Modifica delle impostazioni di autenticazione server Secure Sockets Layer (SSL) sugli switch impilabili serie Sx500

Obiettivo

SSL (Secure Sockets Layer) è un protocollo utilizzato principalmente per la gestione della sicurezza su Internet. Utilizza un livello di programma situato tra i livelli HTTP e TCP. Per l'autenticazione, SSL utilizza certificati con firma digitale e associati alla chiave pubblica per identificare il proprietario della chiave privata. Questa autenticazione consente di controllare l'operatività durante la connessione. Tramite SSL, i certificati vengono scambiati in blocchi durante il processo di autenticazione nel formato descritto nello standard ITU-T X.509. Successivamente, vengono rilasciati certificati X.509 firmati digitalmente dall'autorità di certificazione che è un'autorità esterna.

In questo documento viene spiegato come modificare le impostazioni di autenticazione del server SSL e come generare una richiesta di certificato sugli switch impilabili serie Sx500.

Dispositivi interessati

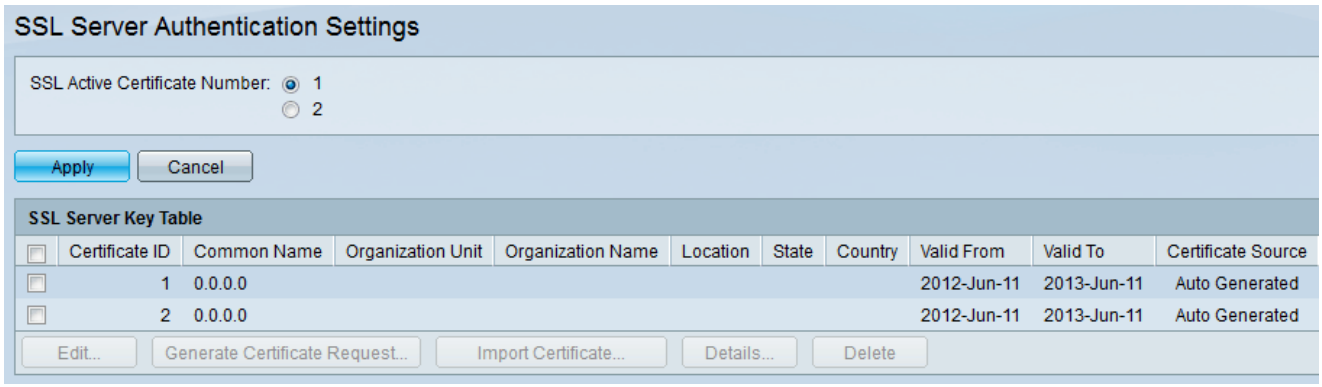
·Switch Stack Serie Sx500

Versione del software

•1.3.0.62

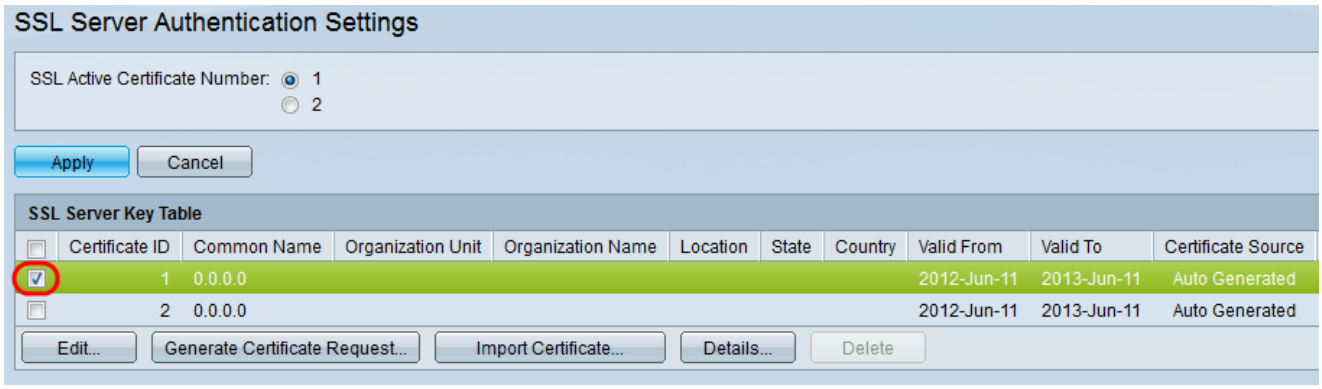
Impostazioni autenticazione server SSL

Passaggio 1. Accedere all'utility di configurazione dello switch e scegliere **Sicurezza > Server SSL > Impostazioni di autenticazione server SSL. Viene** visualizzata la pagina *Impostazioni autenticazione server SSL*:

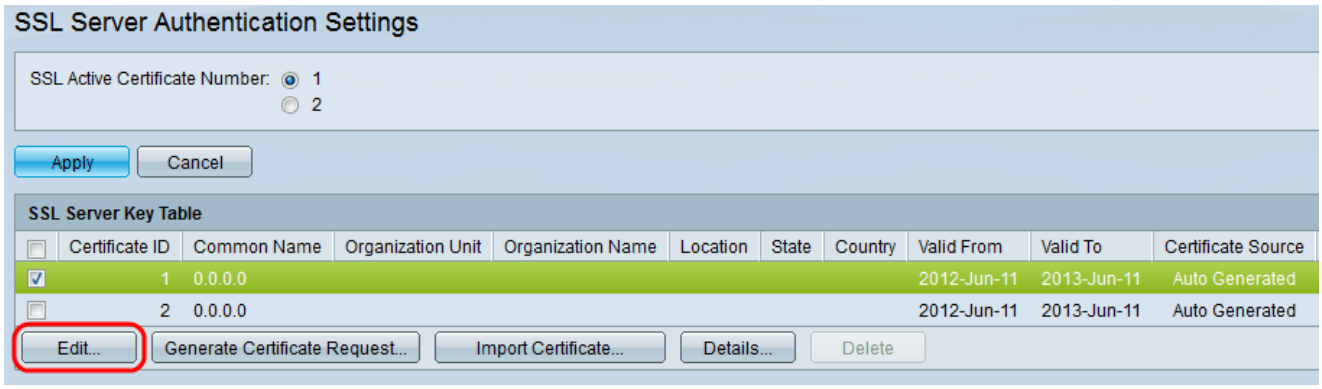


Nota: Seguire le istruzioni Modifica informazioni chiave SSL per generare il certificato automaticamente, Genera richiesta certificato per generare nuovamente la richiesta di certificato da parte dello switch e Importa certificato per importare il certificato desiderato e la chiave.

