Comment importer un certificat sur les commutateurs des gammes Sx350 et Sx550X

Objectif

Cet objectif de ce document est de fournir les étapes permettant d'importer 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 logicielle applicables
- Conditions préalables
- Importer à l'aide de l'interface utilisateur graphique
- Erreurs possibles Erreur d'en-tête de clé manquanteÉchec du chargement de l'erreur de clé publique
- Importer à l'aide de 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 dépasser ces erreurs pour importer un certificat avec succès. Un certificat est un document électronique qui identifie une personne, 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 autosignés 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 certificat 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 une norme de l'industrie et plus sécurisé.

Périphériques et version logicielle 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

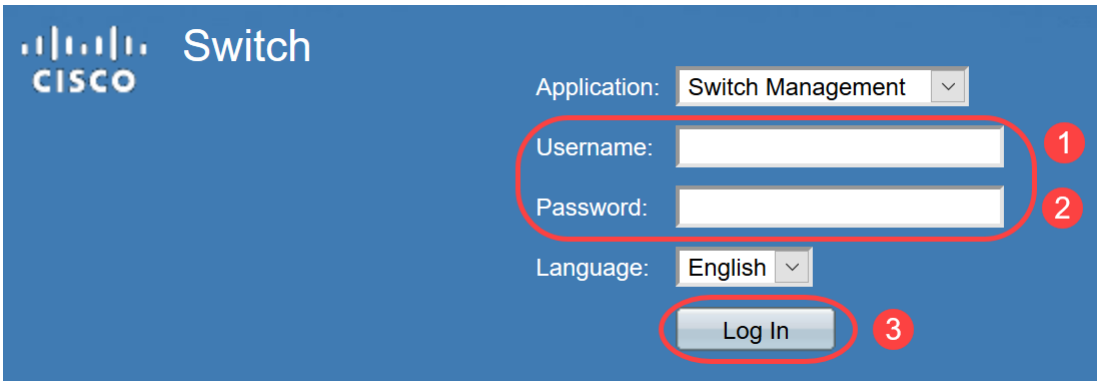
Conditions préalables

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

Importer à l'aide de l'interface utilisateur graphique

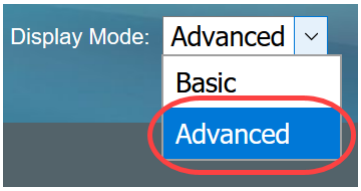
Étape 1

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



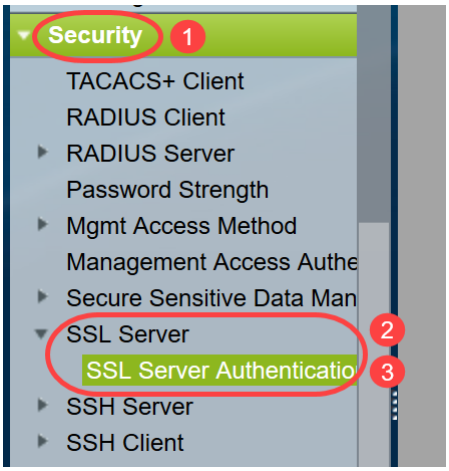
Étape 2

Dans le *mode Affichage* en haut à droite de l'interface utilisateur graphique, sélectionnez **Avancé** à l'aide de l'option de liste déroulante.



Étape 3

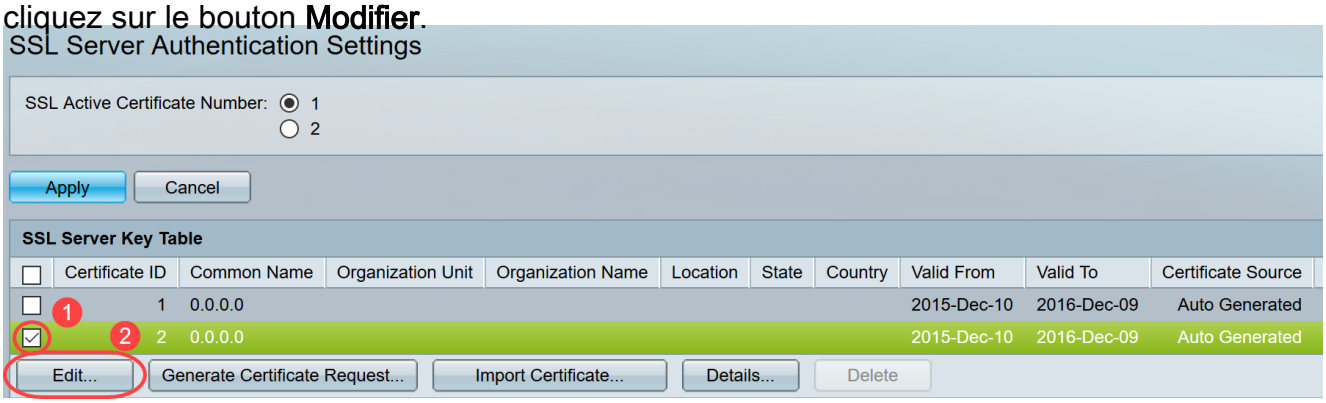
Accédez à **Security > SSL Server > SSL Server Authentication**.



Étape 4

Sélectionnez l'un des certificats *générés automatiquement*. Sélectionnez l'*ID de certificat* 1 ou 2 et

cliquez sur le bouton **Modifier**.



Étape 5

Pour générer un certificat auto-signé, dans la nouvelle fenêtre contextuelle, activez *Régénérer la clé RSA* et saisissez les paramètres suivants :

