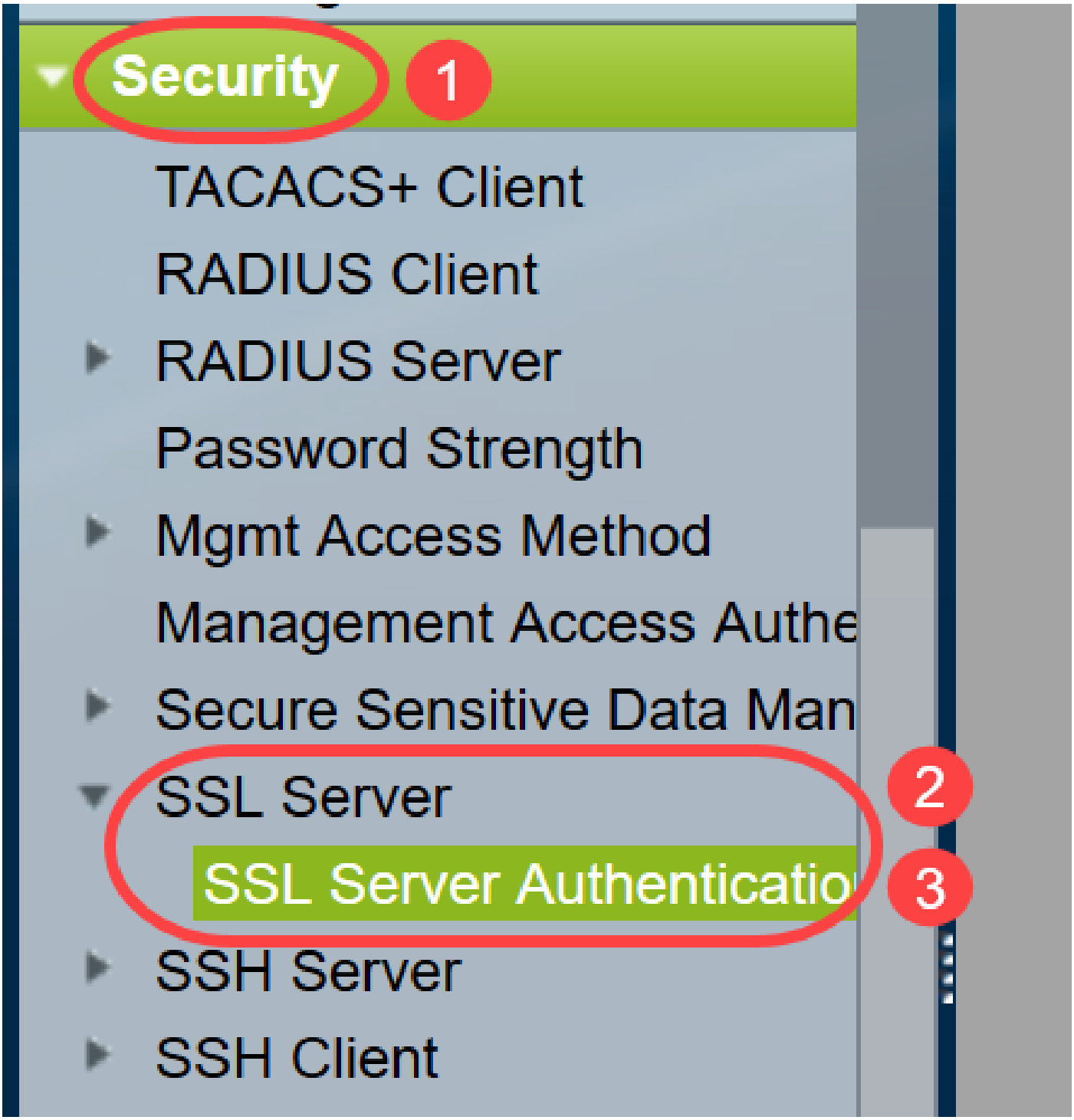
Étape 2

Dans le Mode d'affichage en haut à droite de l'interface graphique utilisateur, sélectionnez Avancé à l'aide de l'option déroulante.



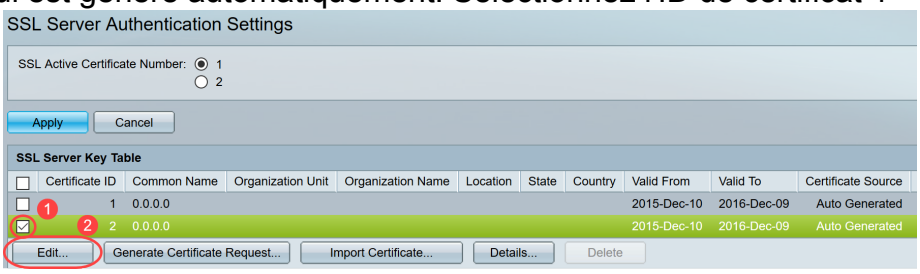
Étape 3

Accédez à Security > SSL Server > SSL Server Authentication.



Étape 4

Sélectionnez l'un des certificats qui est généré automatiquement. Sélectionnez l'ID de certificat 1 ou 2 et cliquez sur le bouton Edit.

