Come importare un certificato sugli switch serie Sx350 e Sx550X

Obiettivo

Questo documento descrive i passaggi per importare un certificato sugli switch serie Sx350 e Sx550X usando l'interfaccia grafica dell'utente (GUI) e l'interfaccia della riga di comando (CLI).

Sommario

Introduzione

Uno dei problemi riscontrati durante l'importazione di un certificato sugli switch Sx350 e Sx550X è che l'***intestazione della chiave*** dell'utente ***è mancante*** e/o ***non è stata in grado di caricare*** gli errori della ***chiave pubblica***. In questo documento verrà illustrato come superare questi errori per importare correttamente un certificato. Un certificato è un documento elettronico che identifica un individuo, un server, una società o un'altra entità e associa tale entità a una chiave pubblica. I certificati vengono utilizzati in una rete per fornire un accesso sicuro. I certificati possono essere autofirmati o firmati digitalmente da un'Autorità di certificazione (CA) esterna. Un certificato autofirmato, come indica il nome, è firmato dal proprio creatore. Le CA gestiscono le richieste di certificati e rilasciano i certificati alle entità partecipanti, ad esempio host, dispositivi di rete o utenti. Un certificato digitale firmato da CA è considerato uno standard del settore e più sicuro.

Dispositivi e versione software interessati

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

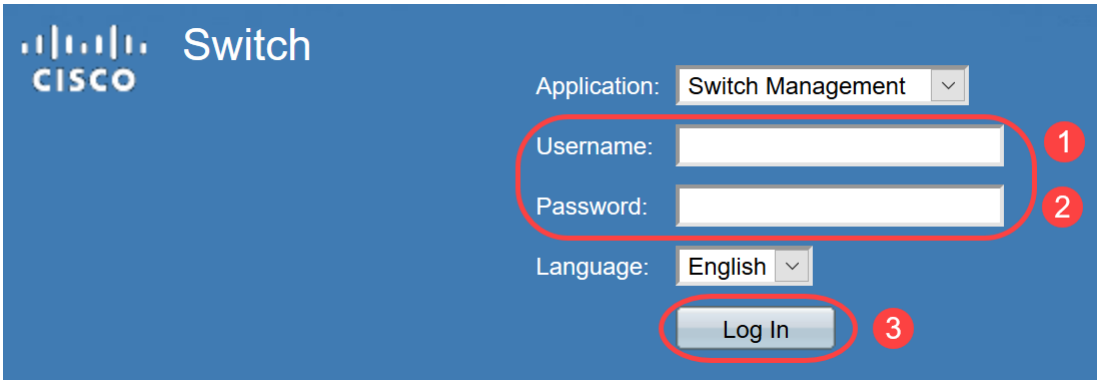
Prerequisiti

Ènecessario disporre di un certificato autofirmato o di un certificato dell'Autorità di certificazione (CA). In questo articolo sono illustrate le procedure per ottenere un certificato autofirmato. Per ulteriori informazioni sui certificati CA, fare clic qui.

Importazione tramite GUI

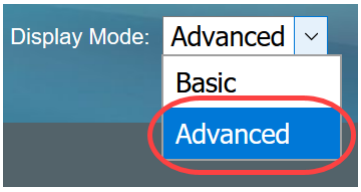
Passaggio 1

Accedere alla GUI dello switch immettendo il *nome utente* e la *password*. Fare clic su **Log In**.



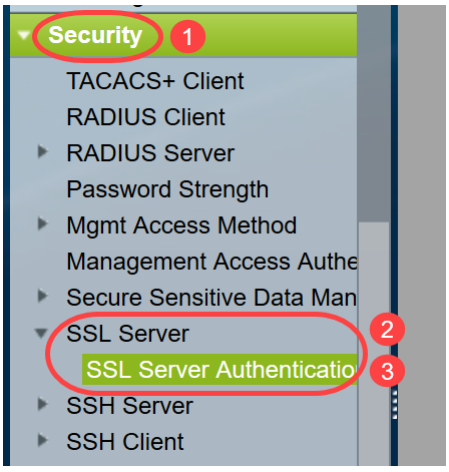
Passaggio 2

Dalla *modalità di visualizzazione* in alto a destra nell'interfaccia utente, scegliere **Advanced** (Avanzate) dall'elenco a discesa.



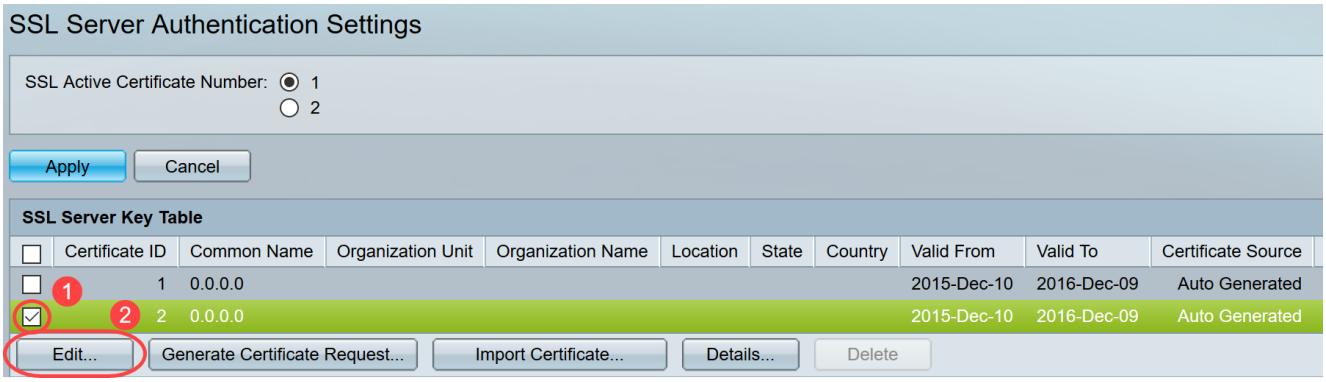
Passaggio 3

Selezionare **Protezione > Server SSL > Autenticazione server SSL**.



Passaggio 4

Selezionare uno dei certificati *generati automaticamente*. Selezionare l'*ID certificato* 1 o 2 e fare clic sul pulsante **Modifica**.