Longueur de la clé

Nom commun

Unité d'organisation

Nom de l'organisation

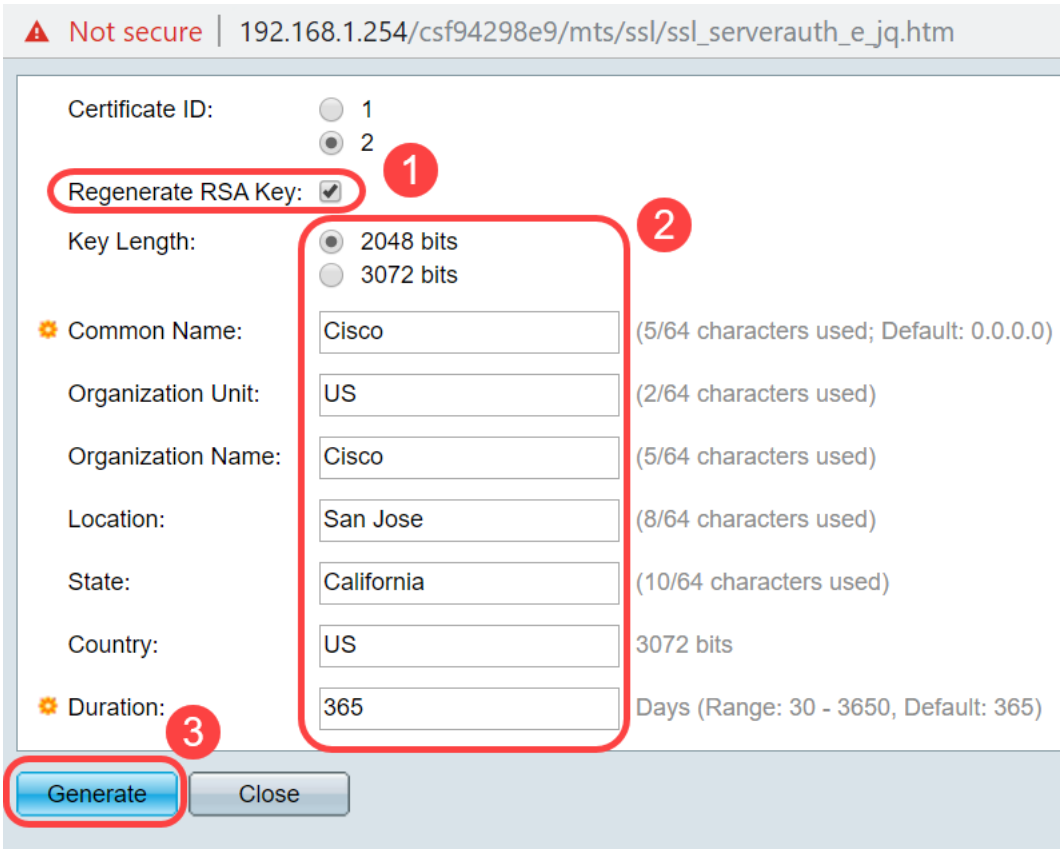
Emplacement

Province

Pays

Durée

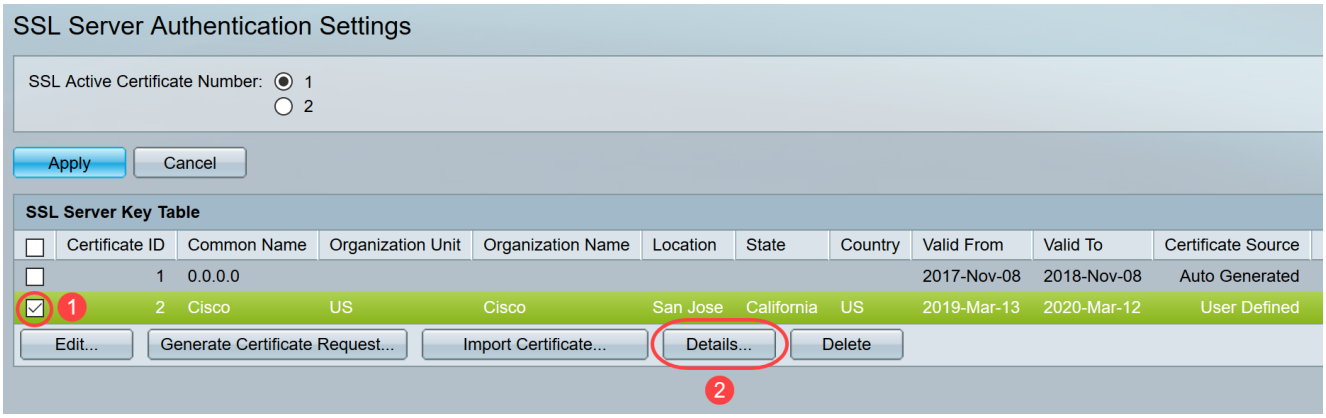
Cliquez sur **Generate**.