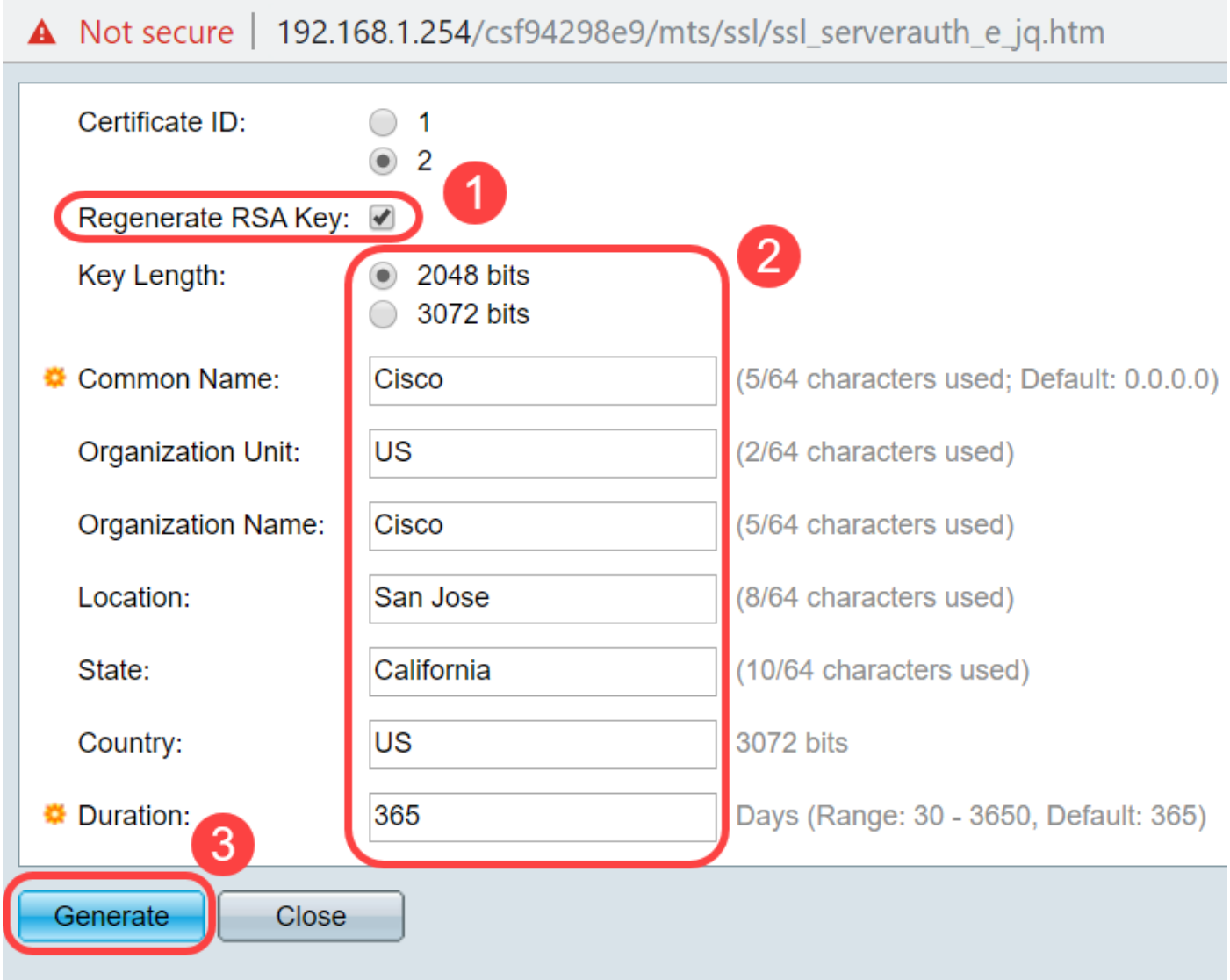


Étape 5

Pour générer un certificat auto-signé, dans la nouvelle fenêtre contextuelle, activez Regenerate RSA Key et entrez les paramètres suivants :

- Longueur de clé
- Nom commun
- Unité D'Organisation
- Nom de l'entreprise
- Emplacement
- Province
- Pays
- Durée

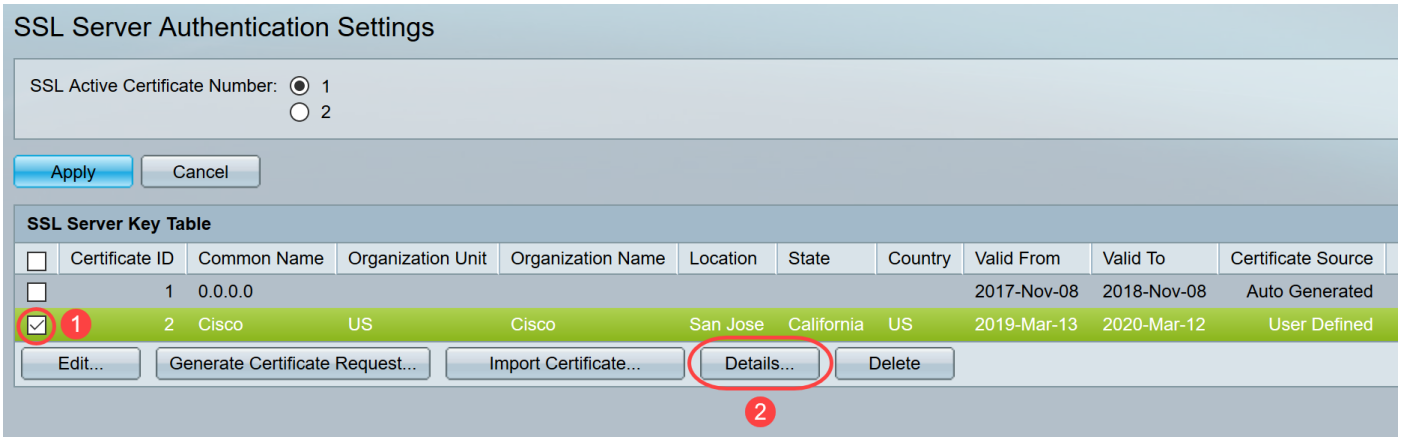
Cliquez sur Générer.



Vous pouvez également créer un certificat à partir d'une autorité de certification tierce.