Passaggio 5

Per generare un certificato autofirmato, nella nuova finestra popup abilitare *Regenerate RSA Key* e immettere i seguenti parametri:

Lunghezza chiave

Nome comune

Unità organizzativa

Nome organizzazione

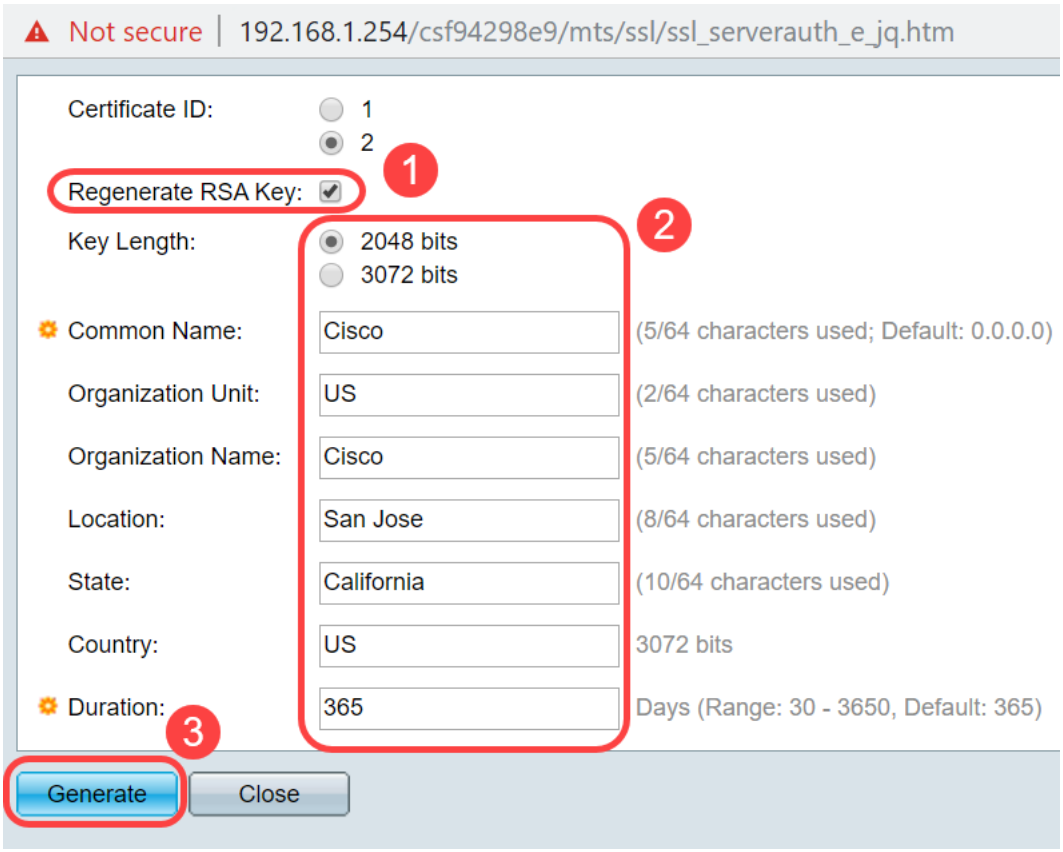
Posizione

State

Paese

Durata

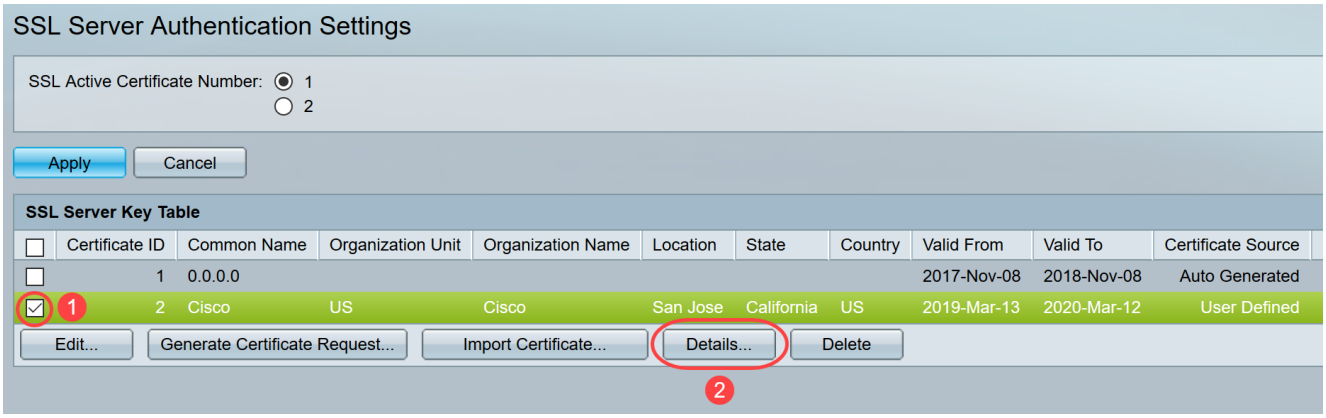
Fare clic su **Genera**.



Èinoltre possibile creare un certificato da una CA di terze parti.