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

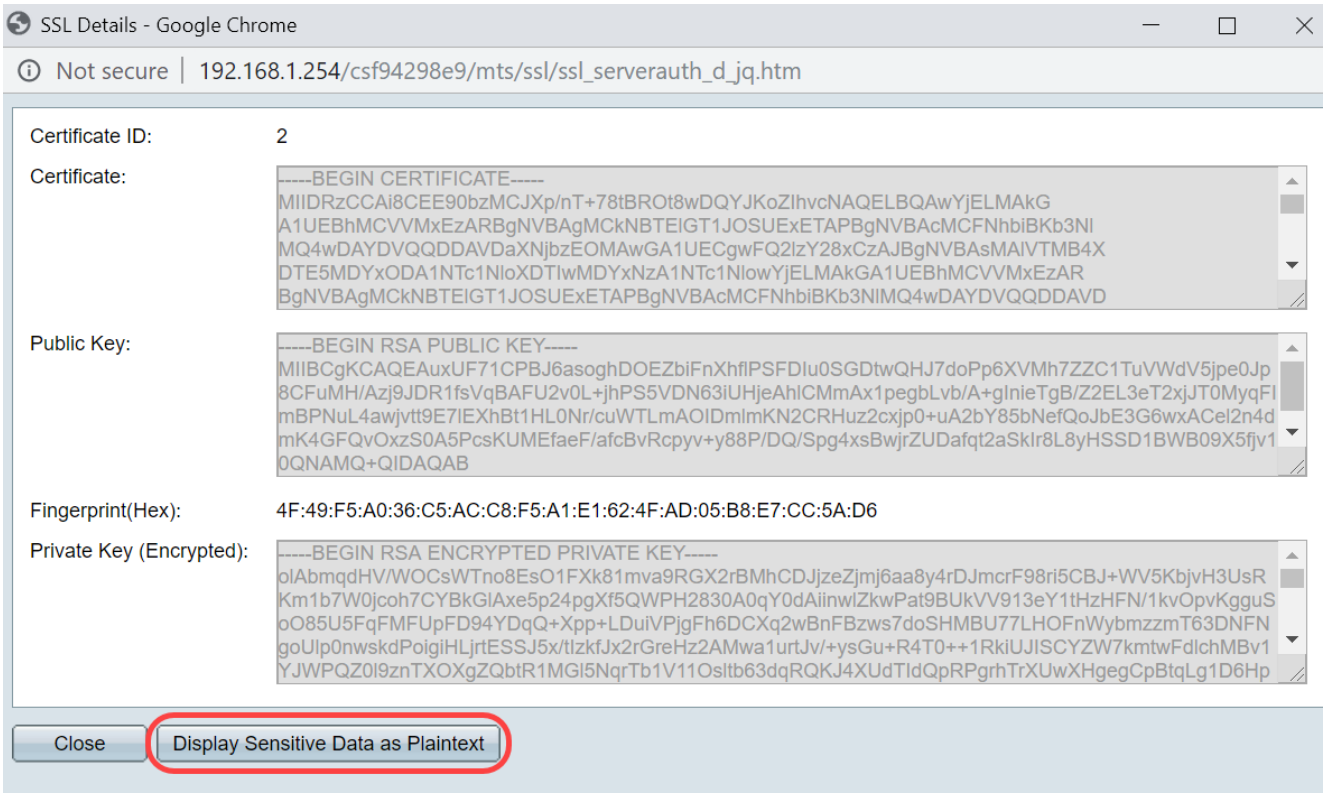
Étape 6

Vous pouvez maintenant voir le certificat *défini par l'utilisateur* sous la *table des clés du serveur SSL*. Sélectionnez le nouveau certificat et cliquez sur **Détails**.



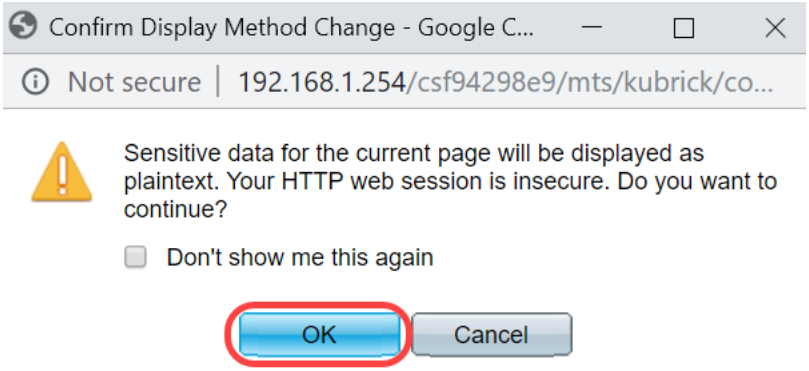
Étape 7

Dans la fenêtre contextuelle, vous pouvez voir les détails *Certificate*, *Public Key et Private Key (Encrypted)*. Vous pouvez les copier sur un autre bloc-notes. Cliquez sur **Afficher les données sensibles en texte clair**.