Modifica informazioni chiave SSL

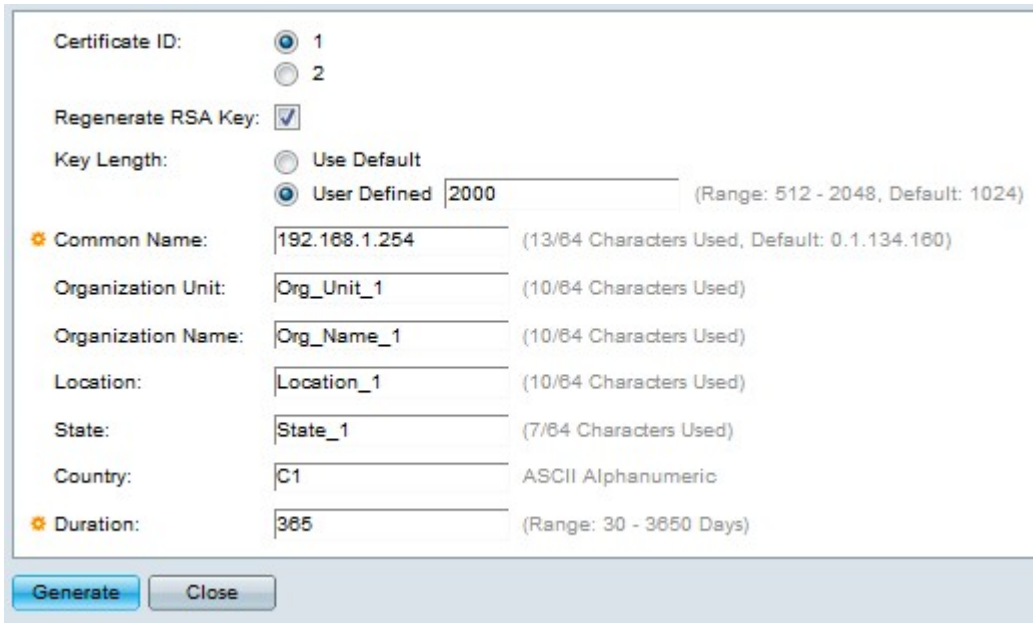


Passaggio 2. Selezionare la casella di controllo del certificato attivo che si desidera modificare nella tabella delle chiavi del server SSL.



Passaggio 3. Fare clic su **Modifica** per apportare le modifiche al certificato esistente. Viene visualizzata la finestra *Modifica certificato*:

Nota: In questo esempio, il certificato 1 è selezionato.



Passaggio 4. Nel campo ID certificato scegliere 1 o 2 come ID del certificato. In questa configurazione sono disponibili solo due opzioni nel campo ID certificato.

Passaggio 5. Selezionare la casella di controllo nel campo Rigenera chiave RSA per rigenerare la chiave RSA.

Passaggio 6. Nel campo Lunghezza chiave, fare clic su uno dei pulsanti di opzione.

·Usa default - Viene utilizzata la lunghezza di default della chiave.

·Definita dall'utente: in questo campo, la lunghezza della chiave può essere compresa tra 512 e 2048. Il valore predefinito è 1024. Nell'esempio, viene immesso 2000.

Passaggio 7. Nel campo Nome comune, immettere l'URL completo del dispositivo o l'indirizzo IP pubblico specifico. Se lasciato vuoto, per impostazione predefinita viene utilizzato l'indirizzo IP più basso del dispositivo (quando viene generato il certificato). Nell'esempio, l'indirizzo predefinito dello switch SG500X viene usato come nome comune.

Passo 8: nel campo Unità organizzazione inserire il nome dell'organizzazione-unità o del reparto.

Passaggio 9. Nel campo Nome organizzazione, inserire il nome dell'organizzazione.

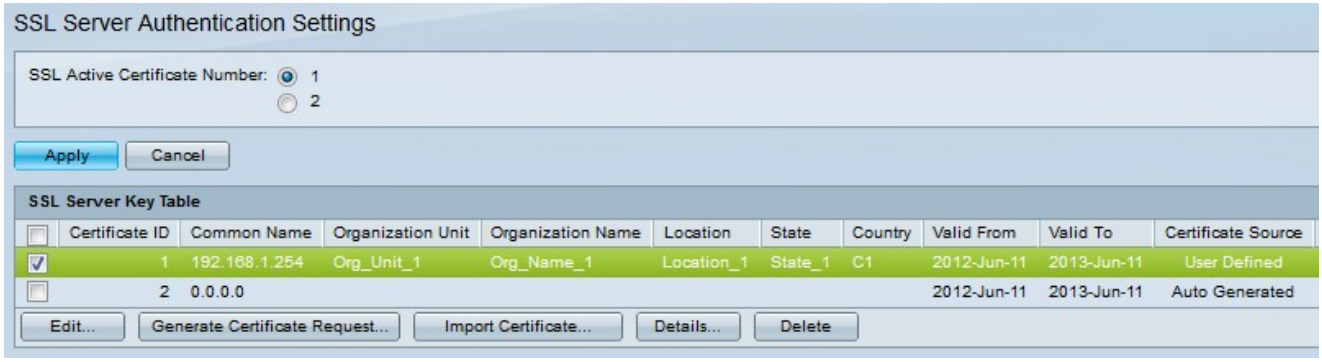
Passaggio 10. Nel campo Ubicazione, inserire il nome dell'ubicazione o della città.

Passaggio 11. Nel campo Stato, immettere il nome dello stato o della provincia.