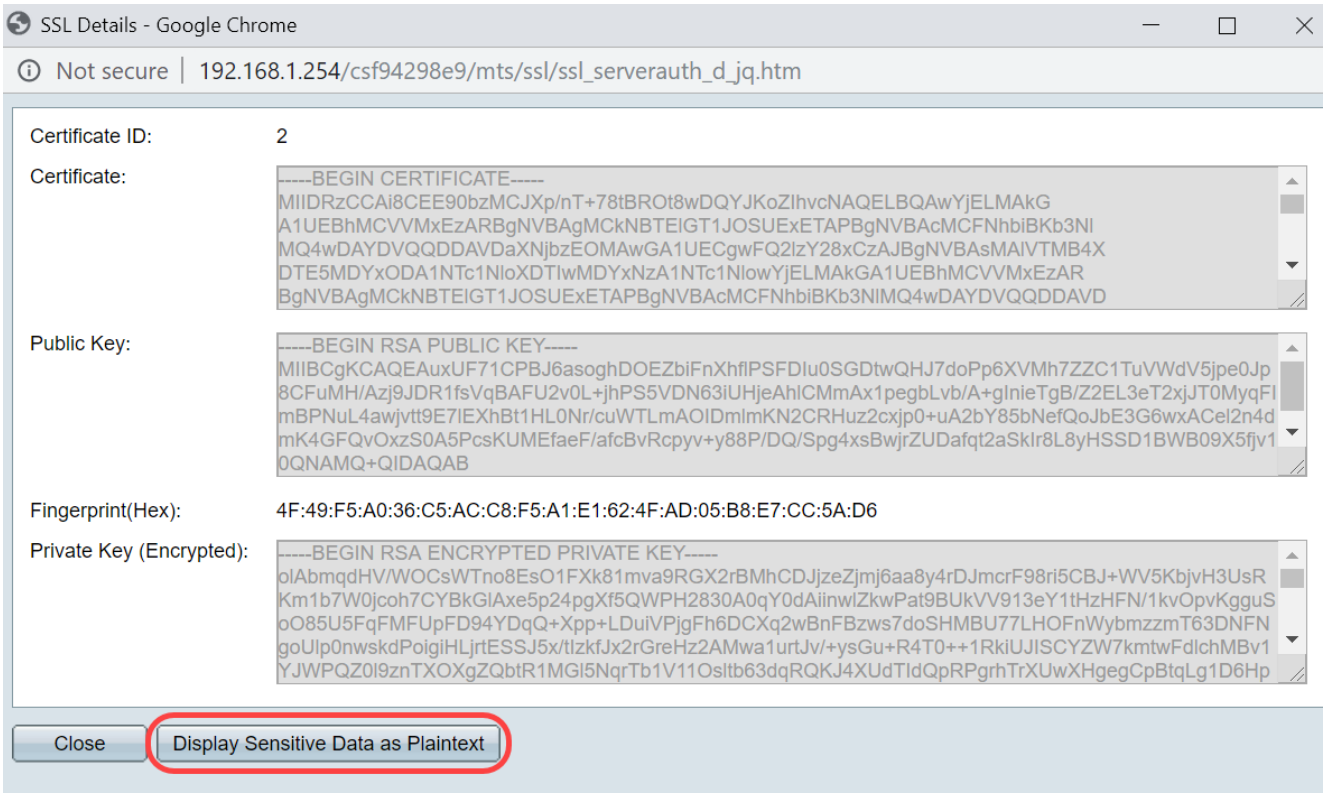
Passaggio 6

A questo punto sarà possibile visualizzare il certificato *definito dall'utente* nella *tabella delle chiavi del server SSL*. Selezionare il certificato appena creato e fare clic su **Dettagli**.



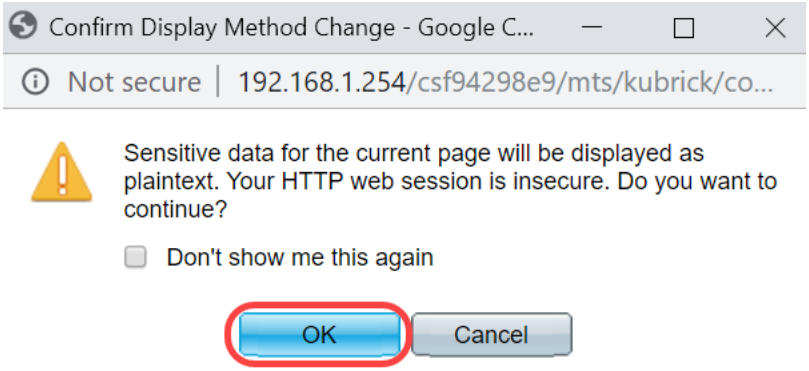
Passaggio 7

Nella finestra popup sarà possibile visualizzare i dettagli *Certificato*, *Chiave pubblica e Chiave privata (crittografata)*. È possibile copiarli in un file del Blocco note separato. Fare clic su **Visualizza dati sensibili come testo normale**.



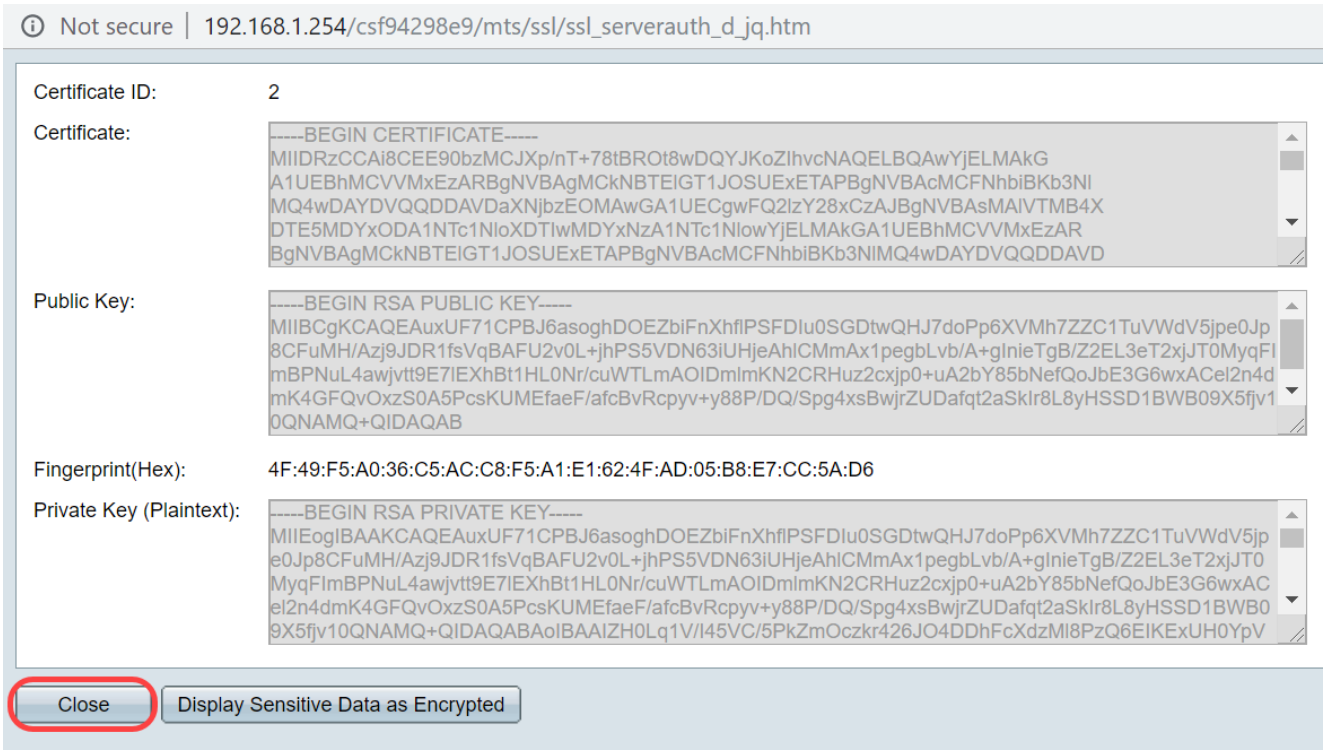
Passaggio 8

Verrà visualizzata una finestra popup per confermare la visualizzazione della chiave privata come testo normale. Fare clic su **OK**.