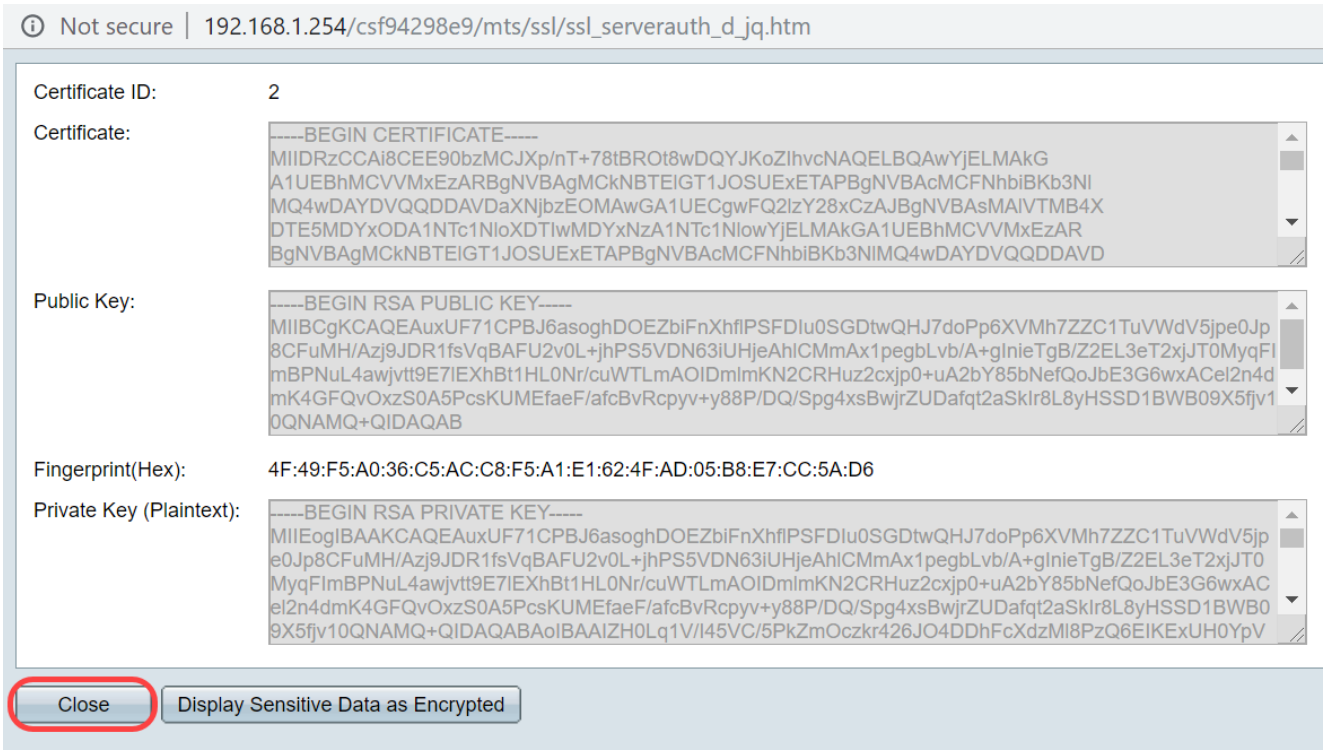
Étape 8

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



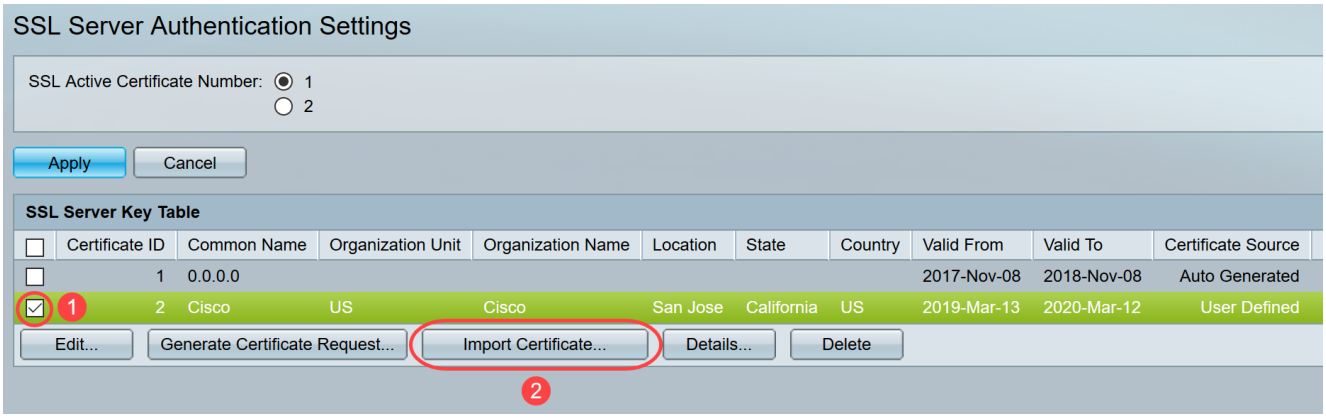
Étape 9

Vous pouvez maintenant voir la *clé privée* en texte clair. Copiez cette sortie en texte clair sur un fichier bloc-notes. Cliquez sur **Close**.



