Cómo importar el certificado en los switches Sx350 y Sx550X Series

Objetivo

Este objetivo de este documento es proporcionar los pasos para importar con éxito un certificado en los switches de las series Sx350 y Sx550X utilizando la interfaz gráfica de usuario (GUI) y la interfaz de línea de comandos (CLI).

Table Of Contents

Introducción

Uno de los problemas encontrados al importar un certificado en los switches Sx350 y Sx550X es que el usuario se enfrenta a ***un encabezado de clave que falta*** y/o ***no pudo cargar*** errores de ***clave pública***. Este documento explicará cómo superar estos errores para importar un certificado correctamente. Un certificado es un documento electrónico que identifica a una persona, un servidor, una empresa u otra entidad y asocia esa entidad a una clave pública. Los certificados se utilizan en una red para proporcionar acceso seguro. Los certificados pueden ser firmados automáticamente o firmados digitalmente por una autoridad certificadora externa (CA). Un certificado autofirmado, como su nombre indica, está firmado por su propio creador. Las CA administran solicitudes de certificados y emiten certificados a entidades participantes como hosts, dispositivos de red o usuarios. Un certificado digital firmado por CA se considera estándar del sector y más seguro.

Dispositivos y versión de software aplicables

- SG350 versión 2.5.0.83
- SG350X versión 2.5.0.83
- SG350XG versión 2.5.0.83
- SF350 versión 2.5.0.83
- SG550X versión 2.5.0.83
- SF550X versión 2.5.0.83
- SG550XG versión 2.5.0.83
- SX550X versión 2.5.0.83

Prerequisites

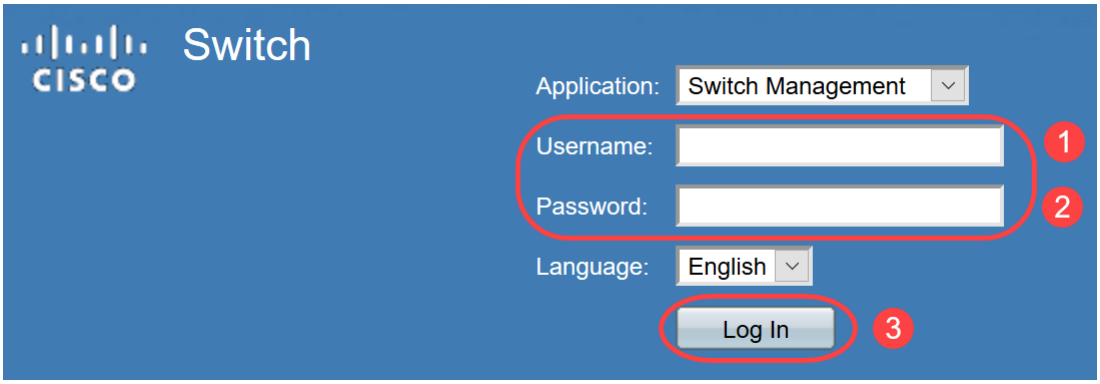
Debe tener un certificado de autoridad certificadora (CA) o autofirmado. En este artículo se

incluyen los pasos para obtener un certificado autofirmado. Para obtener más información sobre los certificados de CA, haga clic aquí.

Importar mediante la GUI

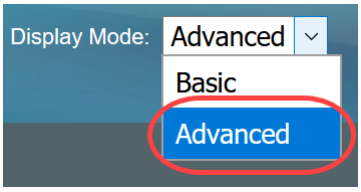
Paso 1

Inicie sesión en la GUI del switch ingresando su *nombre de usuario* y *contraseña*. Haga clic en **Iniciar sesión**.



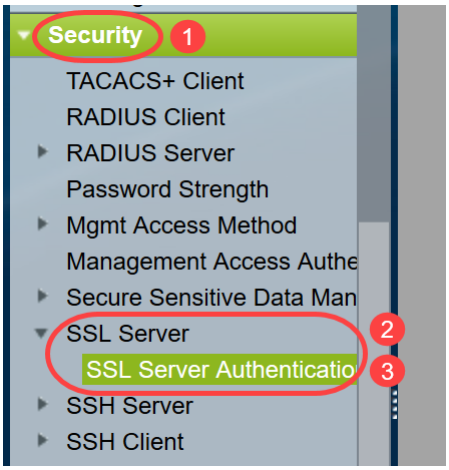
Paso 2

En el *Modo de visualización* en la parte superior derecha de la GUI, elija **Avanzado** usando la opción desplegable.



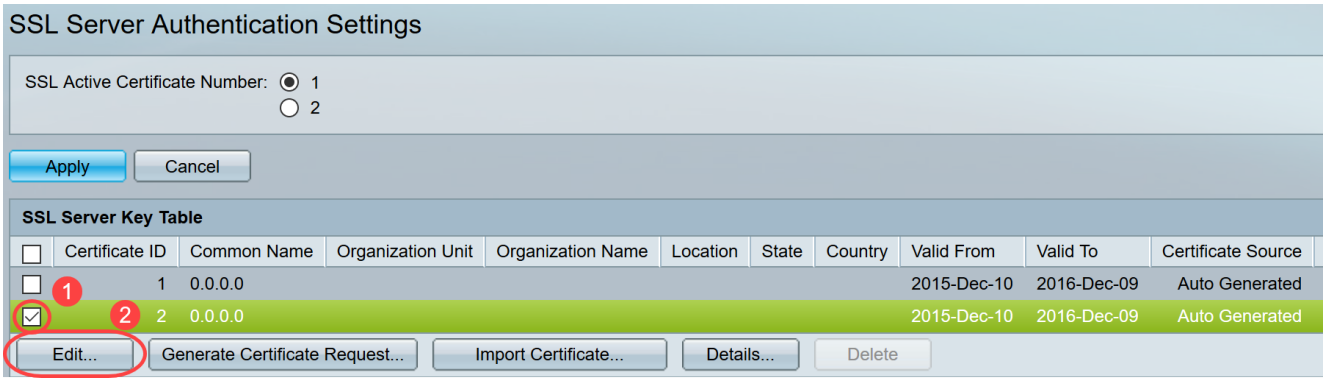
Paso 3

Vaya a **Security > SSL Server > SSL Server Authentication**.



Paso 4

Seleccione uno de los certificados que se *Generó automáticamente*. Seleccione el *ID de certificado* 1 ó 2 y haga clic en el **botón Editar**.