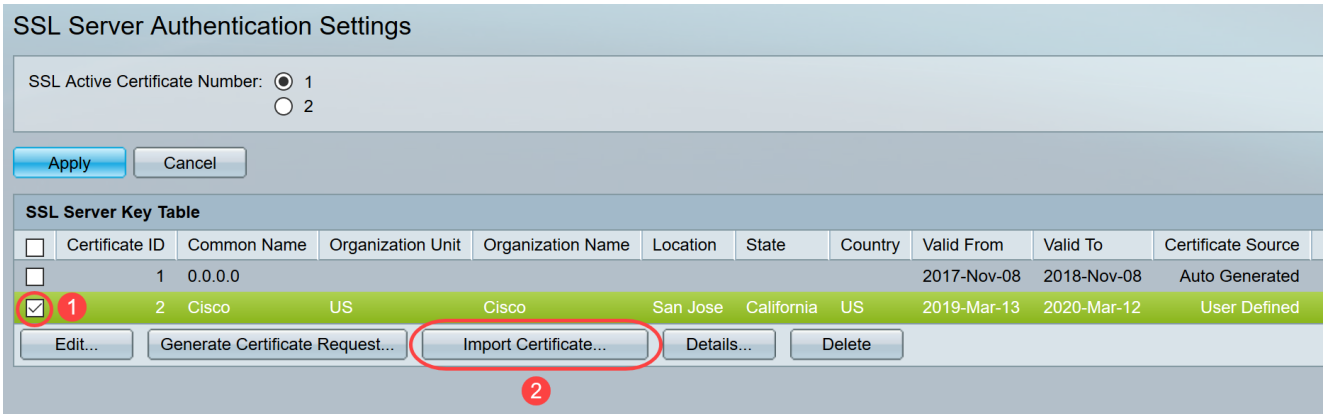
Passaggio 9

Ora sarà possibile visualizzare la *chiave privata* in formato testo normale. Copiare l'output di testo normale in un file del Blocco note. Fare clic su **Close** (Chiudi).



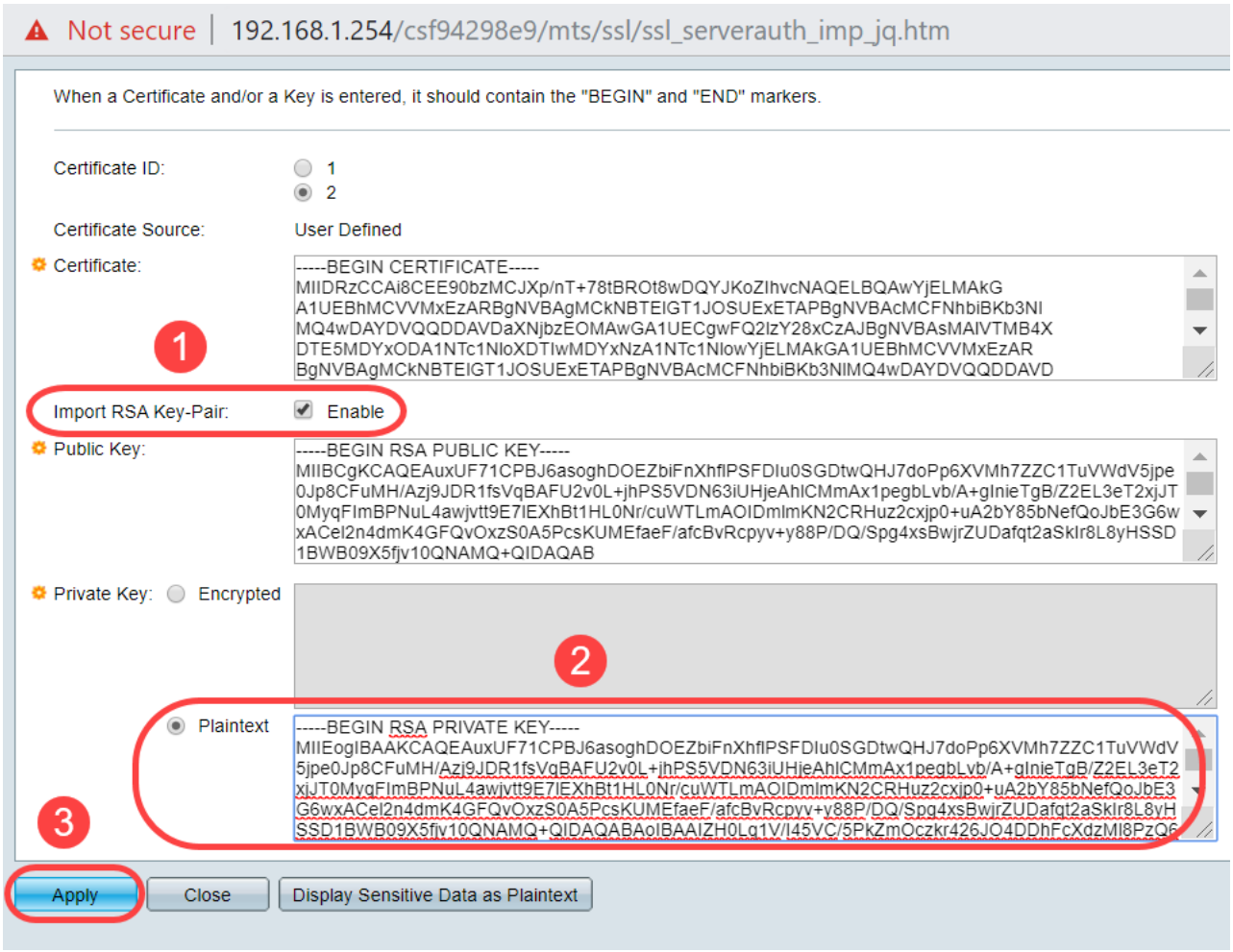
Passaggio 10

Selezionare il nuovo certificato *definito dall'utente* creato e fare clic su **Importa certificato**.