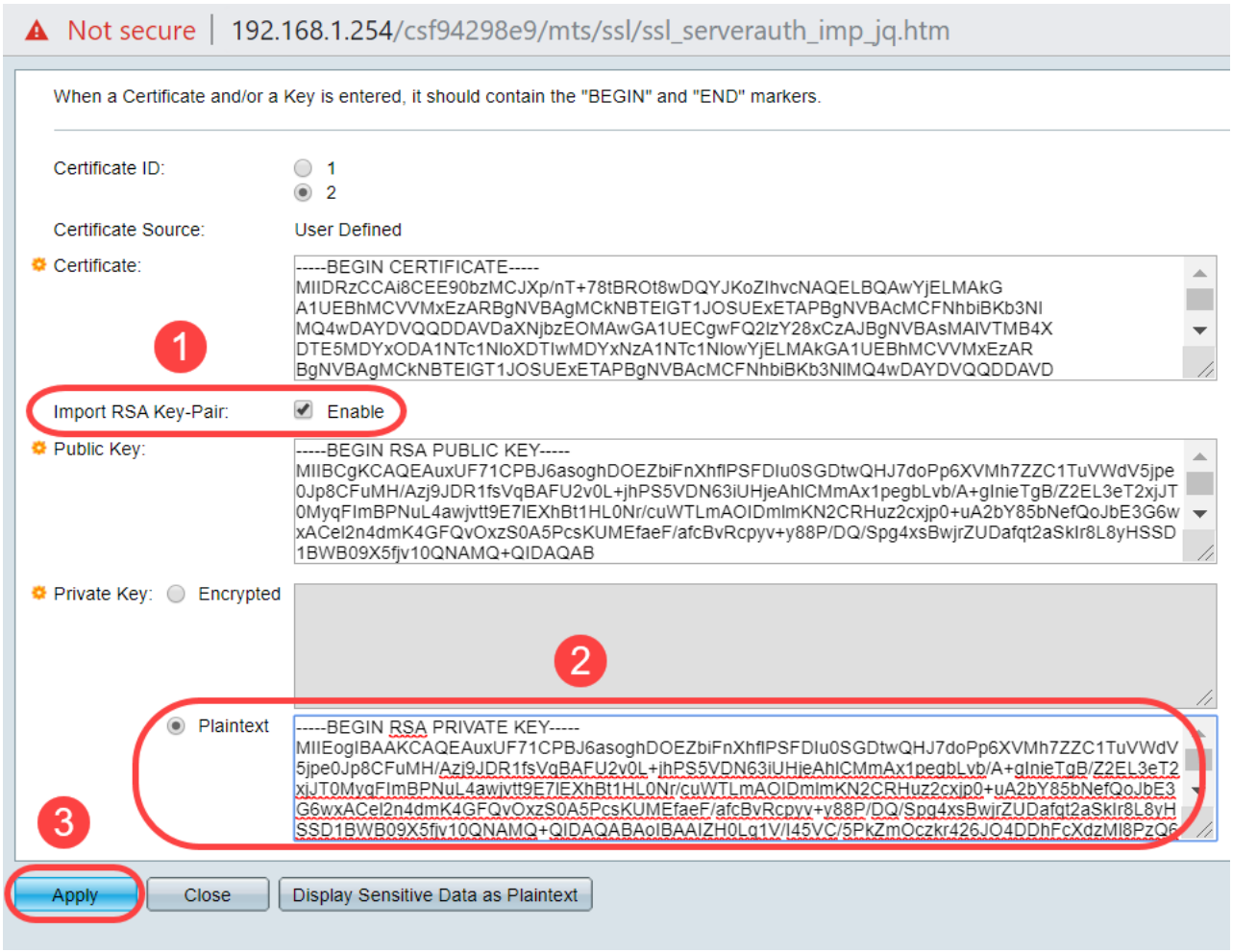
Étape 10

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



Étape 11

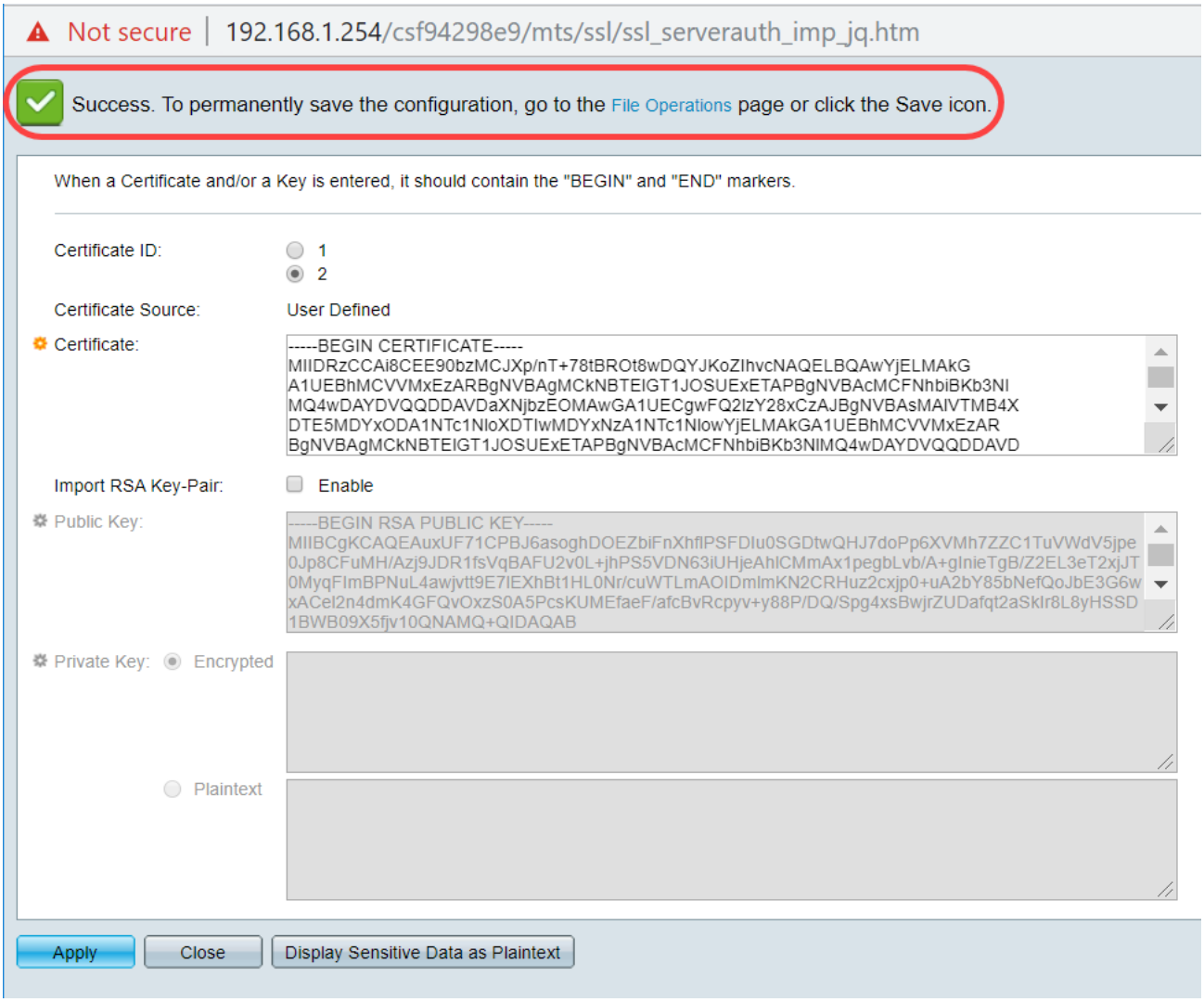
Dans la nouvelle fenêtre contextuelle, activez l'option *Importer la paire de clés RSA* et collez la clé privée (copiée à l'étape 9) en texte clair. Cliquez sur Apply.



Dans cet exemple, le mot clé *RSA* est inclus dans les *DEBUTS* et *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

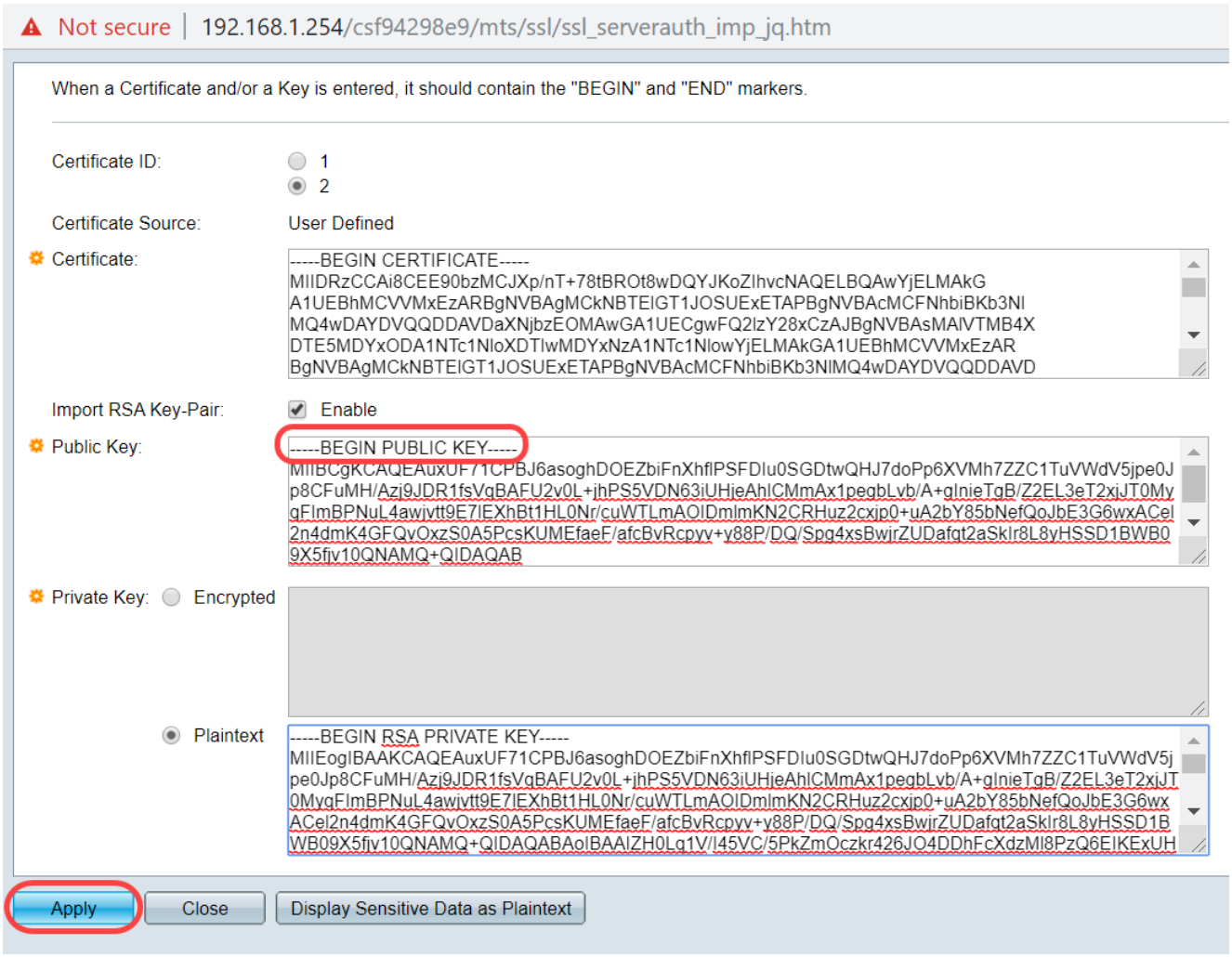
Les erreurs discutées concernent la clé publique. Normalement, deux types de formats de clé publique sont utilisés :