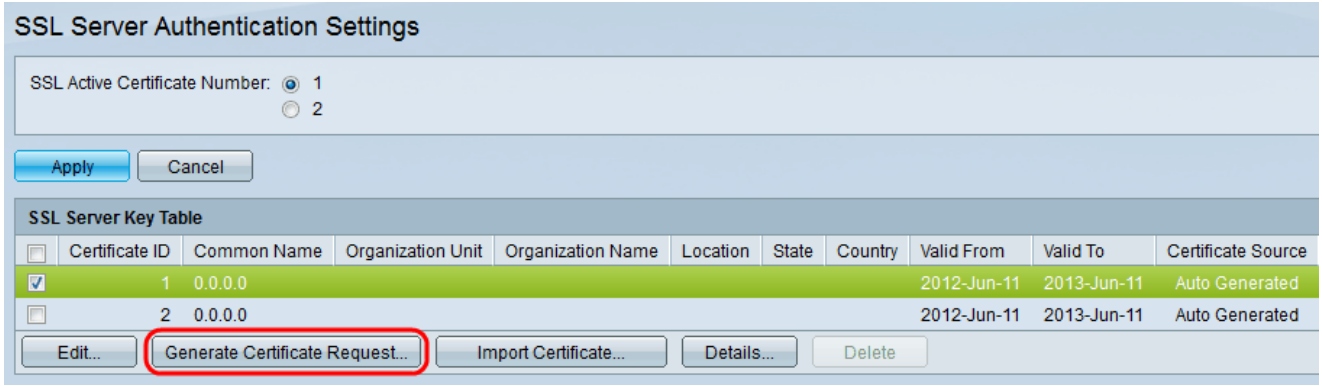
Passaggio 12. Nel campo Paese, inserire il nome del paese. Poiché questa opzione accetta solo valori alfanumerici, utilizzare il formato globale a 2 lettere. Ad esempio, per gli Stati Uniti immettere US.

Passaggio 13. Nel campo Durata immettere il numero di giorni di validità di una certificazione.

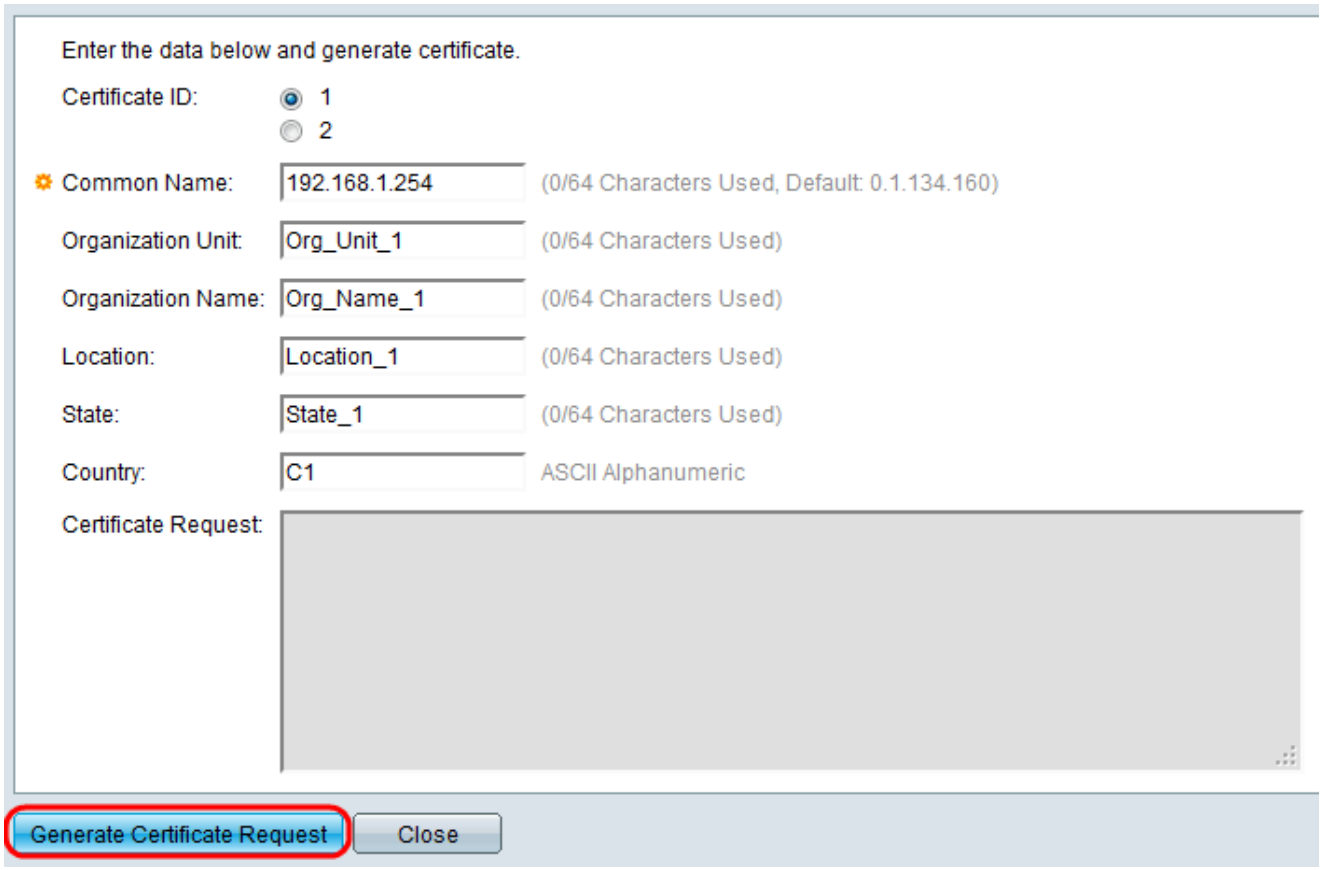
Passaggio 14. Fare clic su **Genera** per salvare le impostazioni.