Paso 5

Para generar un certificado autofirmado, en la nueva ventana emergente active *Regenerar clave RSA* e ingrese los siguientes parámetros:

Longitud de la clave

Nombre común

Unidad de organización

Nombre de la organización

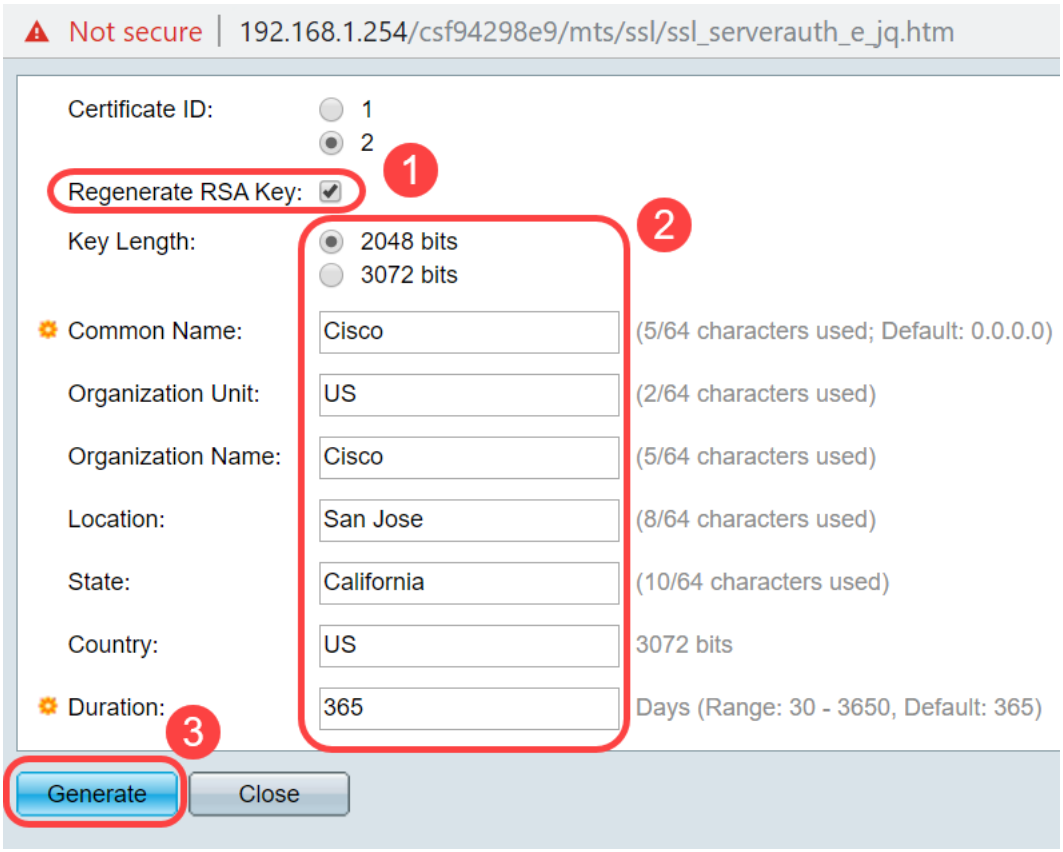
Ubicación

Estado

País

Duration

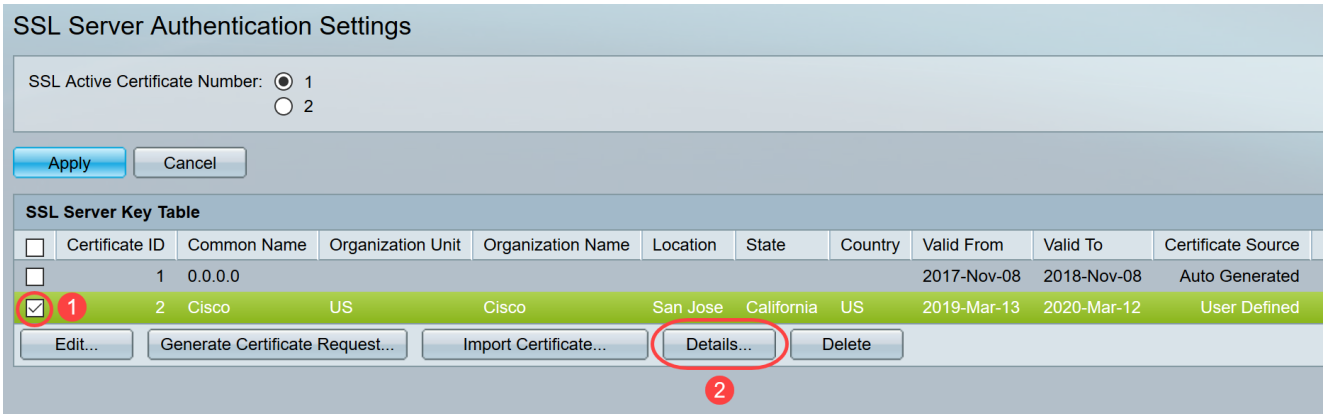
Haga clic en **Generar**.



También puede crear un certificado de una CA de terceros.