1. Fichier de clé publique RSA (PKCS#1) : Ceci est spécifique pour les clés RSA.
Elle commence et se termine par les balises :
—COMMENCER LA CLÉ PUBLIQUE RSA—
DONNÉES ENCODÉES BASE64
—FIN DE LA CLÉ PUBLIQUE RSA—

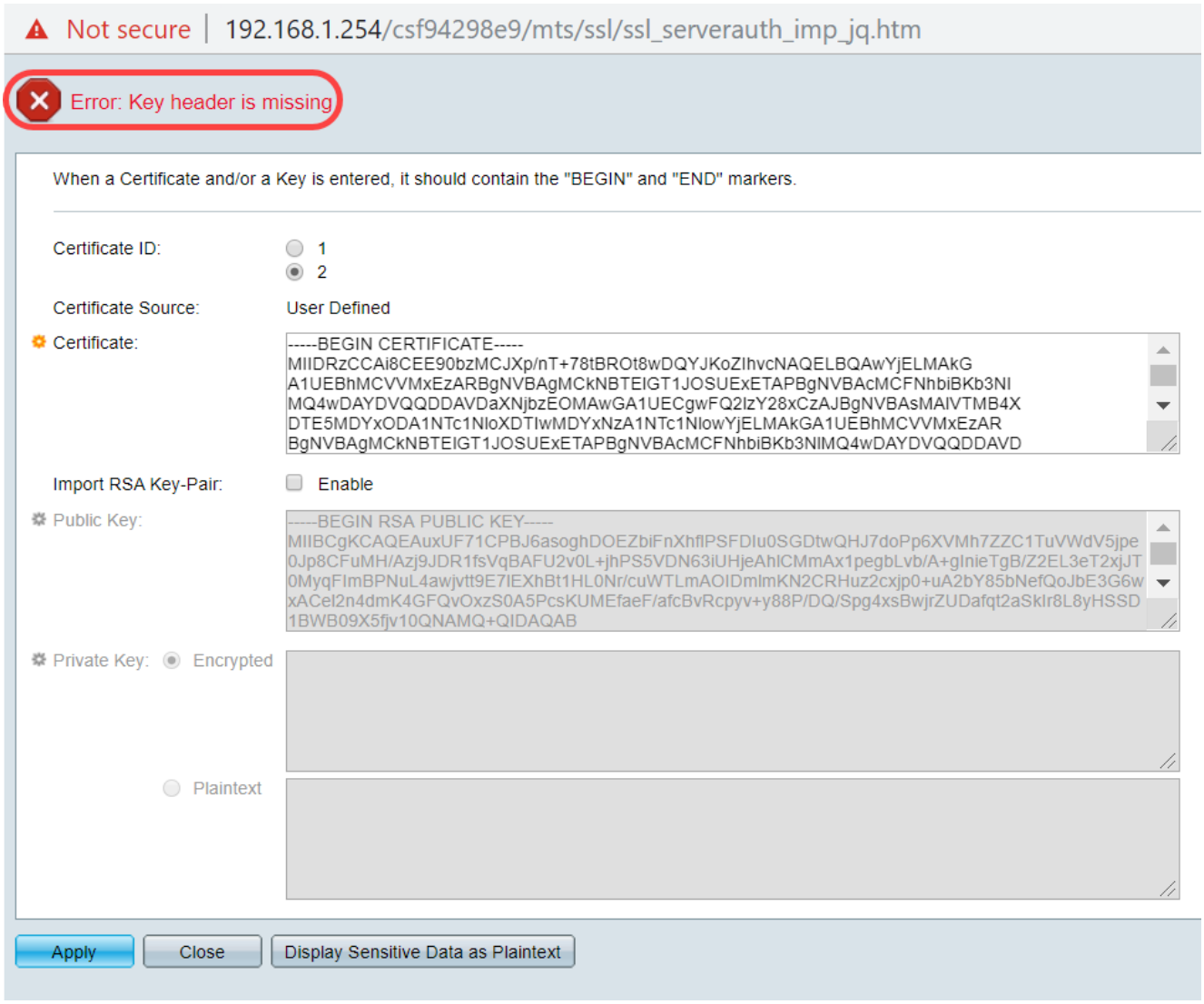
2. Fichier de clé publique (PKCS#8) : Il s'agit d'un format de clé plus générique qui identifie le type de clé publique et contient les données pertinentes.
Elle commence et se termine par les balises :
—COMMENCER LA CLÉ PUBLIQUE—
DONNÉES ENCODÉES BASE64
—CLÉ PUBLIQUE FINALE—

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 **Appliquer**.



Vous avez reçu le message, *Erreur : En-tête de clé manquant*. Fermez la fenêtre. Quelques modifications peuvent être apportées pour faire disparaître ce problème.

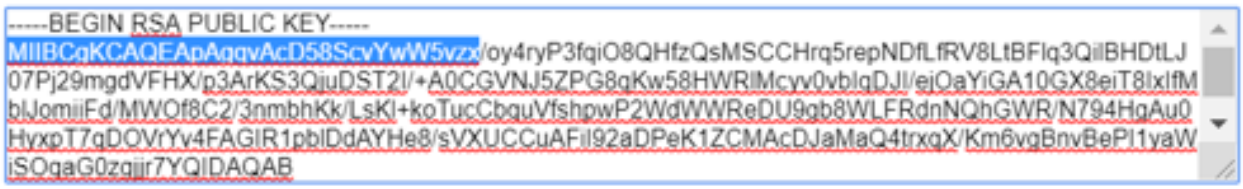


Pour corriger cette erreur :

Ajoutez le mot clé *RSA* au début de la clé publique : *COMMENCER LA CLÉ PUBLIQUE* ***RSA***

Ajoutez le mot clé *RSA* à la fin de la clé publique : *TERMINER LA CLÉ PUBLIQUE* ***RSA***

Supprimez les 32 premiers caractères du code clé. La partie mise en surbrillance ci-dessous est un exemple des 32 premiers caractères.