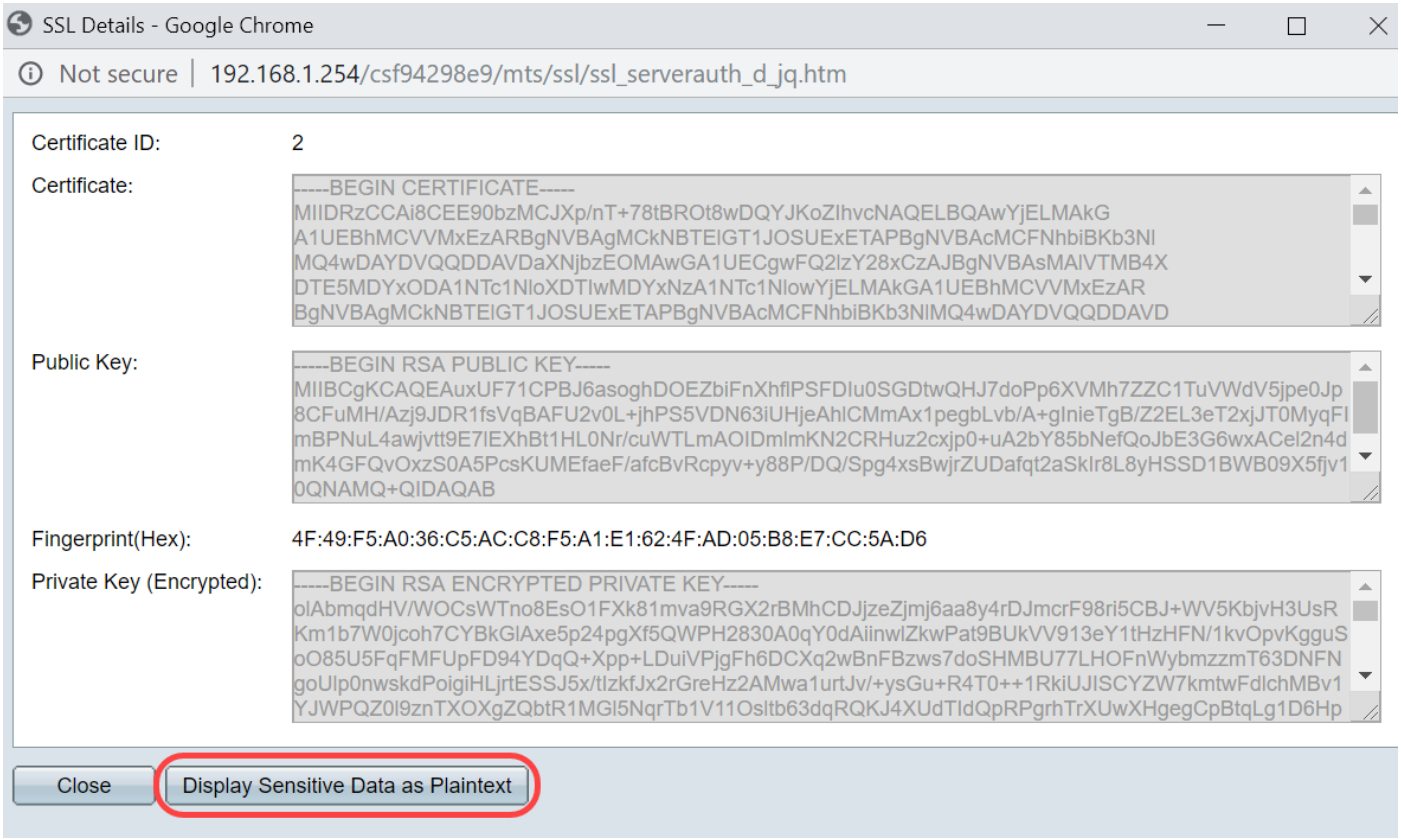
Étape 6

Vous pouvez maintenant voir le certificat défini par l'utilisateur sous la table de clés de serveur SSL. Sélectionnez le certificat nouvellement créé et cliquez sur Détails.



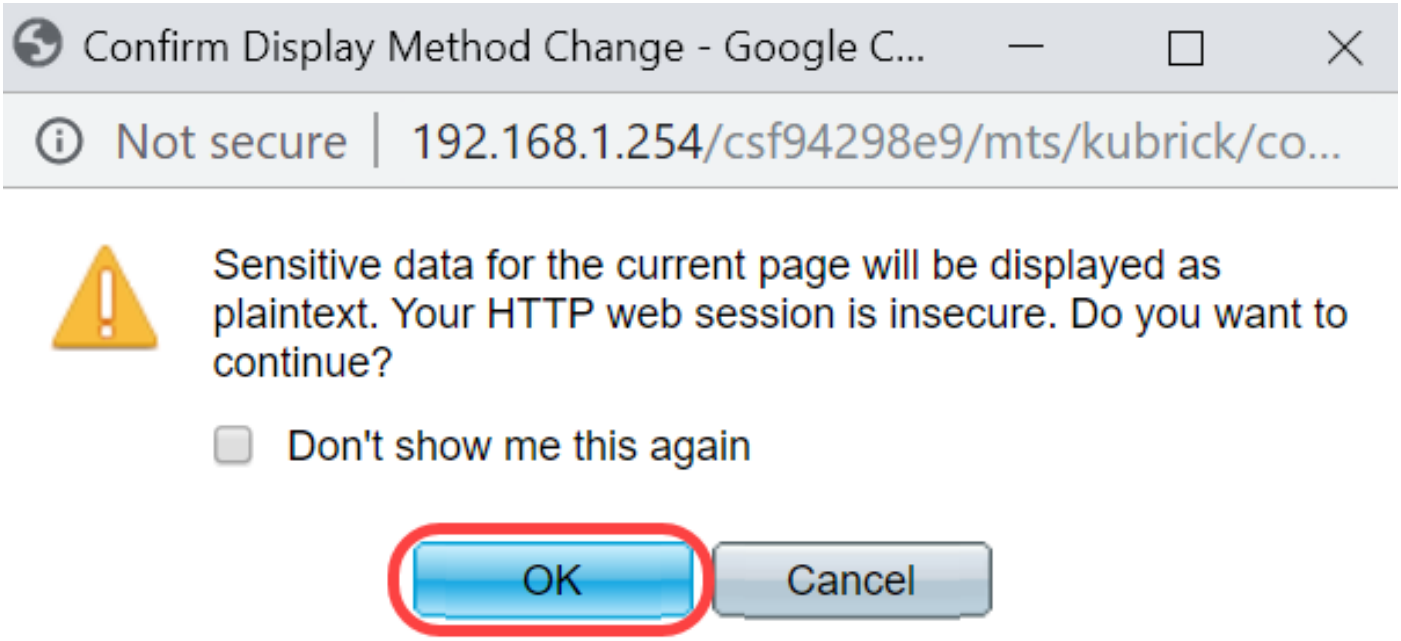
Étape 7

Dans la fenêtre contextuelle, vous pourrez voir les détails du certificat, de la clé publique et de la clé privée (cryptée). Vous pouvez les copier sur un autre fichier du bloc-notes. Cliquez sur Afficher les données sensibles en texte clair.