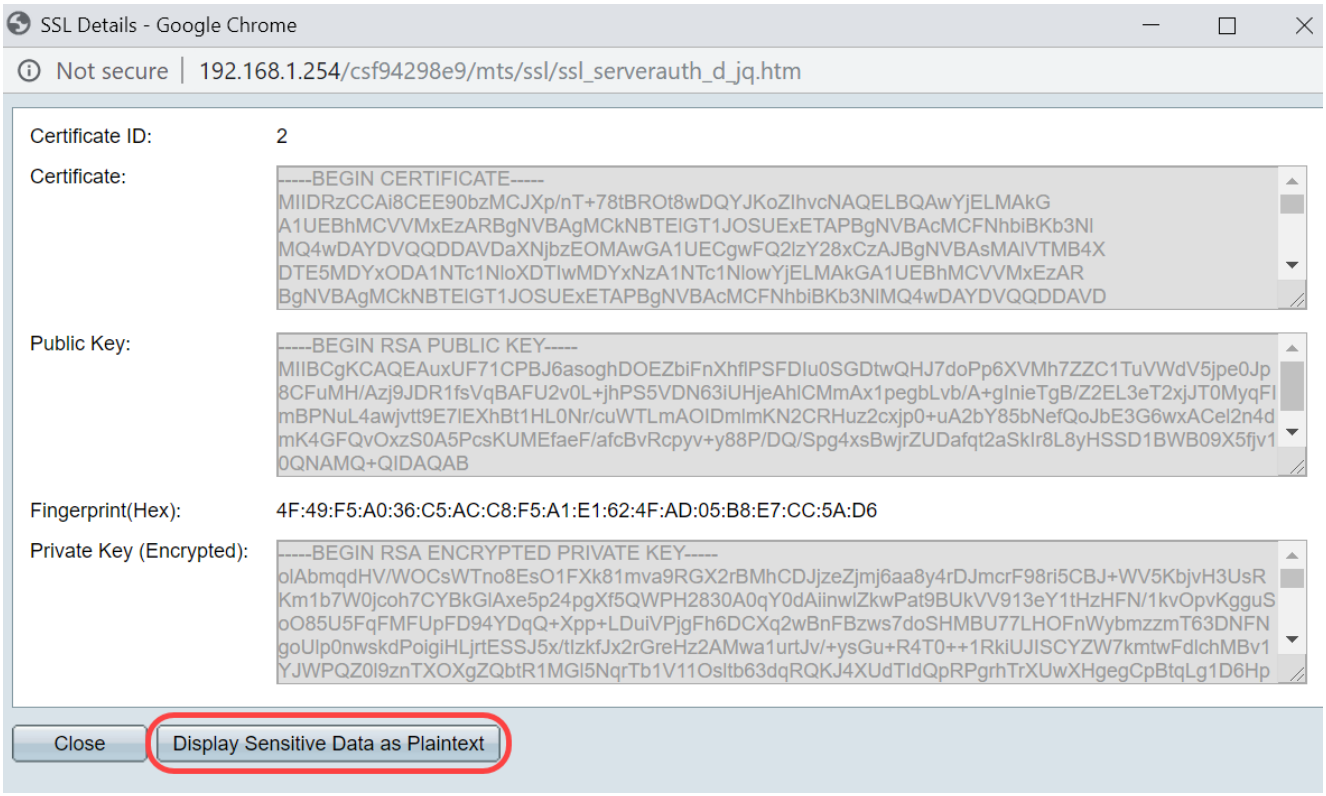
Paso 6

Ahora podrá ver el certificado *definido por el usuario* bajo la *Tabla de claves de servidor SSL*. Seleccione el certificado recién creado y haga clic en **Detalles**.



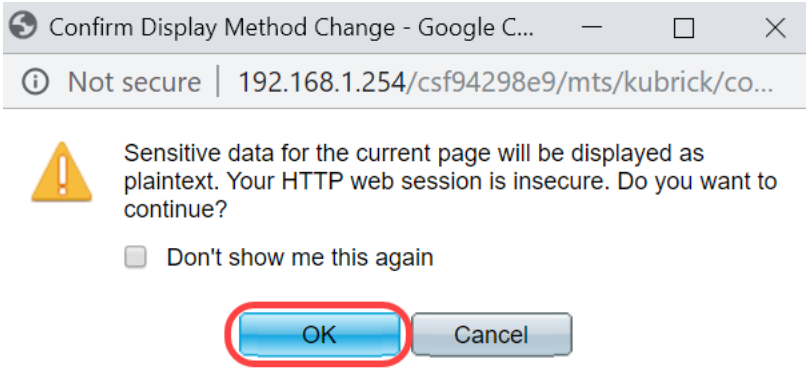
Paso 7

En la ventana emergente podrá ver los detalles *Certificate*, *Public Key y Private Key (Encrypted)*. Puede copiarlos en un archivo de bloc de notas independiente. Haga clic en **Mostrar datos confidenciales como texto sin formato**.



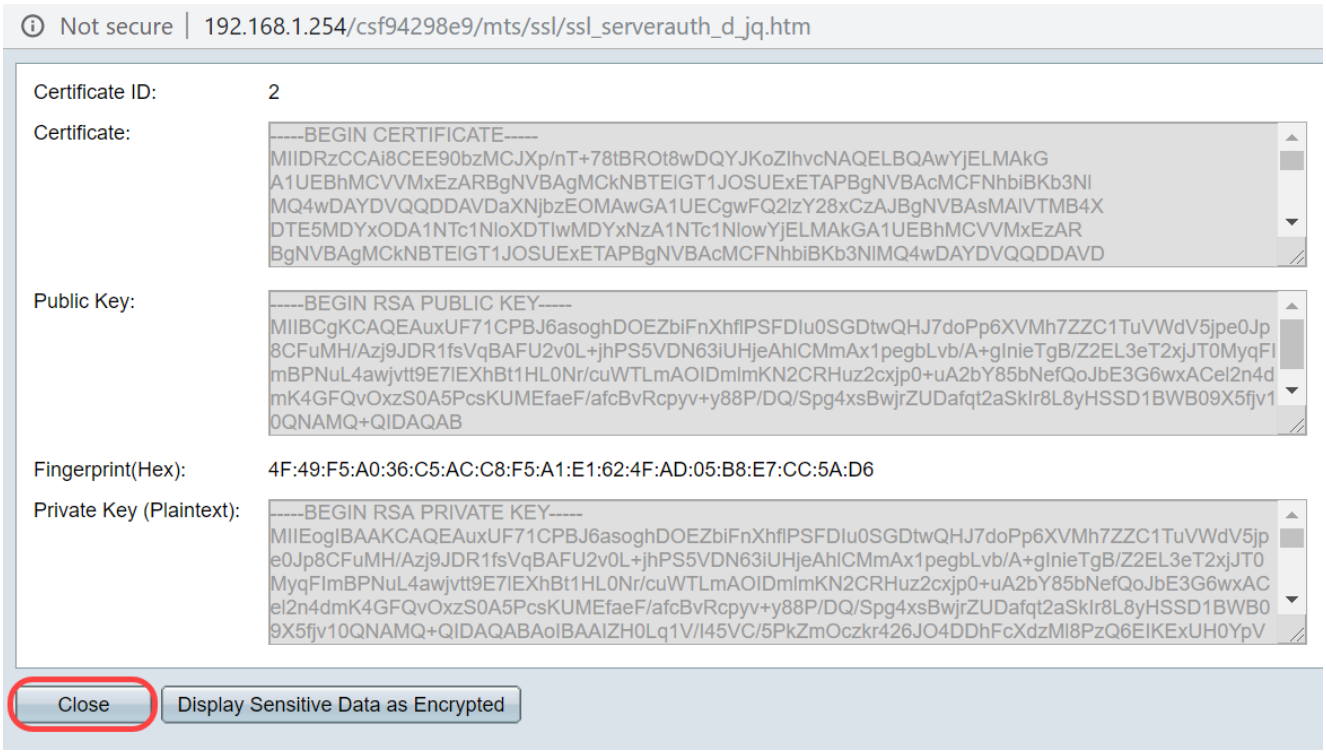
Paso 8

Se abrirá una ventana emergente para confirmar la visualización de la clave privada como texto sin formato, haga clic en **Aceptar**.