Passaggio 11

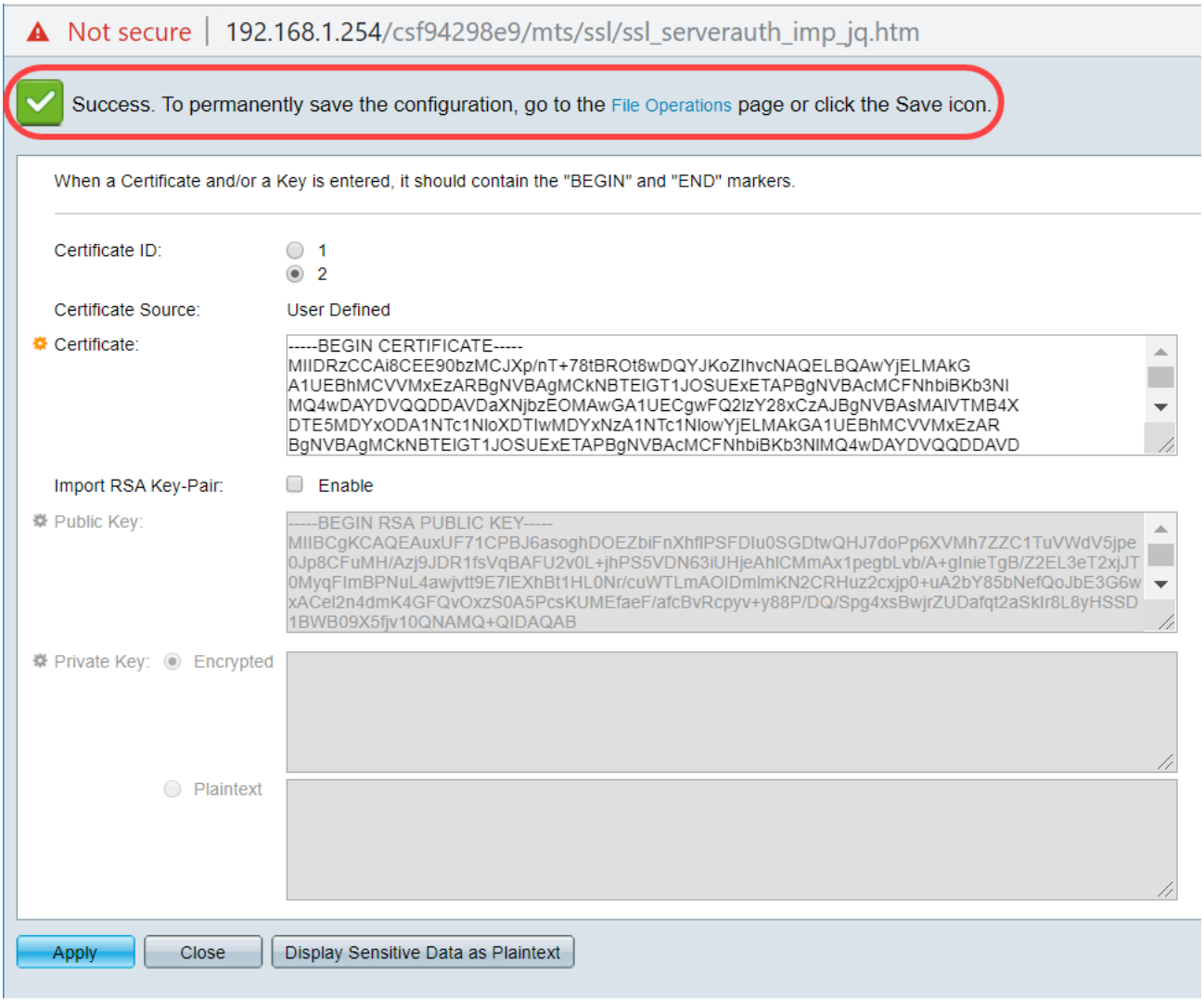
Nella nuova finestra popup, abilitare l'opzione *Import RSA Key-Pair* e incollare la chiave privata (copiata al passaggio 9) in formato testo normale. Fare clic su **Apply** (Applica).



Nell'esempio, la parola chiave *RSA* viene inclusa in *BEGIN* e *END* della *chiave pubblica*.

Passaggio 12

Sullo schermo verrà visualizzata la notifica di esito positivo. È possibile chiudere questa finestra e salvare la configurazione sullo switch.



Errori possibili

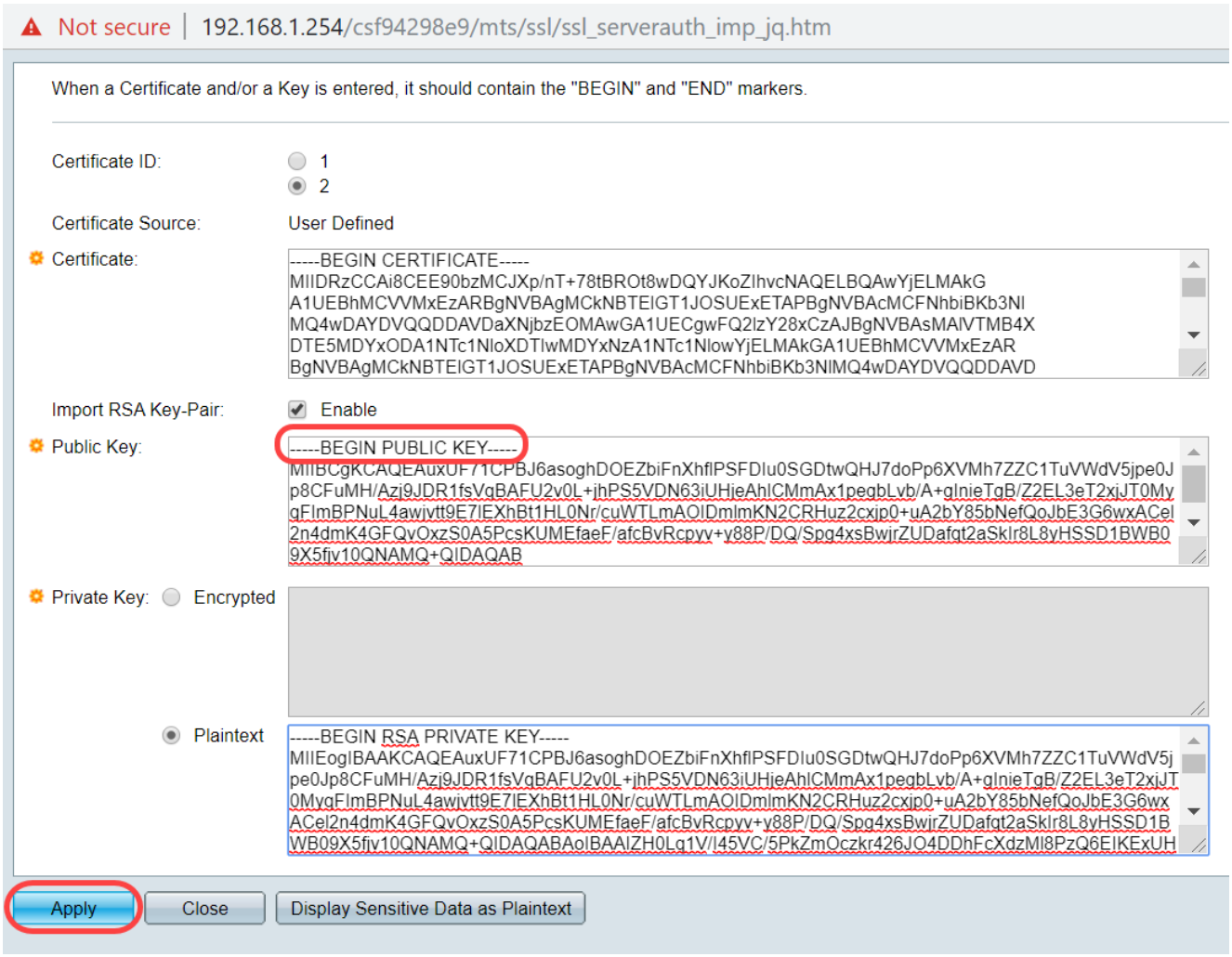
Gli errori discussi riguardano la chiave pubblica. In genere vengono utilizzati due tipi di formati di chiave pubblica:

1. File di chiave pubblica RSA (PKCS#1): È specifico per le chiavi RSA.
Inizia e termina con i tag:
—INIZIO CHIAVE PUBBLICA RSA—
DATI CODIFICATI BASE64
—END RSA PUBLIC KEY—

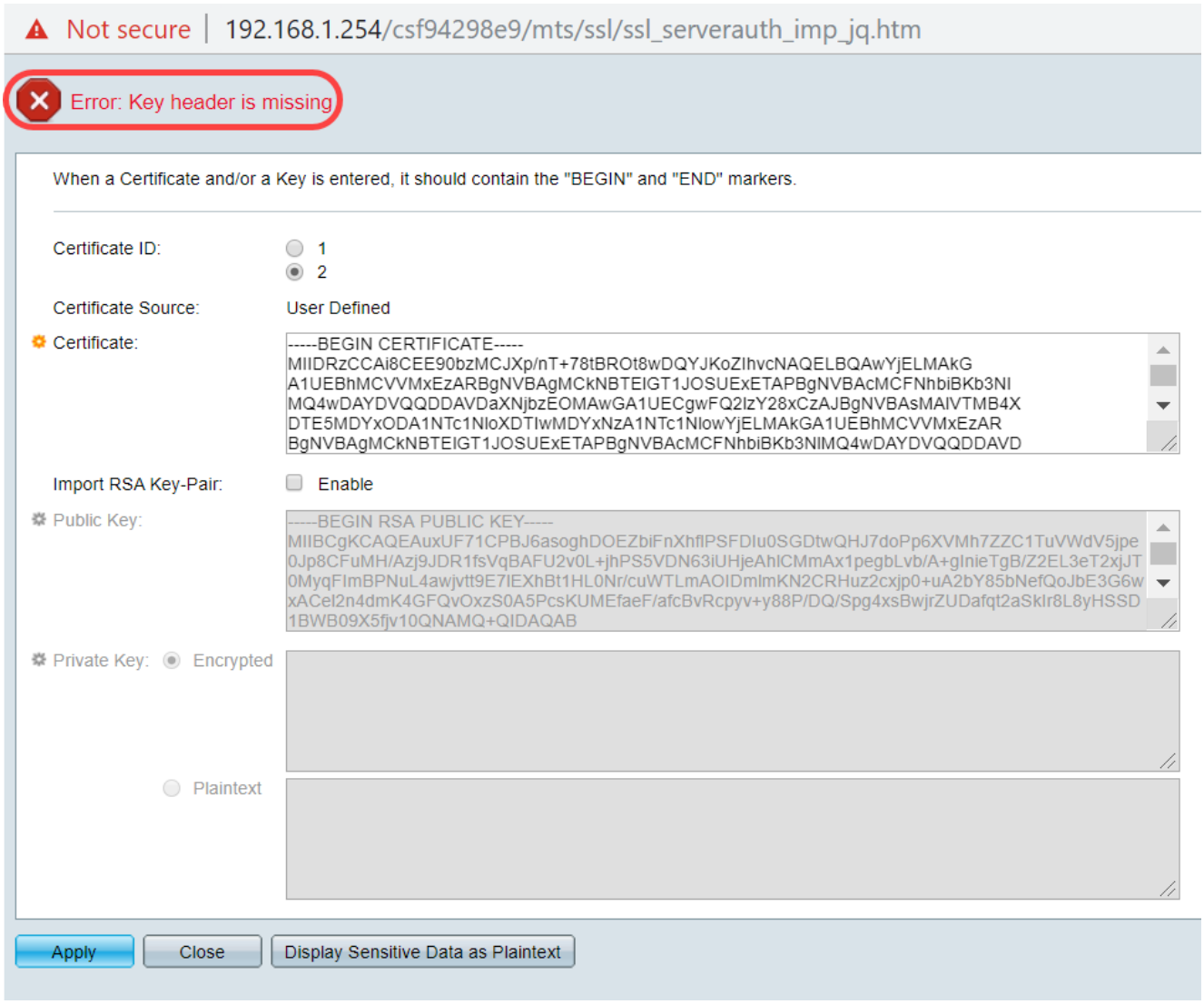
2. File di chiave pubblica (PKCS#8): Si tratta di un formato di chiave più generico che identifica il tipo di chiave pubblica e contiene i dati rilevanti.
Inizia e termina con i tag:
—INIZIA CHIAVE PUBBLICA—
DATI CODIFICATI BASE64
—END PUBLIC KEY—

Intestazione chiave mancante

Scenario 1: Il certificato è stato generato da una CA di terze parti. La chiave pubblica è stata copiata e incollata e si è fatto clic su **Applica**.



Èstato visualizzato il messaggio *Errore: Intestazione chiave mancante*. Chiudete la finestra. È possibile apportare alcune modifiche per eliminare questo problema.