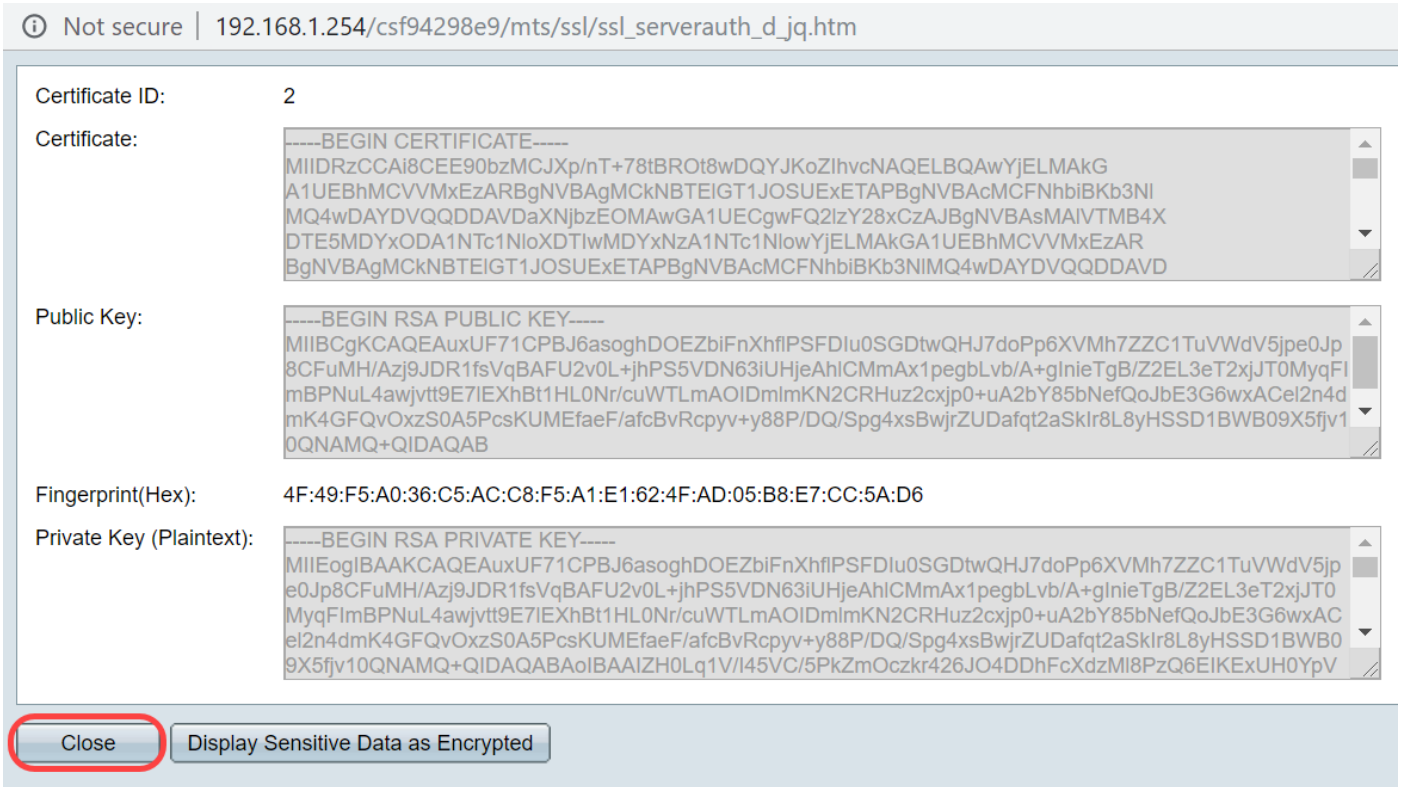
Étape 8

Une fenêtre contextuelle s'ouvre pour confirmer l'affichage de la clé privée en texte clair, cliquez sur OK.



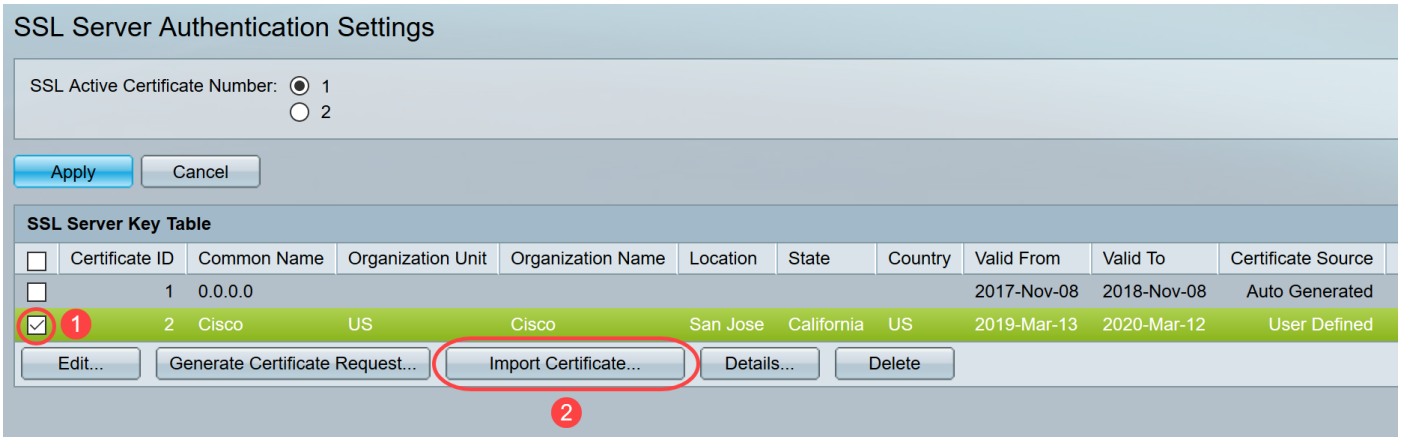
Étape 9

Vous pouvez maintenant voir la clé privée sous la forme de texte clair. Copiez cette sortie en texte clair dans un fichier de bloc-notes. Cliquez sur Fermer.



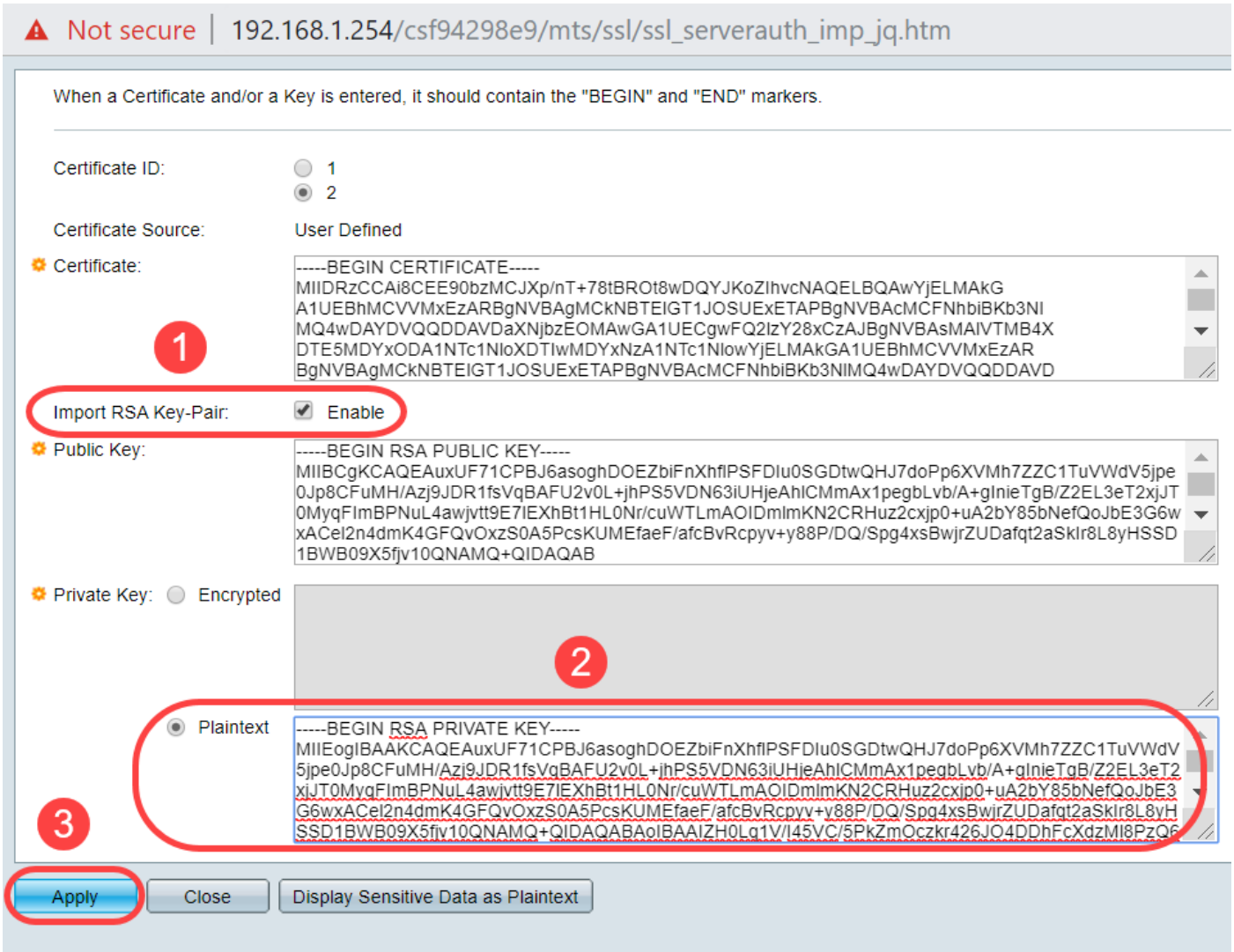
Étape 10

Sélectionnez le nouveau certificat défini par l'utilisateur créé et cliquez sur Importer un certificat.