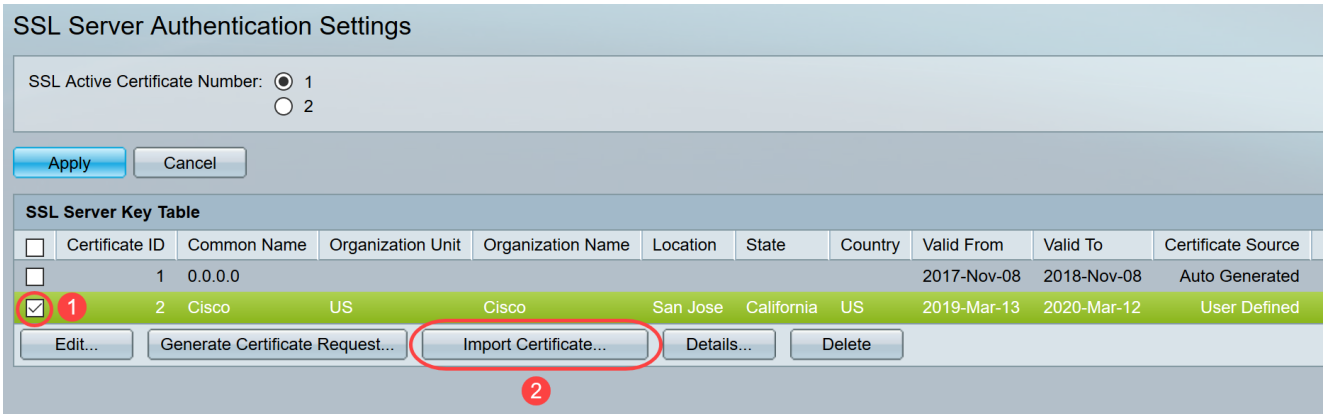
Paso 9

Ahora podrá ver la *clave privada* en formato de texto sin formato. Copie ese resultado de texto sin formato en un archivo de bloc de notas. Haga clic en Close (Cerrar).



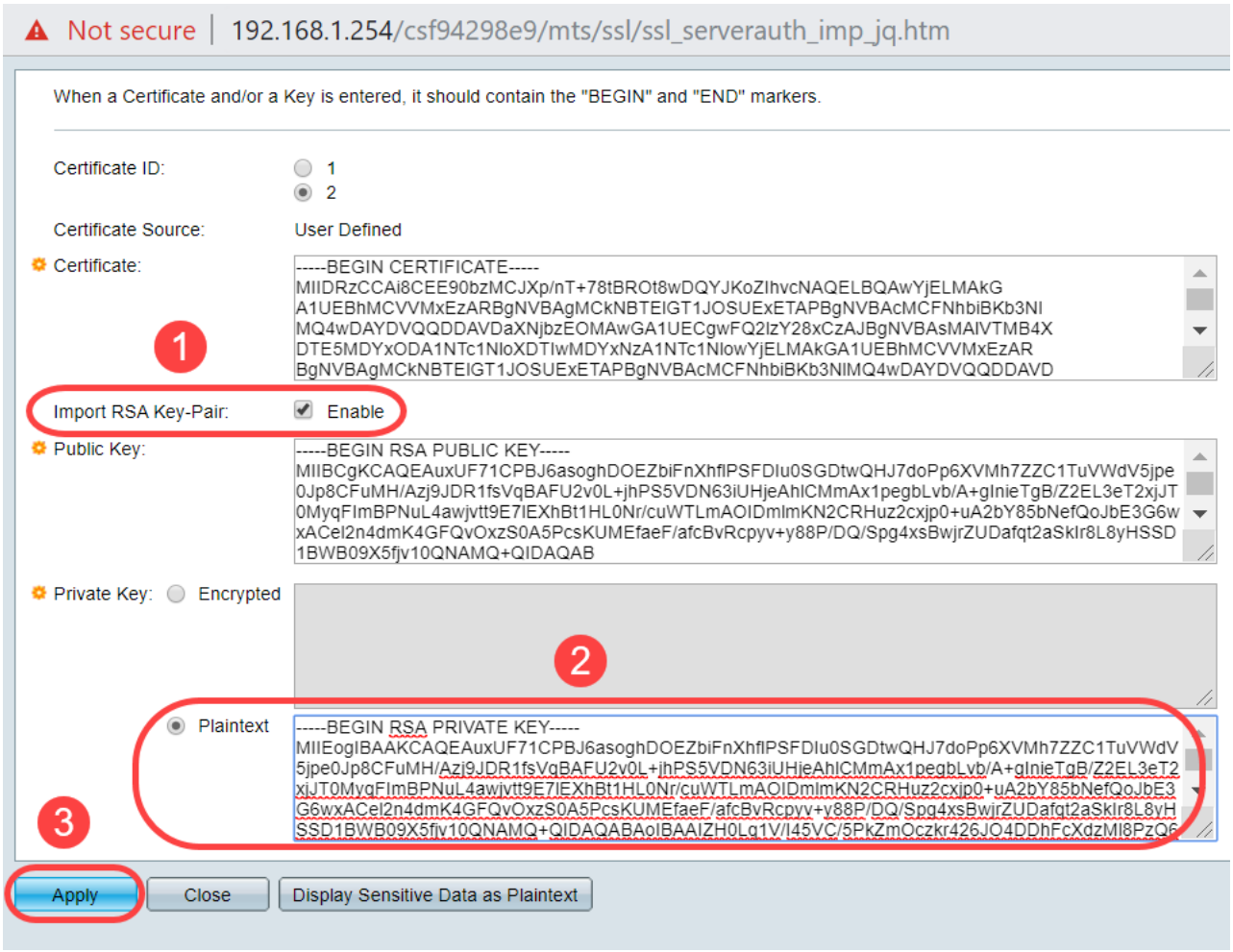
Paso 10

Seleccione el certificado *definido por el usuario* recién creado y haga clic en **Importar certificado**.