Per correggere l'errore:

Aggiungere la parola chiave *RSA* all'inizio della chiave pubblica: *INIZIO CHIAVE PUBBLICA RSA*

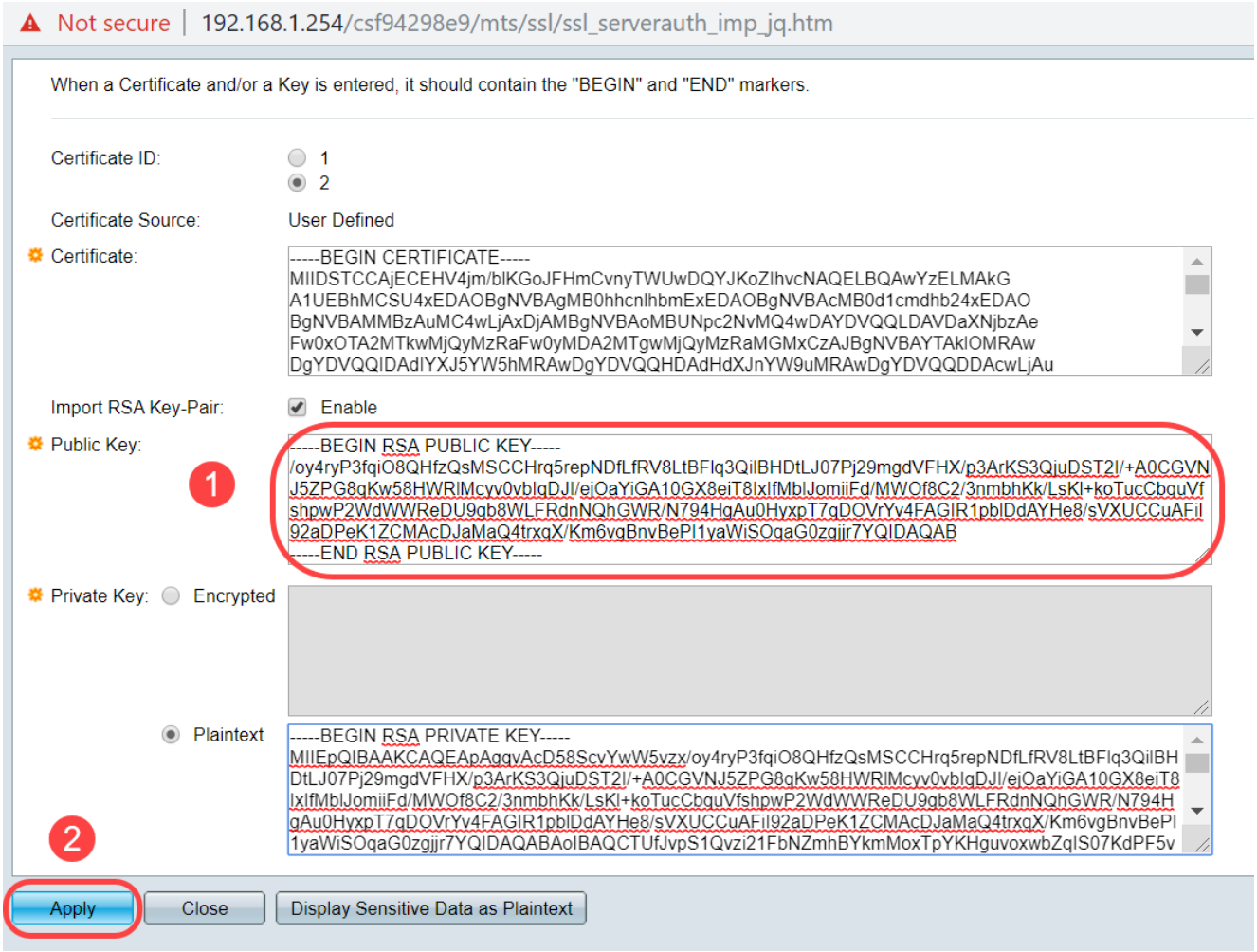
Aggiungere la parola chiave *RSA* alla fine della chiave pubblica: *FINE CHIAVE PUBBLICA RSA*

Rimuovere i primi 32 caratteri dal codice del tasto. La parte evidenziata mostrata di seguito è un esempio dei primi 32 caratteri.

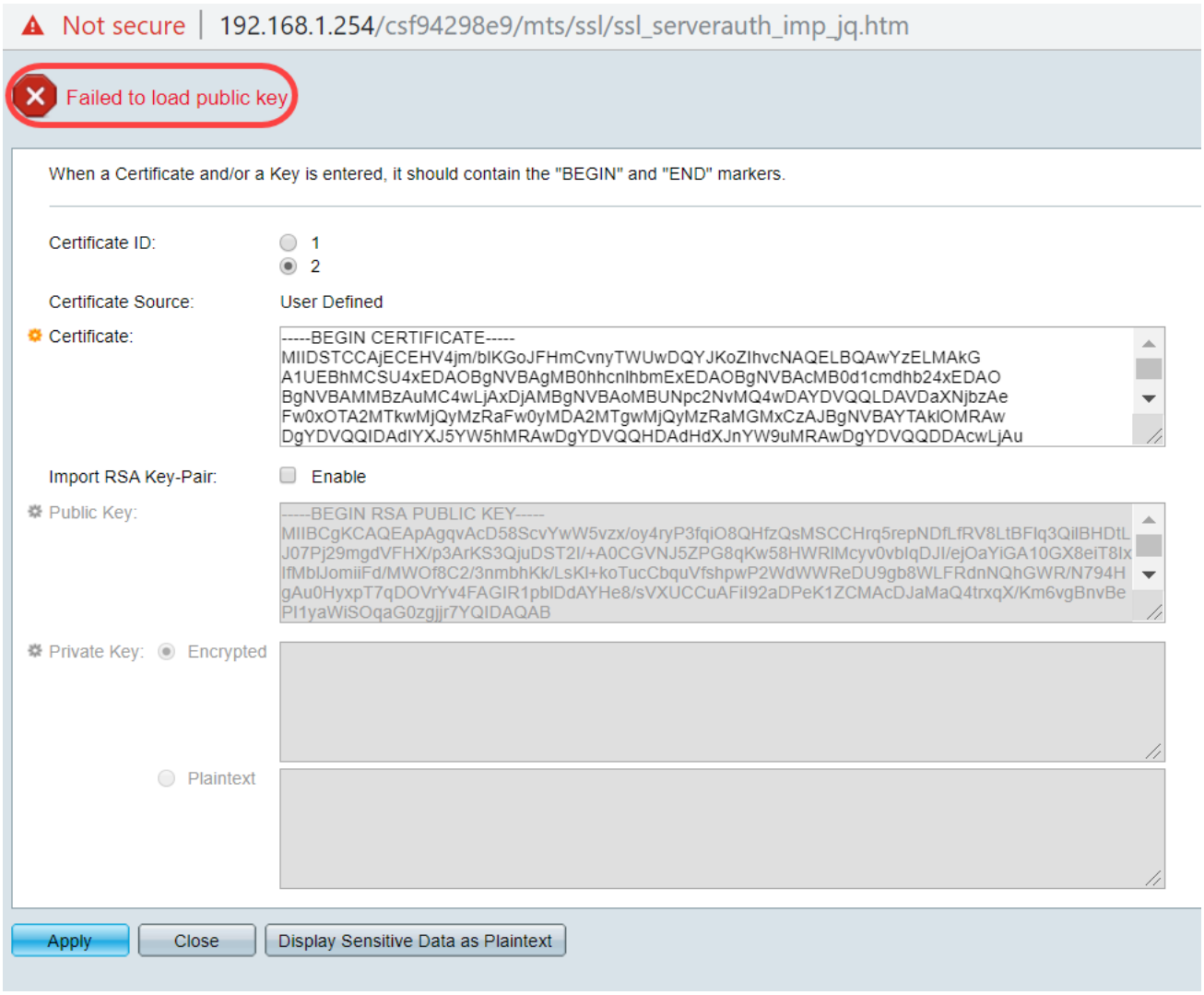
Quando si applicano le impostazioni, nella maggior parte dei casi l'*intestazione Chiave mancante* non viene visualizzata.