Étape 11

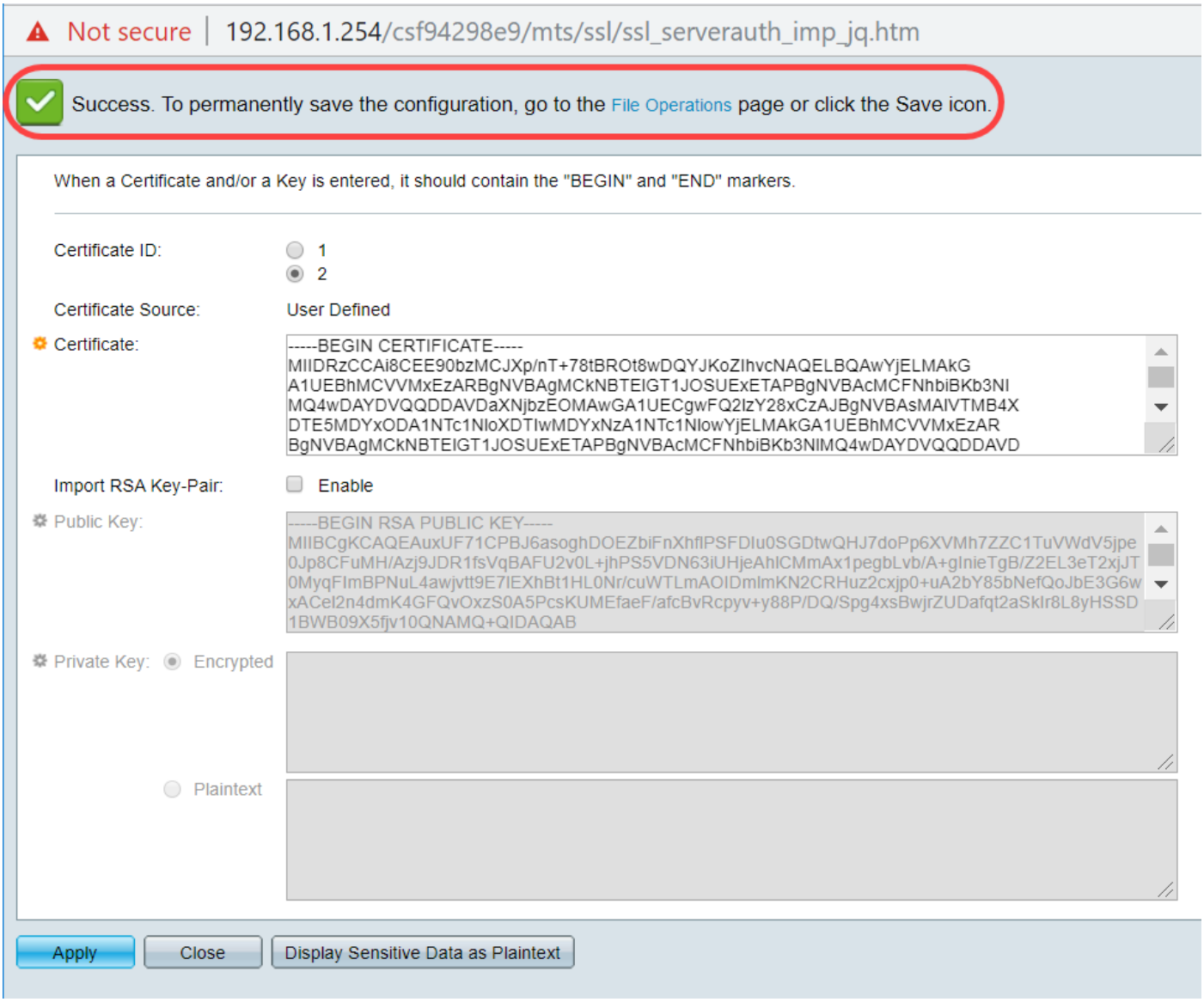
Dans la nouvelle fenêtre contextuelle, activez l'option Import RSA Key-Pair et collez la clé privée (copiée à l'étape 9) au format texte clair. Cliquez sur Apply.



Dans cet exemple, le mot clé RSA est inclus au BEGIN et à la FIN de la clé publique.

Étape 12

La notification de réussite s'affiche à l'écran. Vous pouvez fermer cette fenêtre et enregistrer la configuration sur le commutateur.



Erreurs possibles

Les erreurs abordées concernent la clé publique. Normalement, deux types de formats de clé publique sont utilisés :

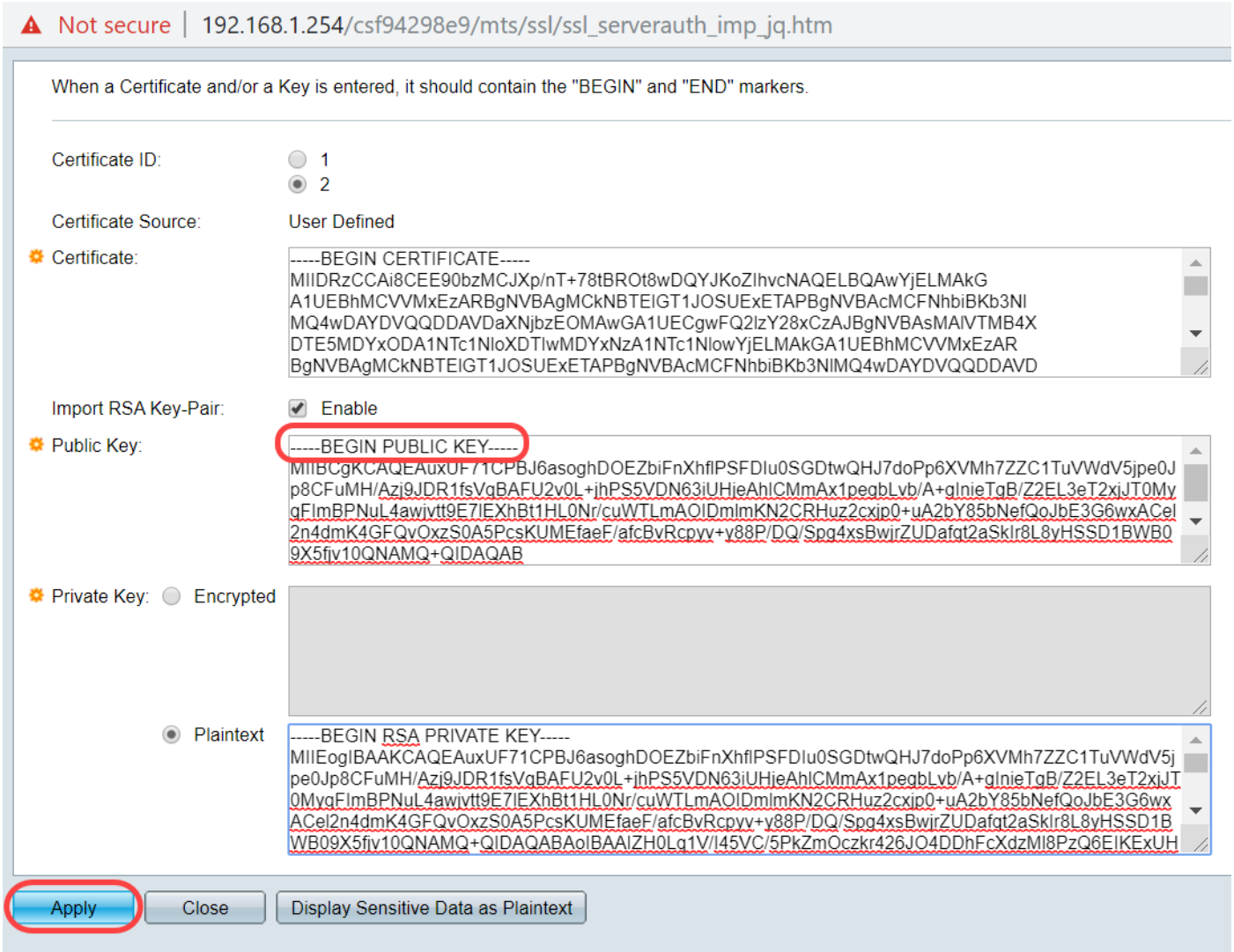
1. Fichier de clé publique RSA (PKCS#1) : Ceci est spécifique pour les clés RSA.