Genera una richiesta di certificato



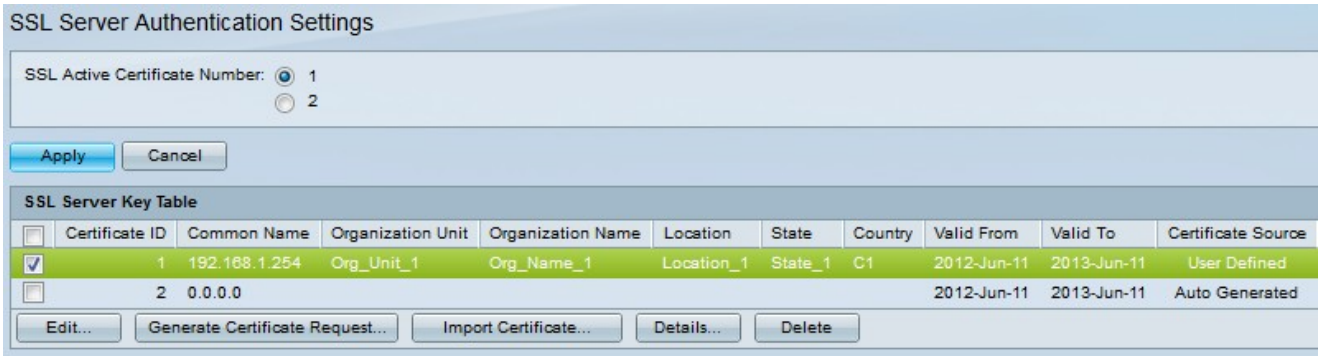
Passaggio 1. Nella pagina *Impostazioni autenticazione server SSL*, controllare l'ID certificato e fare clic su **Genera richiesta certificato**.



Passaggio 2. Fare clic su **Genera richiesta certificato** nella pagina *Modifica impostazioni di autenticazione server SSL*.

Nel campo Richiesta certificato è ora possibile visualizzare le informazioni sul certificato crittografato.

Passaggio 3. Fare clic su **Genera richiesta certificato** per salvare le impostazioni.