Impossibile caricare errore di chiave pubblica

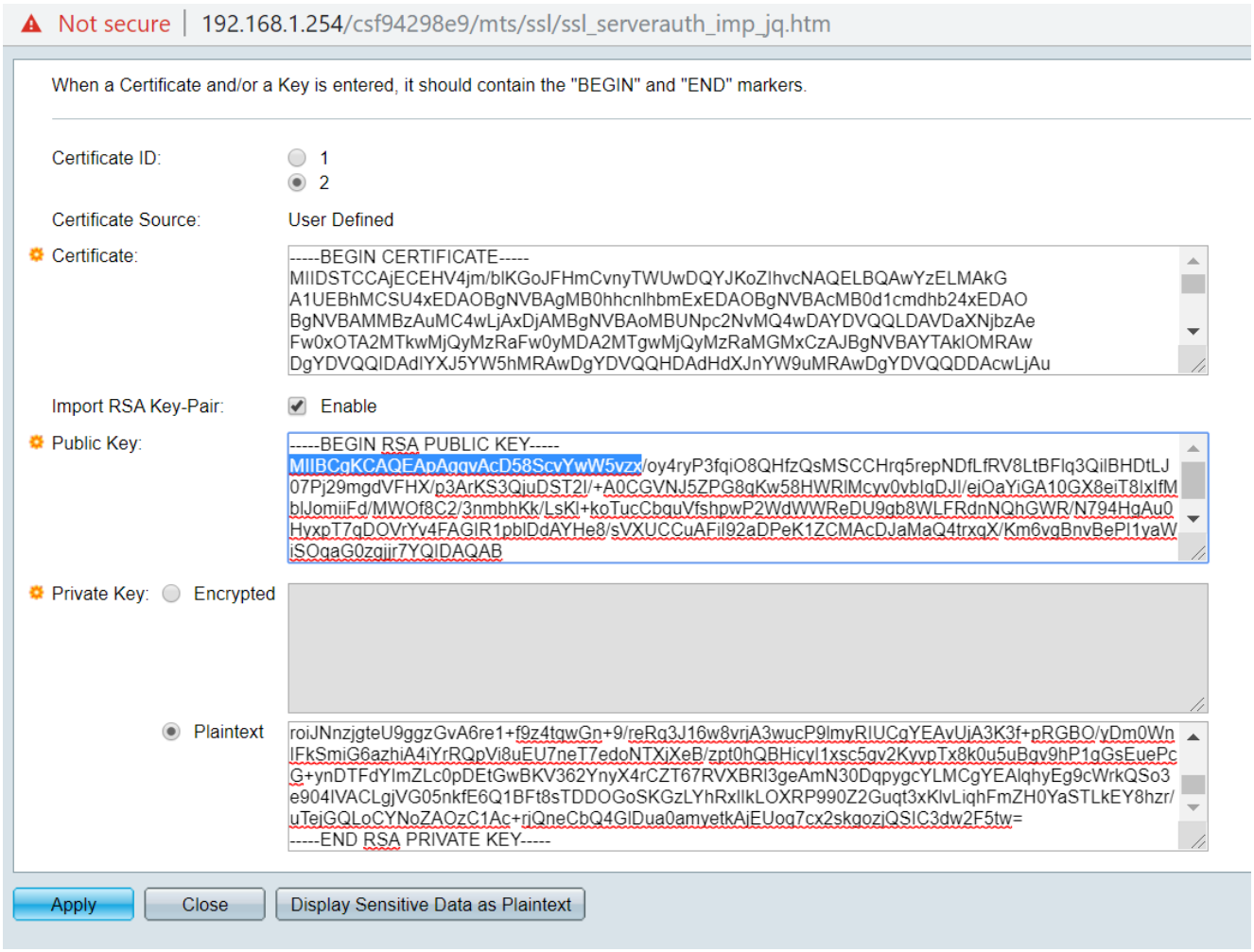
Scenario 2: Il certificato è stato generato su uno switch e importato su un altro switch. La chiave pubblica è stata copiata e incollata dopo aver rimosso i primi 32 caratteri e aver fatto clic su **Applica**.



Èstato visualizzato il messaggio di errore *Impossibile caricare la chiave pubblica*.



Per correggere l'errore, NON eliminare i primi 32 caratteri della chiave pubblica in questo caso.



Importazione tramite CLI

Passaggio 1

Per importare il certificato tramite CLI, immettere il comando seguente.

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

In questo esempio viene importato il certificato 2.

```
switch(config)#importazione certificato crittografico 2
```

Passaggio 2

Incollare l'input; **aggiungere un punto (.)** su una riga separata dopo l'input.

```
—INIZIO CHIAVE PRIVATA RSA—
MIIEvgIBADANBgkqkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...24 linee troncate....
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
—END RSA PRIVATE KEY—
—INIZIO CHIAVE PUBBLICA RSA—
MIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfT0l
...troncato di 3 righe....
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
—END RSA PUBLIC KEY—
—BEGIN CERTIFICATE—
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
- 28 linee troncate...
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwOJcsTrMV
JDPtnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBHt1VyjAP
—END CERTIFICATE—
.
Importazione del certificato completata
Rilasciato da: C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Convalida organizzazione CA
Secure Server
Valido da: 14 giu 00:00:00 2017 GMT
Valido fino al: 11 set 23:59:59 2020 GMT
Oggetto: C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx , OU=IT, CN=*.kowi.eu
Impronta digitale SHA: xxxxxx
```

Conclusioni

A questo punto, è possibile importare un certificato sugli switch serie Sx350 e Sx550X dalla GUI e dalla CLI.