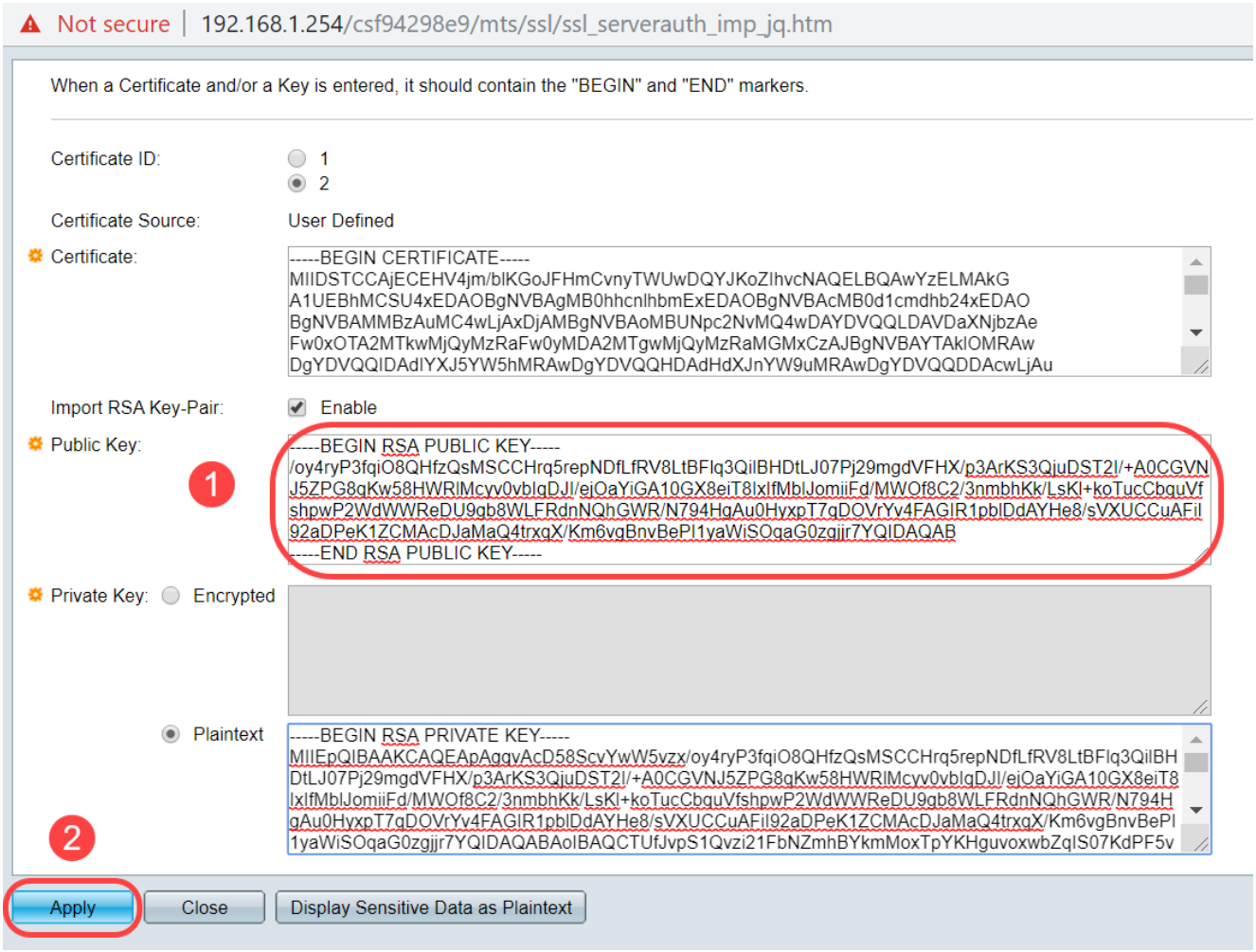


Lorsque vous appliquez les paramètres, vous n'obtiendrez pas l'*en-tête de clé* dans la plupart des cas.

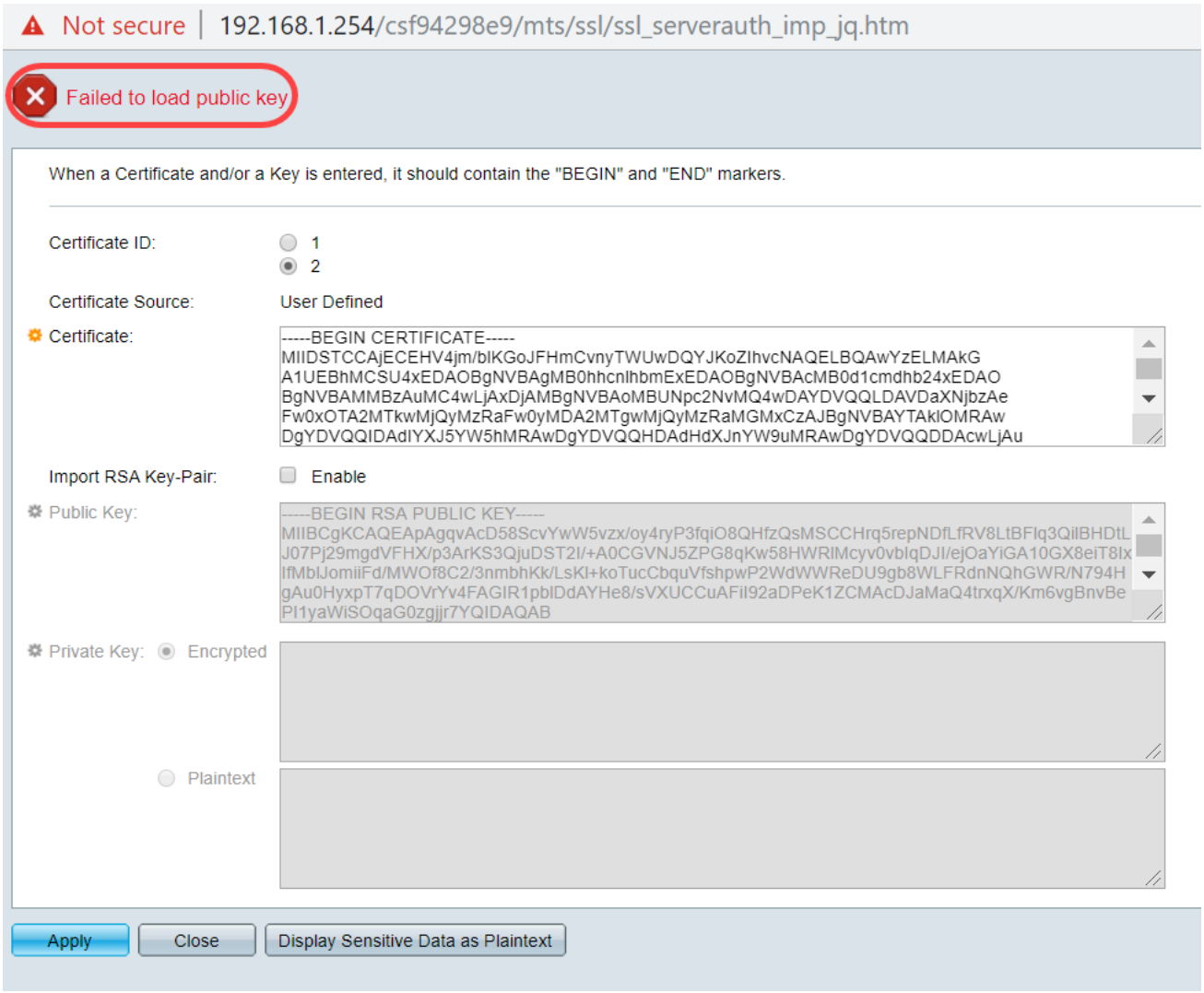
Échec du chargement de l'erreur de clé publique