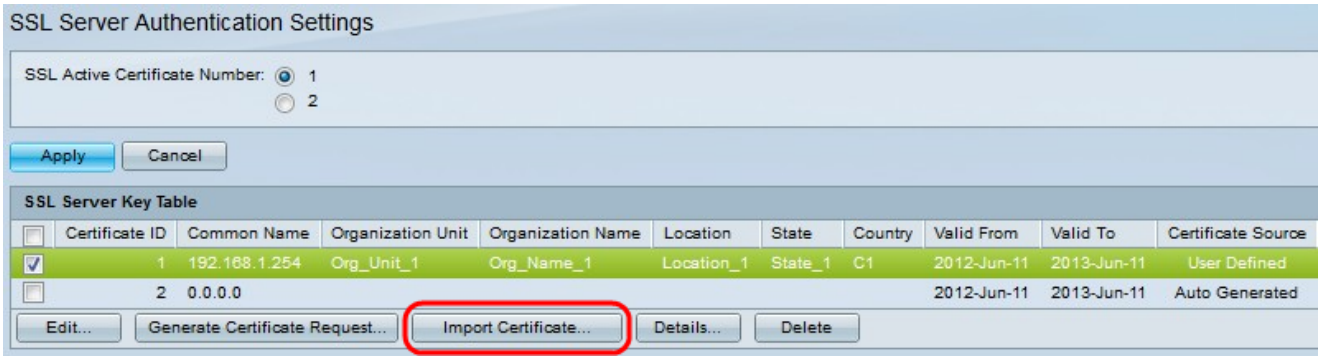
A questo punto, nella pagina *Impostazioni autenticazione server SSL* è possibile visualizzare il certificato modificato con tutte le informazioni immesse in precedenza.

·Valido - Specifica la data a partire dalla quale il certificato è valido.

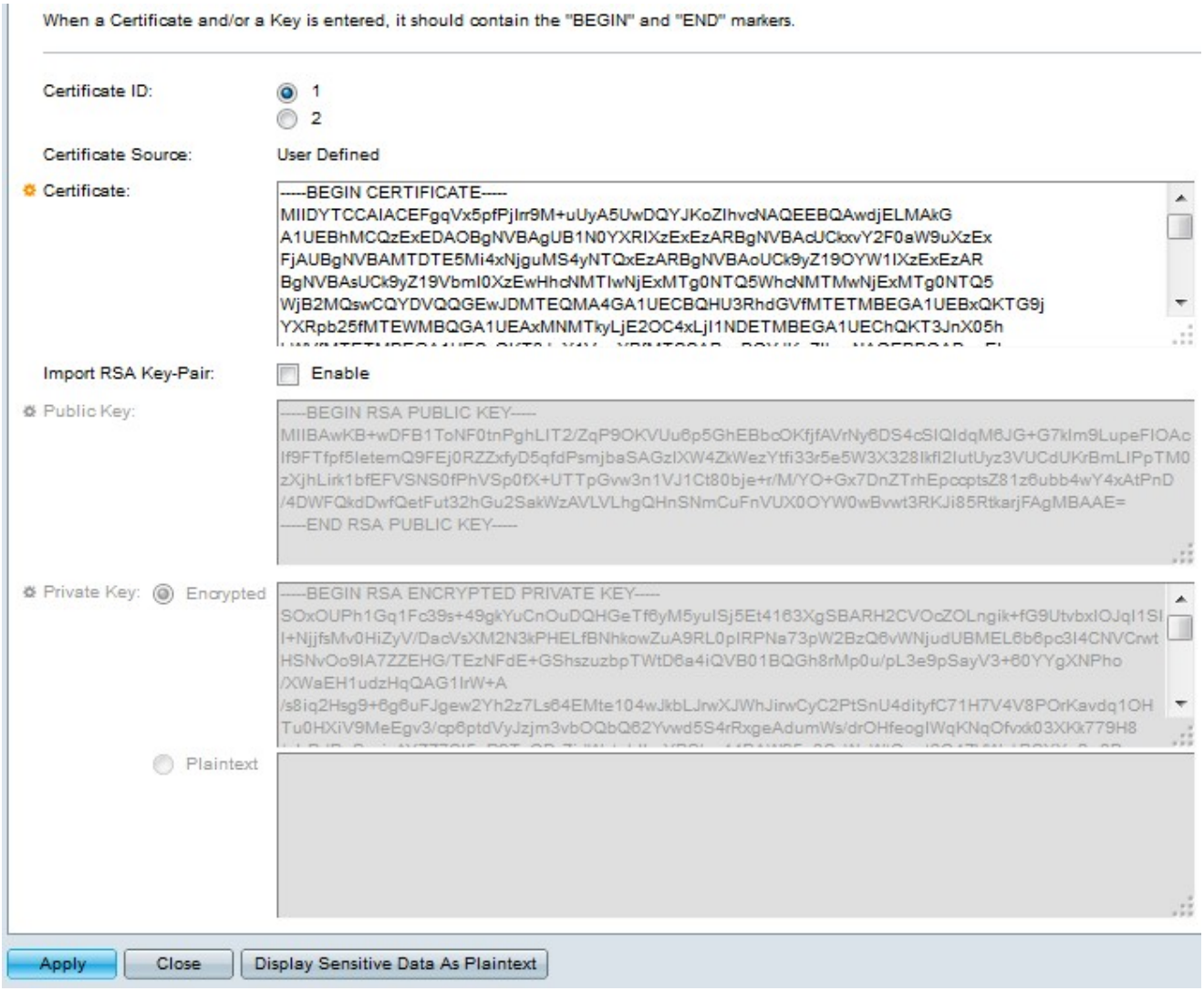
·Valido fino a - Specifica la data fino alla quale il certificato è valido.