Elle commence et se termine par les balises suivantes :
-----DÉBUT DE LA CLÉ PUBLIQUE RSA-----
DONNÉES CODÉES EN BASE64
-----END CLÉ PUBLIQUE RSA-----

2. Fichier de clé publique (PKCS#8) : Il s'agit d'un format de clé plus générique qui identifie le type de clé publique et contient les données pertinentes.
Elle commence et se termine par les balises suivantes :
-----DÉBUT DE LA CLÉ PUBLIQUE-----
DONNÉES CODÉES EN BASE64
-----CLÉ PUBLIQUE DE FIN-----

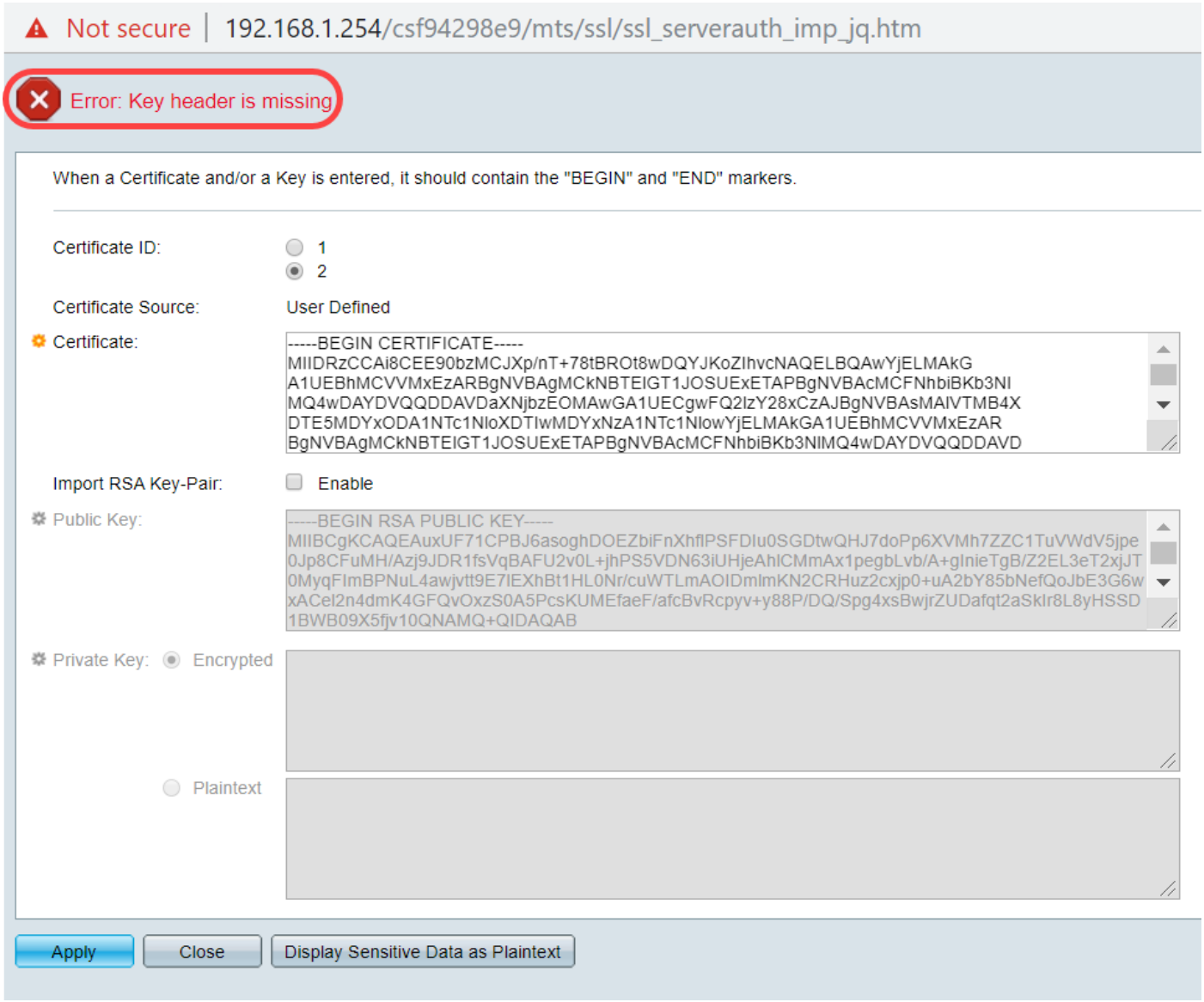
Erreur d'en-tête de clé manquante

Scénario 1 : Vous avez généré le certificat à partir d'une autorité de certification tierce. Vous avez copié et collé la clé publique et cliqué sur Apply.



Vous avez reçu le message Erreur : En-tête de clé manquant. Fermez la fenêtre. Quelques

modifications peuvent être apportées pour faire disparaître ce problème.