Paso 11

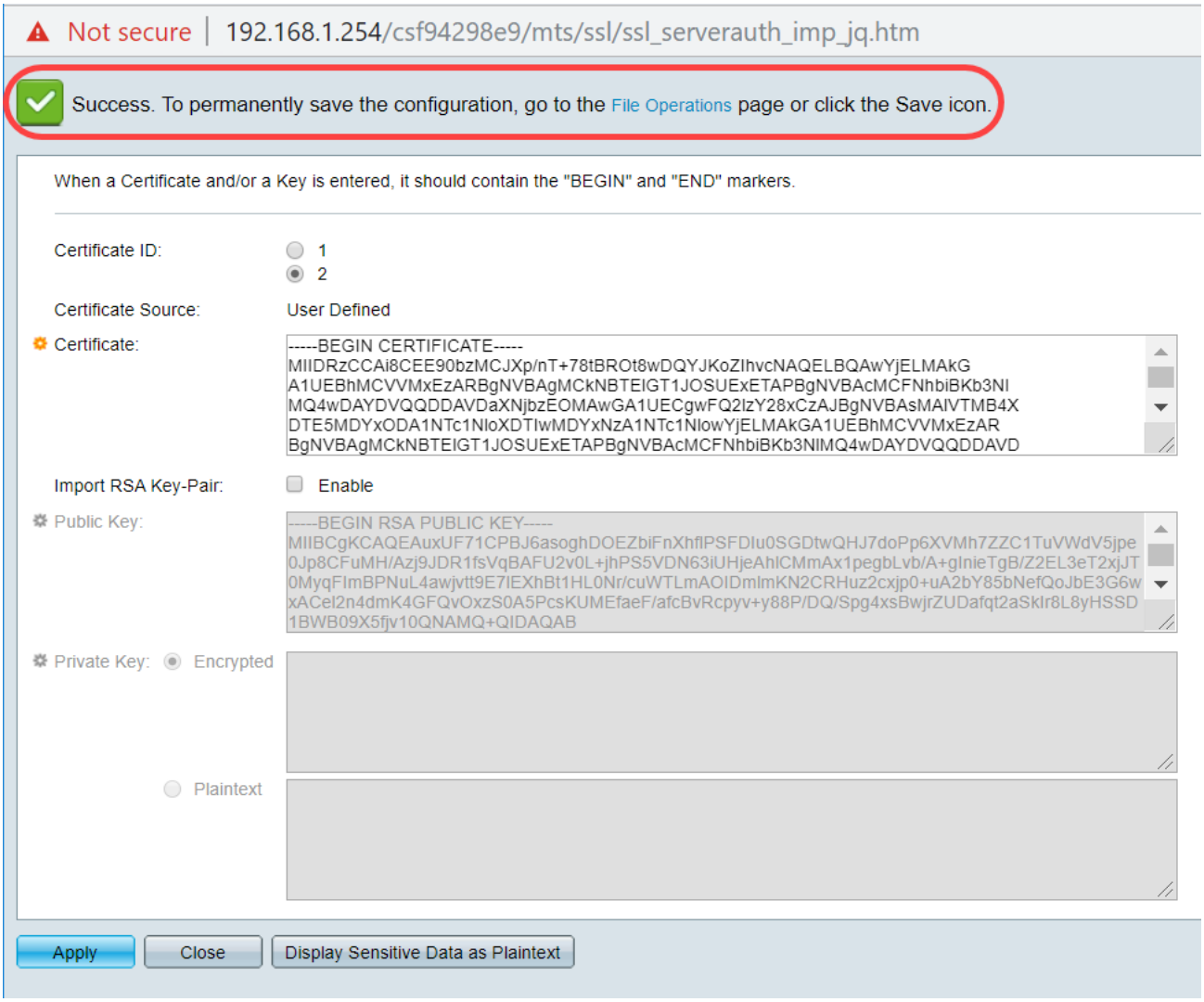
En la nueva ventana emergente, active la opción *Importar par de claves RSA* y pegue la clave privada (copiada en el paso 9) en formato de texto sin formato. Haga clic en Apply (Aplicar).



En este ejemplo, la palabra clave, *RSA*, se incluye en el *COMIENZO* y el *FIN* de la *Clave Pública*.

Paso 12

Verá la notificación de éxito en la pantalla. Puede cerrar esta ventana y guardar la configuración en el switch.



Errores posibles

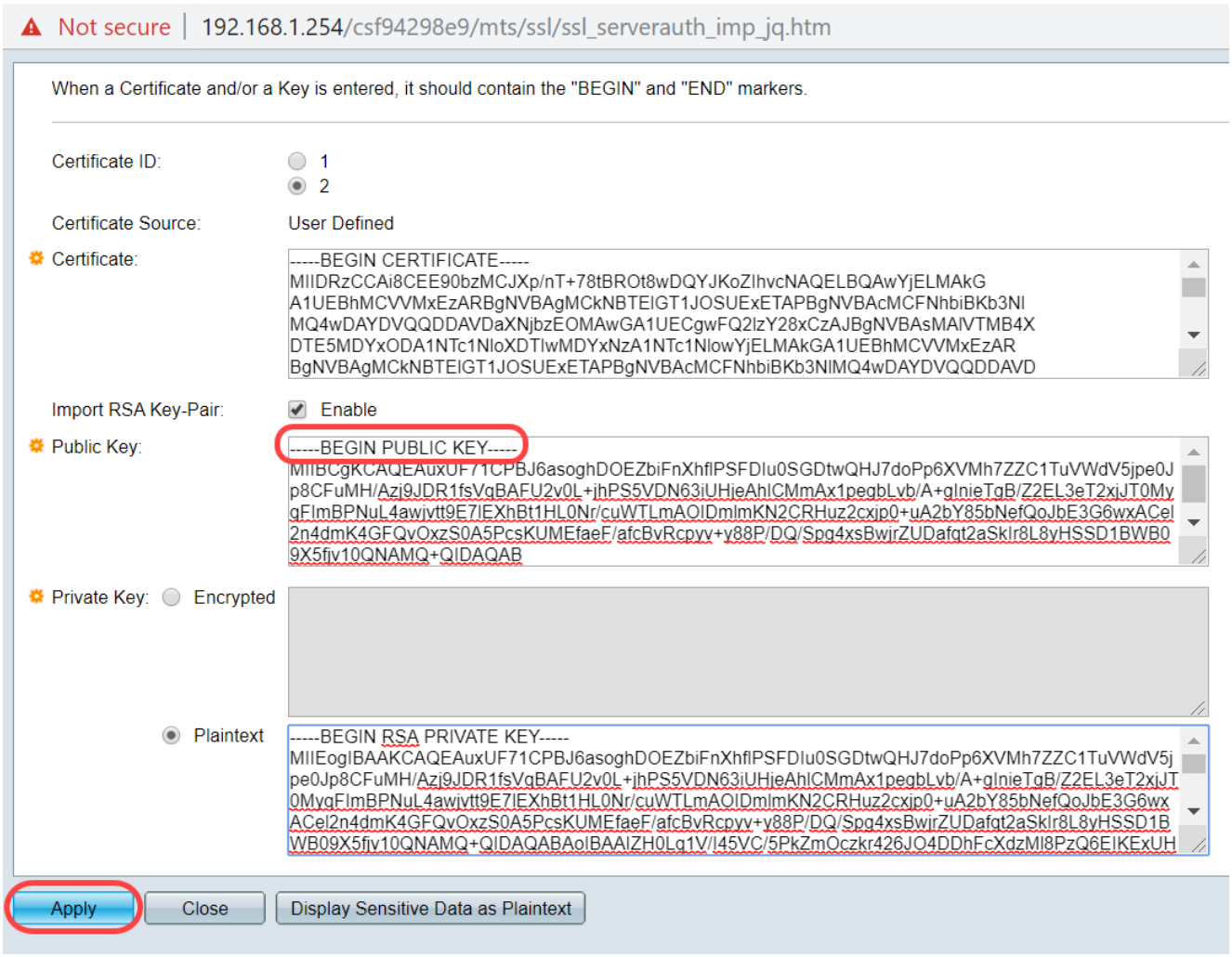
Los errores analizados pertenecen a la clave pública. Normalmente se utilizan dos tipos de formatos de clave pública:

1. Archivo de clave pública RSA (PKCS#1): Esto es específico para las claves RSA. Comienza y termina con las etiquetas:
—COMENZAR CLAVE PÚBLICA RSA—
DATOS CODIFICADOS BASE64
—FINALIZAR CLAVE PÚBLICA RSA—

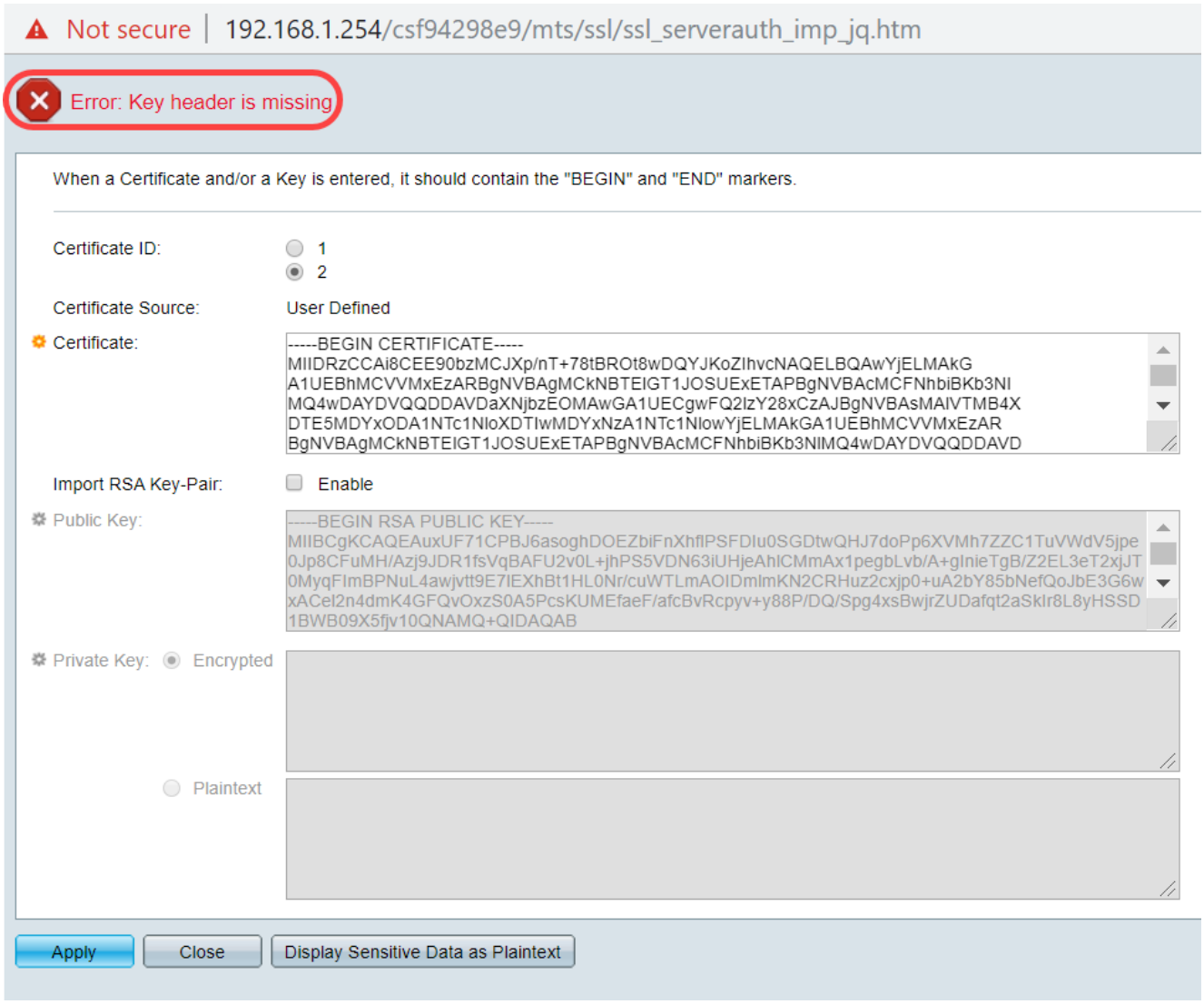
2. Archivo de clave pública (PKCS#8): Este es un formato de clave más genérico que identifica el tipo de clave pública y contiene los datos relevantes.
Comienza y termina con las etiquetas:
—INICIE CLAVE PÚBLICA—
DATOS CODIFICADOS BASE64
—FINALIZAR CLAVE PÚBLICA—

Falta el encabezado de la clave

Escenario 1: Ha generado el certificado de una CA de terceros. Ha copiado y pegado la clave pública y ha hecho clic en **Aplicar**.



Ha recibido el mensaje, *Error: Falta el encabezado de la clave*. Cerrar ventana Se pueden hacer algunas modificaciones para hacer desaparecer este problema.

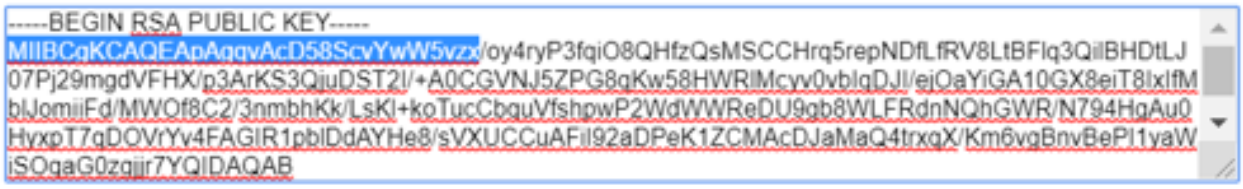


Para corregir este error:

Agregue la palabra clave, *RSA*, al principio de la clave pública: *COMIENCE **LA** CLAVE PÚBLICA **RSA***

Agregue la palabra clave, *RSA*, al final de la Clave Pública: *CLAVE PÚBLICA **RSA** FINAL*