·Origine certificato — specifica se il certificato è stato generato dal sistema (generato automaticamente) o dall'utente (definito dall'utente).

Importa certificato



Passaggio 1. Selezionare la casella di controllo desiderata e fare clic su **Importa certificato** per importare un certificato.



·ID certificato — Scegliere il certificato attivo

·Certificato — Copia o incolla il certificato in un file configurato.

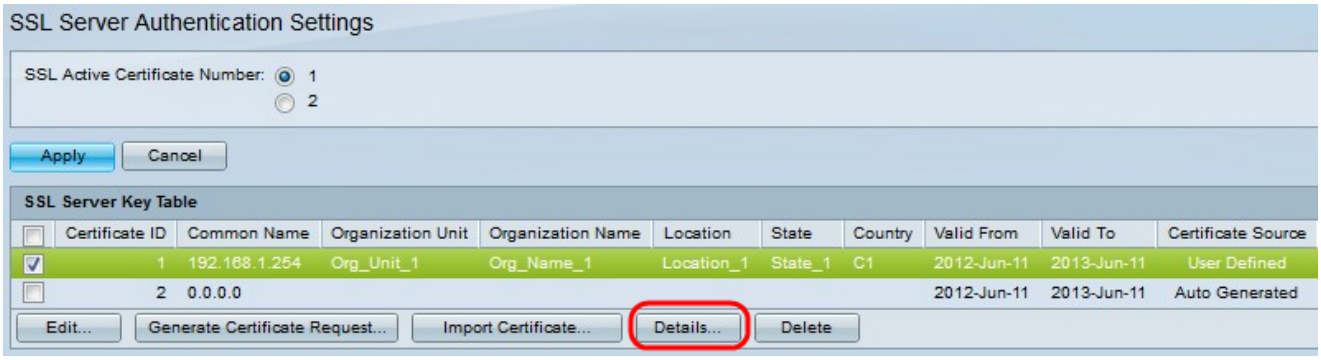
·Importa coppia di chiavi RSS: scegliere se abilitare la coppia di chiavi RSA.

·Chiave pubblica (crittografata) — Copia o incolla la chiave pubblica in forma crittografata.

·Chiave privata (testo normale) — Copia o incolla la chiave privata in formato testo normale.

·Visualizza dati sensibili come crittografati: scegliere questa opzione se si desidera che le chiavi private vengano scritte in forma crittografata nel file di configurazione.

Passaggio 2. Fare clic su **Applica**.



Passaggio 3. (Facoltativo) Fare clic sull'ID certificato desiderato e fare clic su **Dettagli** per visualizzare i dettagli SSL.

Passaggio 4. (Facoltativo) Fare clic sull'ID certificato desiderato e fare clic su **Elimina** per eliminare i dettagli del server SSL dalla tabella del server SSL.