Pour corriger cette erreur :

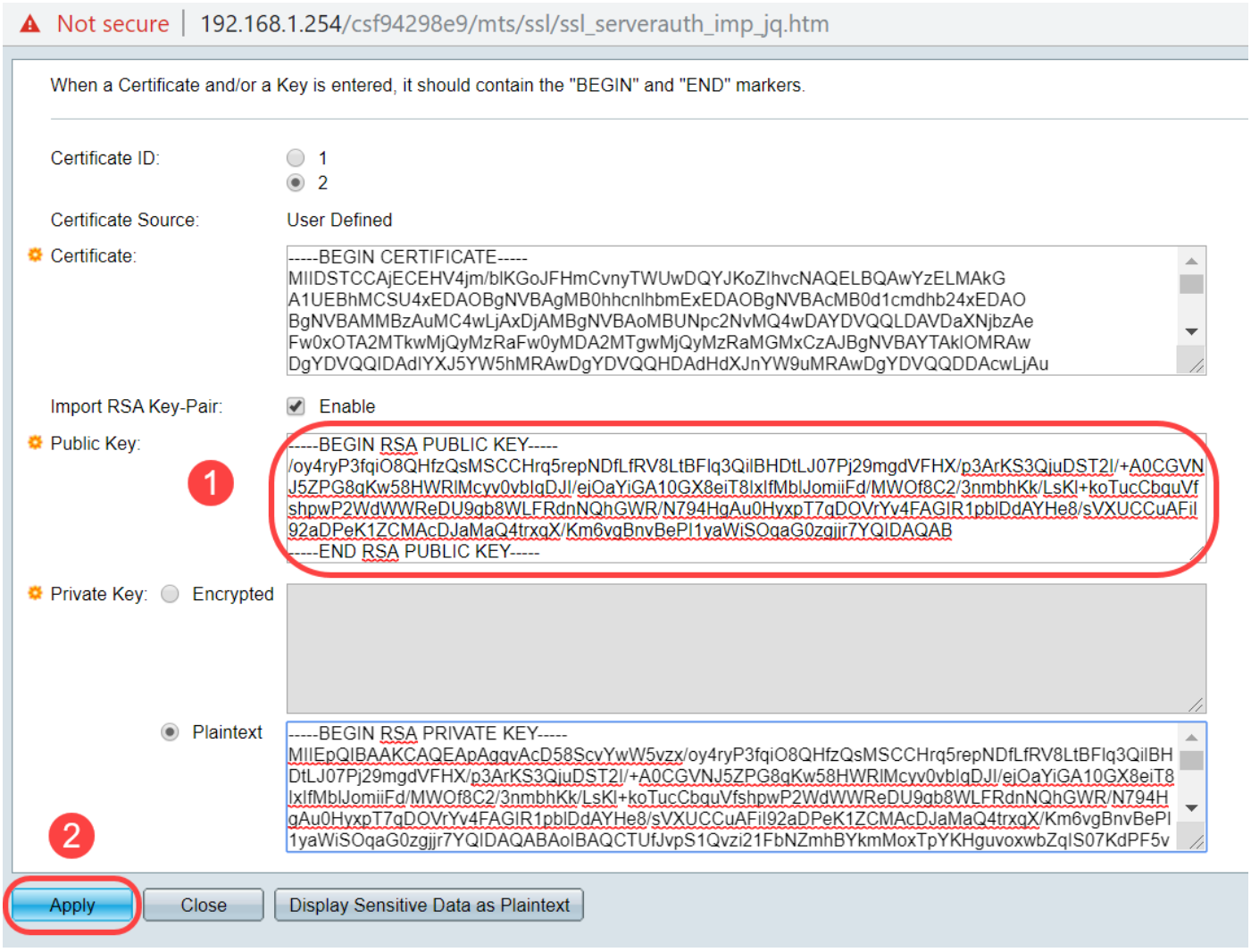
- Ajoutez le mot clé RSA au début de la clé publique : BEGIN RSA PUBLIC KEY
- Ajoutez le mot clé RSA à la fin de la clé publique : END RSA PUBLIC KEY
- Supprimez les 32 premiers caractères du code clé. La partie mise en surbrillance ci-dessous est un exemple des 32 premiers caractères.



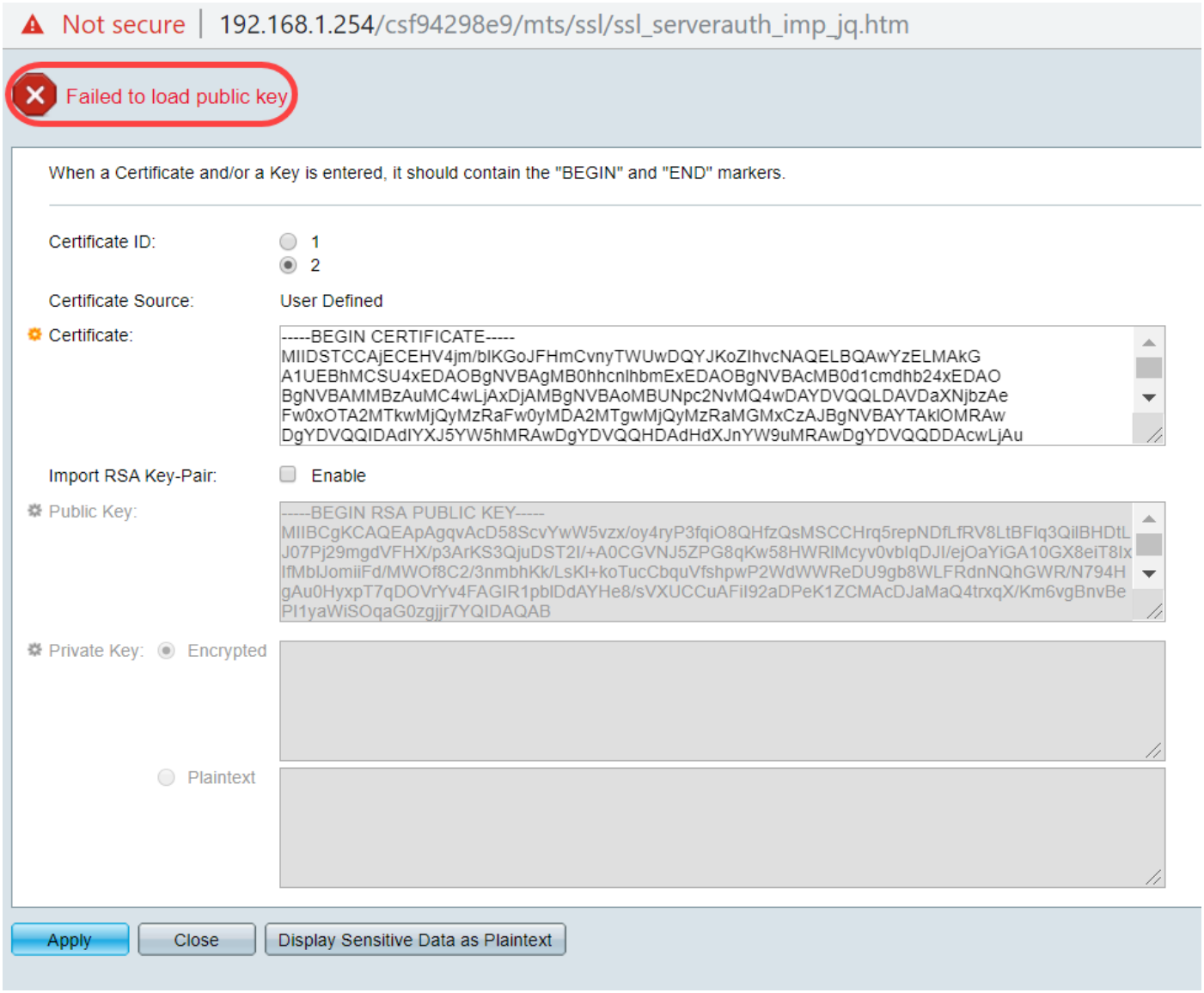
Lorsque vous appliquez les paramètres, vous n'obtiendrez pas l'erreur Key header is missing dans la plupart des cas.