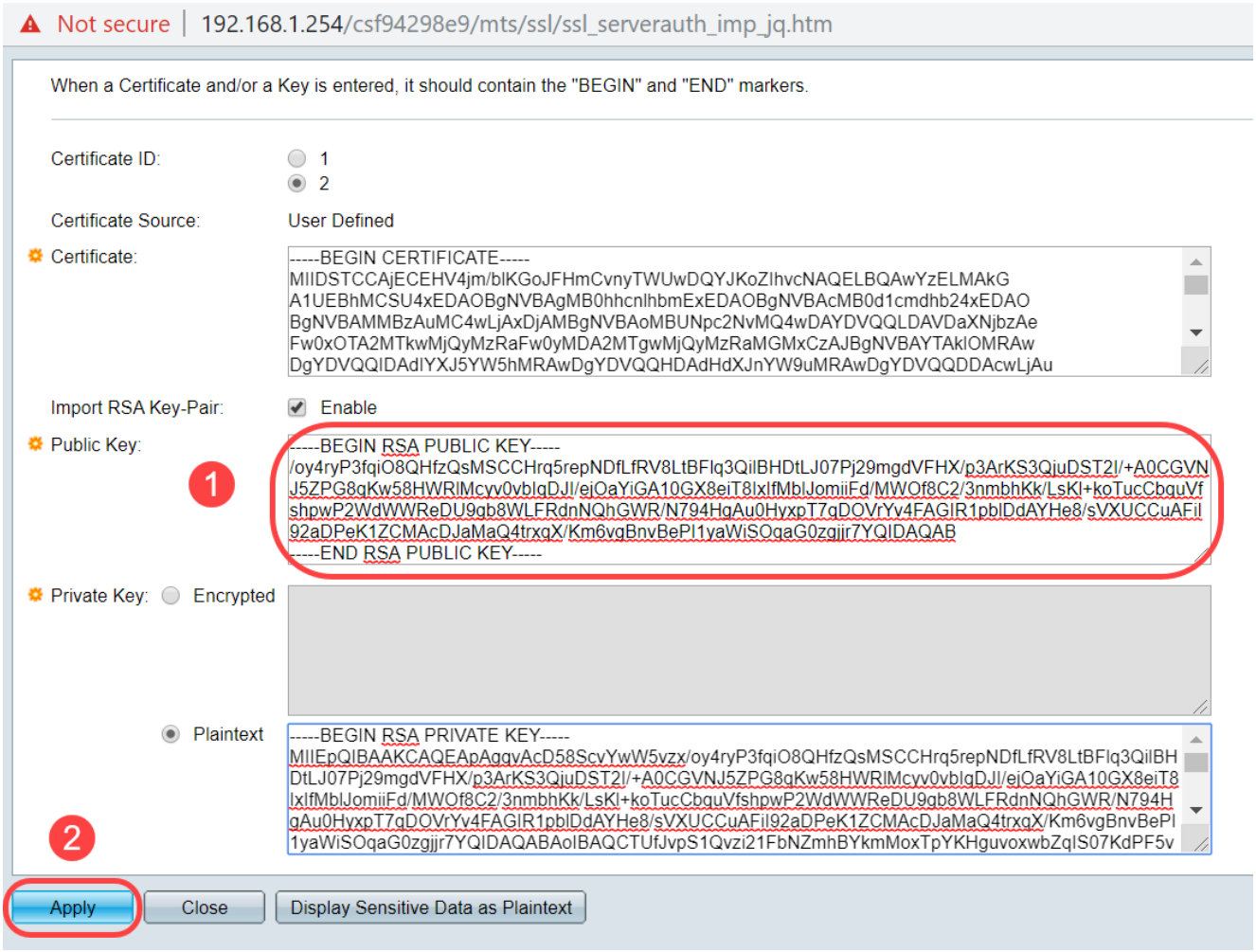
Quite los primeros 32 caracteres del código de clave. La parte resaltada que se muestra a continuación es un ejemplo de los primeros 32 caracteres.



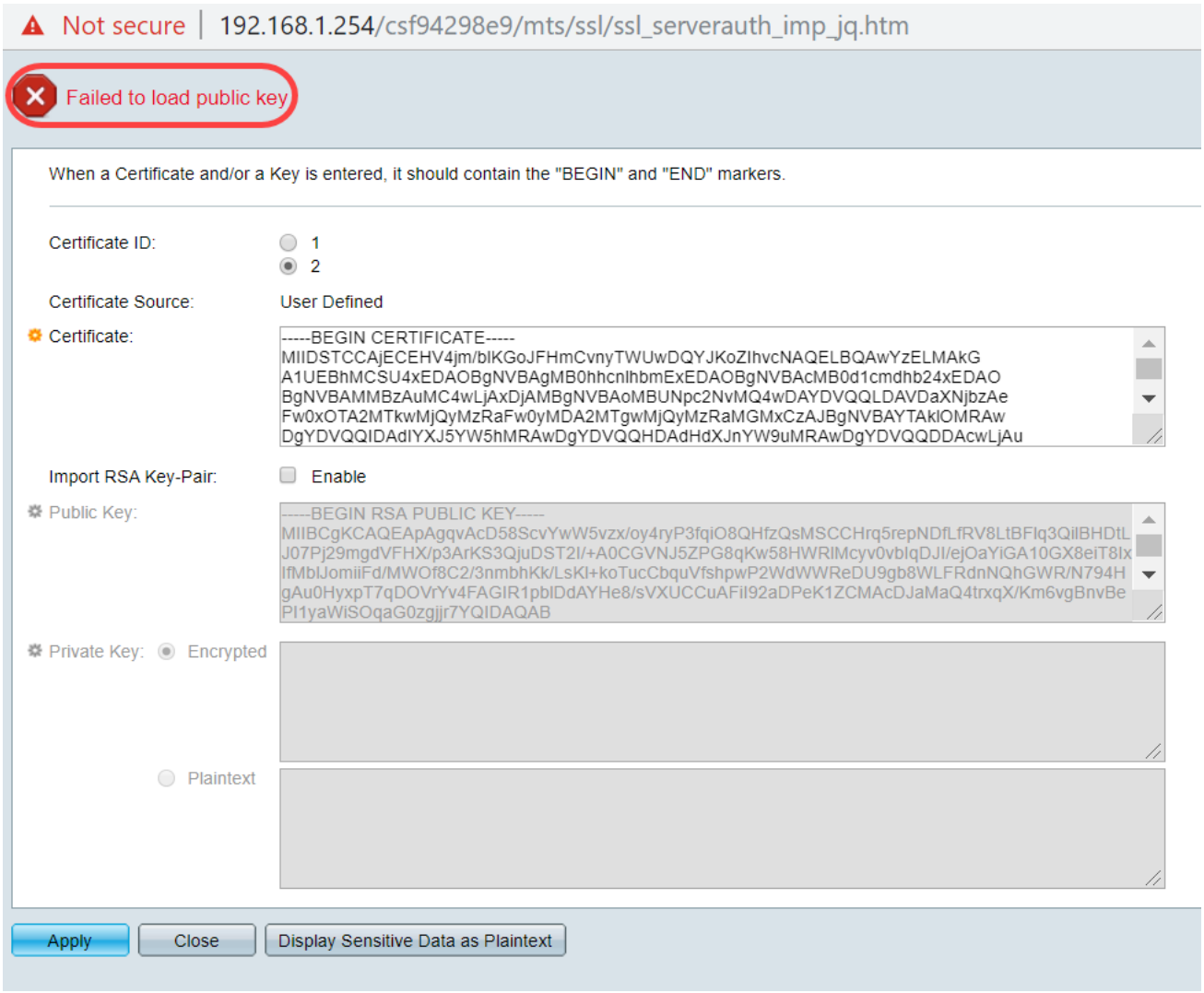
Cuando aplique la configuración, no obtendrá el error *Key header is missing* en la mayoría de los casos.