Scénario 2 : Vous avez généré un certificat sur un commutateur et l'avez importé sur un autre

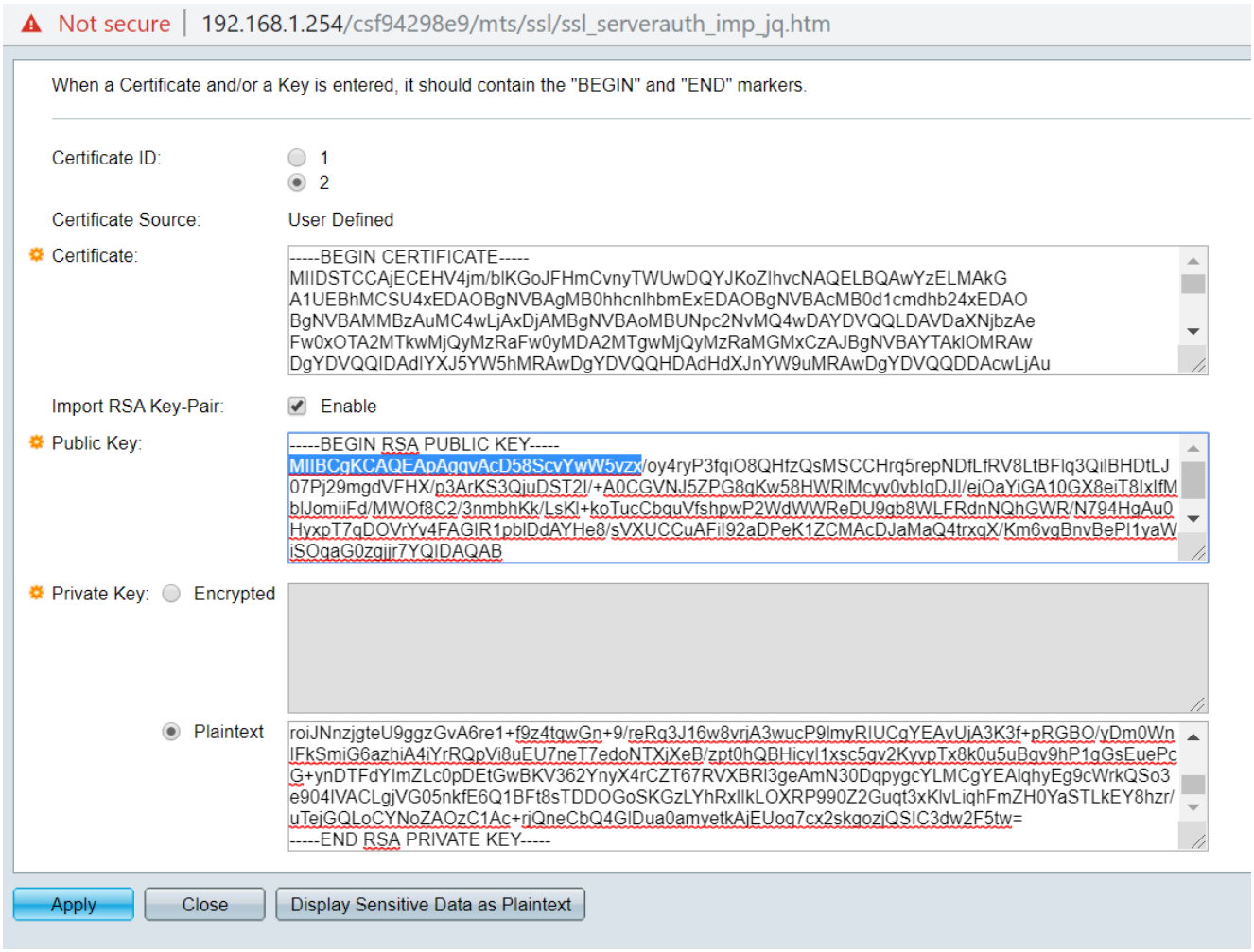
commutateur. Vous avez copié et collé la clé publique après avoir supprimé les 32 premiers caractères et cliqué sur **Appliquer**.



L'erreur *Échec du chargement de la clé publique* s'affiche à l'écran.



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



Importer à l'aide de CLI

Étape 1

Pour importer un certificat à l'aide de l'interface de ligne de commande, 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.

```
—COMMENCER LA CLÉ PRIVÉE RSA—
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...24 lignes tronquées....
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
—FIN DE LA CLÉ PRIVÉE RSA—
—COMMENCER LA CLÉ PUBLIQUE RSA—
MIIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkf0l
...3 lignes tronquées....
```

```
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
—FIN DE LA CLÉ PUBLIQUE RSA—
—CERTIFICAT DE DÉBUT—
MIIFvTCCBKWgIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
—28 lignes tronquées...
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwJOcsTrMV
JDPtnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBHt1VyjAP
—CERTIFICAT DE FIN—
.
Le certificat a été importé
Émis par : C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation Secure
Server CA
Valide à partir de : 14 juin 00:00:00 2017 GMT
Valide : 11 septembre 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 digitale SHA : xxxxxx
```

Conclusion

Vous avez maintenant appris les étapes permettant d'importer un certificat sur les commutateurs des gammes Sx350 et Sx550X à l'aide de l'interface utilisateur graphique et de l'interface de ligne de commande.