Erreur de chargement de la clé publique impossible

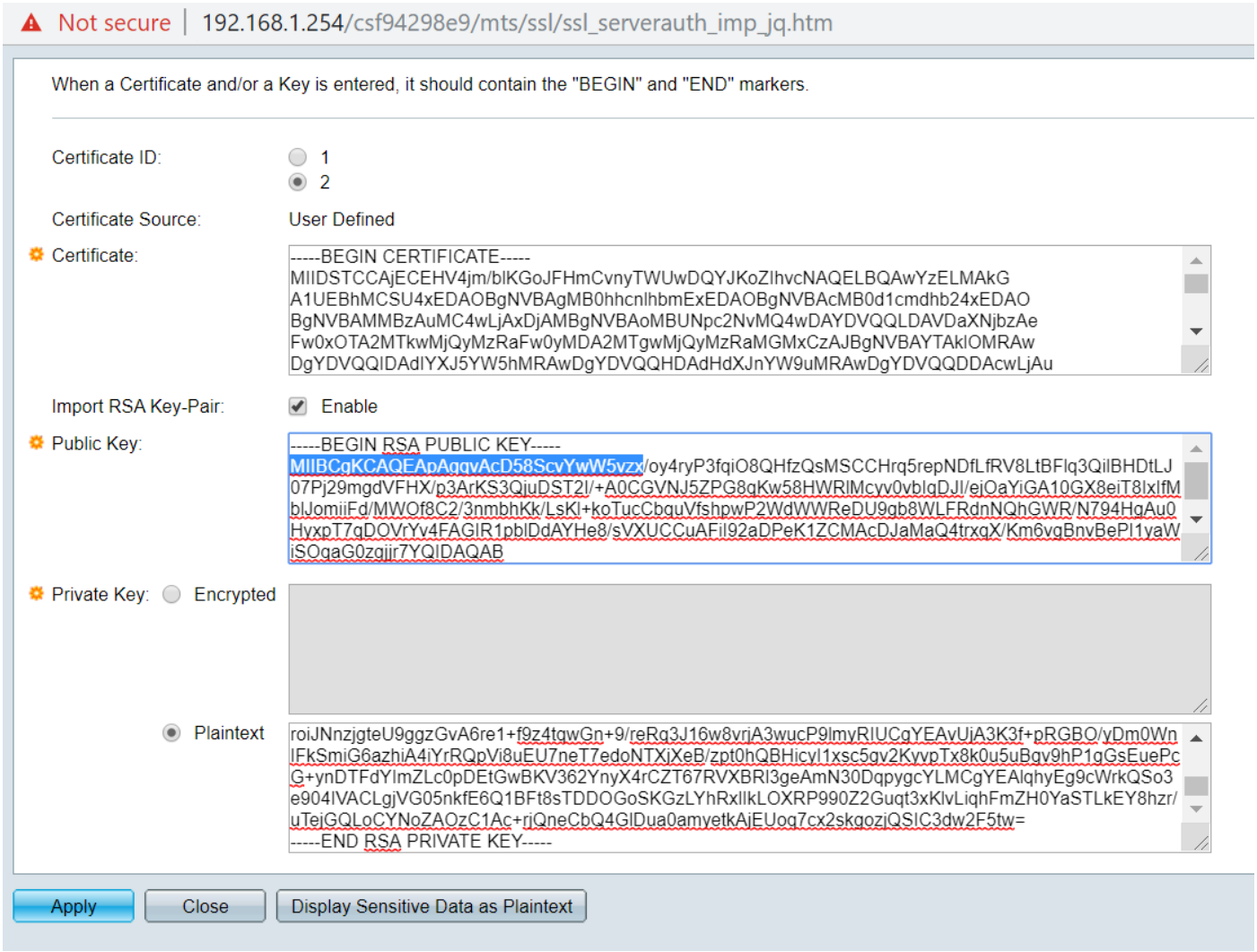
Scénario 2 : Vous avez généré un certificat sur un commutateur et l'avez importé sur un autre commutateur. Vous avez copié et collé la clé publique après avoir supprimé les 32 premiers caractères et cliqué sur Apply.



L'erreur Failed to load public key s'affiche à l'écran.



Pour corriger cette erreur, NE SUPPRIMEZ PAS les 32 premiers caractères de la clé publique dans ce cas.



Importer avec CLI

Étape 1

Pour importer un certificat à l'aide de la CLI, entrez la commande suivante.

```
switch(config)#crypto certificate [numéro de certificat] import
```

Le certificat 2 est importé dans cet exemple.

```
switch(config)#crypto certificate 2 import
```

Étape 2

Collez l'entrée ; ajoutez un point (.) sur une ligne distincte après l'entrée.

```
-----DÉMARRER LA CLÉ PRIVÉE RSA-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgAoIBAQC/rZQ6f0rj8neA
...24 lignes tronquées....
```

```
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
-----TERMINER LA CLÉ PRIVÉE RSA-----
-----DÉBUT DE LA CLÉ PUBLIQUE RSA-----
MIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfTOl
...3 lignes tronquées....
64jc5fzIfNnE2QpgBX/9M4OE41BX5ZOB/QIDAQAB
-----END CLÉ PUBLIQUE RSA-----
-----COMMENCER LE CERTIFICAT-----
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
: 28 lignes tronquées...
8S+39m9wPAOZipIOJA1/OIeG7ChLWOXKncMeZWVTIUZewVFOcUzqXwOJcsTrMV
JDPtnbKXG56wOTrecu6UQ9HsUBoDQnlsN5ZBHt1VyjAP
-----TERMINER LE CERTIFICAT-----
.
Certificat importé avec succès
Émis par : C=xx, ST=Gxxxxx, L=xx, O=xx CA limitée, CN=xx Validation de l'organisation RSA Secure
Server CA
Valide à partir de : 14 juin 00:00:00 2017 GMT
Valide jusqu'à : Sep 11 23:59:59 2020 GMT
Objet : C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx, OU=IT, CN=*.kowi.eu
Empreinte numérique SHA : xxxxxx
```

Conclusion

Vous avez maintenant appris les étapes à suivre pour importer avec succès un certificat sur les commutateurs des gammes Sx350 et Sx550X à l'aide de l'interface graphique et de l'interface de ligne de commande.

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.