Error al cargar el error de clave pública

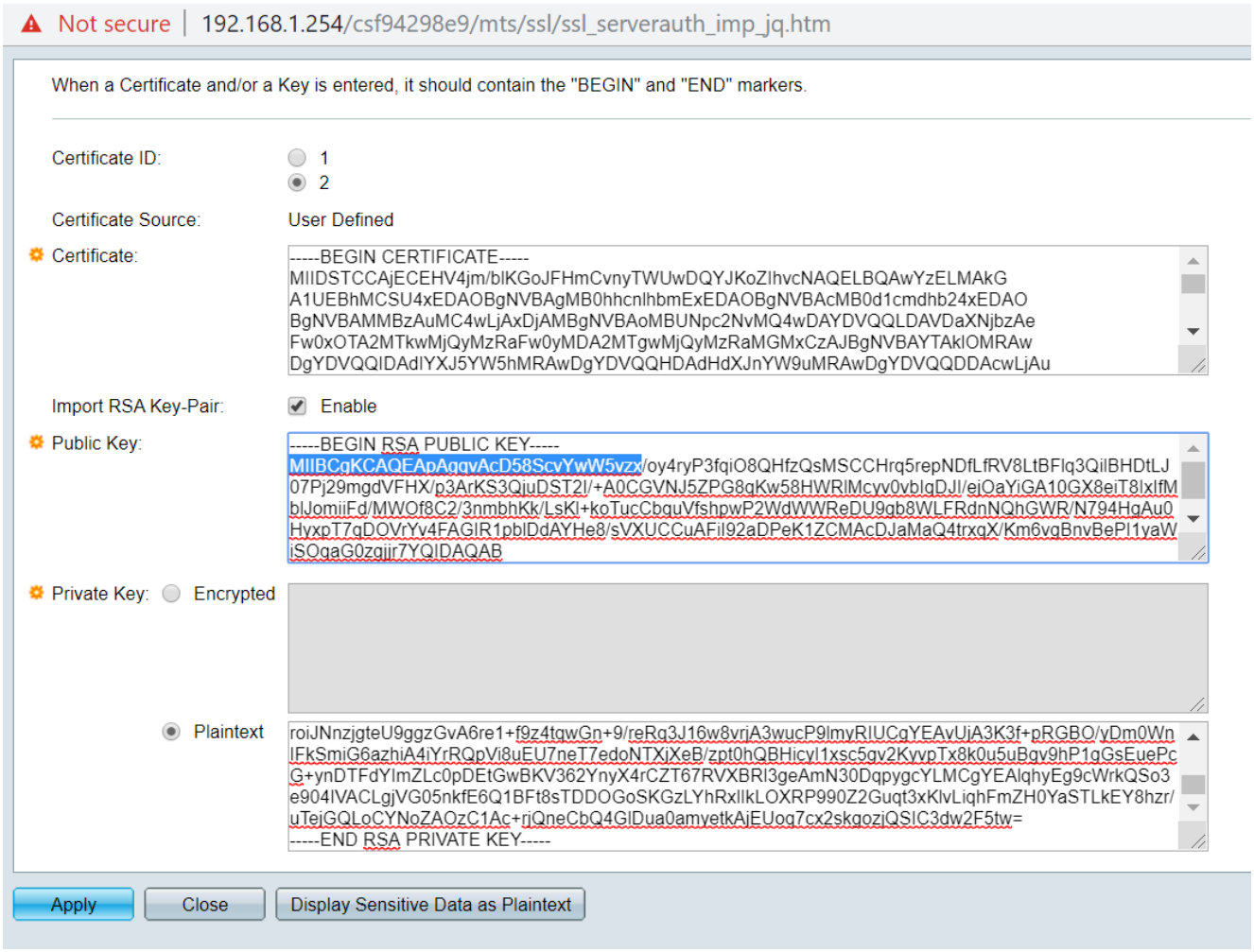
Escenario 2: Ha generado un certificado en un switch y lo ha importado en otro switch. La clave pública se copió y pegó después de quitar los primeros 32 caracteres y se hizo clic en **Aplicar**.



Se ha producido el error *Failed to load public key* en la pantalla.



Para corregir este error, NO elimine los primeros 32 caracteres de la clave pública en este caso.



Importar mediante CLI

Paso 1

Para importar el certificado mediante CLI, introduzca el siguiente comando.

```
switch(config)#crypto certificate [certificate number] import
```

El certificado 2 se importa en este ejemplo.

```
switch(config)#importación de certificado 2 de criptografía
```

Paso 2

Pegar la entrada; **agregue un punto (.)** en una línea independiente después de la entrada.

```
—COMENZAR CLAVE PRIVADA RSA—
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...truncado 24 líneas....
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
—FINALIZAR CLAVE PRIVADA RSA—
—COMENZAR CLAVE PÚBLICA RSA—
MIIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfT0l
...3 líneas truncadas....
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
—FINALIZAR CLAVE PÚBLICA RSA—
—CERTIFICADO DE INICIO—
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
—truncado 28 líneas...
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwOJcsTrMV
JDPtnbKXG56w0Tæ6UQ9HsUBoDQnlsN5ZBHt1VyjAP
—CERTIFICADO FINAL—
.
Certificado importado correctamente
Emitido por: C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation Secure
Server CA
Válido desde: 14 jun 00:00:00 2017 GMT
Válido para: 11 sep 23:59:59 2020 GMT
Asunto: C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx , OU=IT, CN=*.kowi.eu
Huella digital SHA: xxxxxx
```

Conclusión

Ya ha aprendido los pasos para importar correctamente un certificado en los switches de las series Sx350 y Sx550X mediante la GUI y la CLI.