Autenticazione utente Client Secure Shell (SSH) per gli switch SG350XG e SG550XG

Obiettivo

Secure Shell (SSH) è un protocollo che permette di connettersi in modo sicuro a un dispositivo specifico. Gli switch gestiti serie 350XG e 550XG consentono di autenticare e gestire gli utenti per la connessione al dispositivo tramite SSH. L'autenticazione viene effettuata tramite una chiave pubblica, quindi l'utente può utilizzare questa chiave per stabilire una connessione SSH a un dispositivo specifico. Le connessioni SSH sono utili per risolvere i problemi di una rete in remoto, nel caso in cui l'amministratore di rete non si trovi nel sito di rete.

In questo documento viene spiegato come configurare l'autenticazione dell'utente client sugli switch gestiti serie SG350XG e SG550XG.

Dispositivi interessati

- SG350XG
- SG550XG

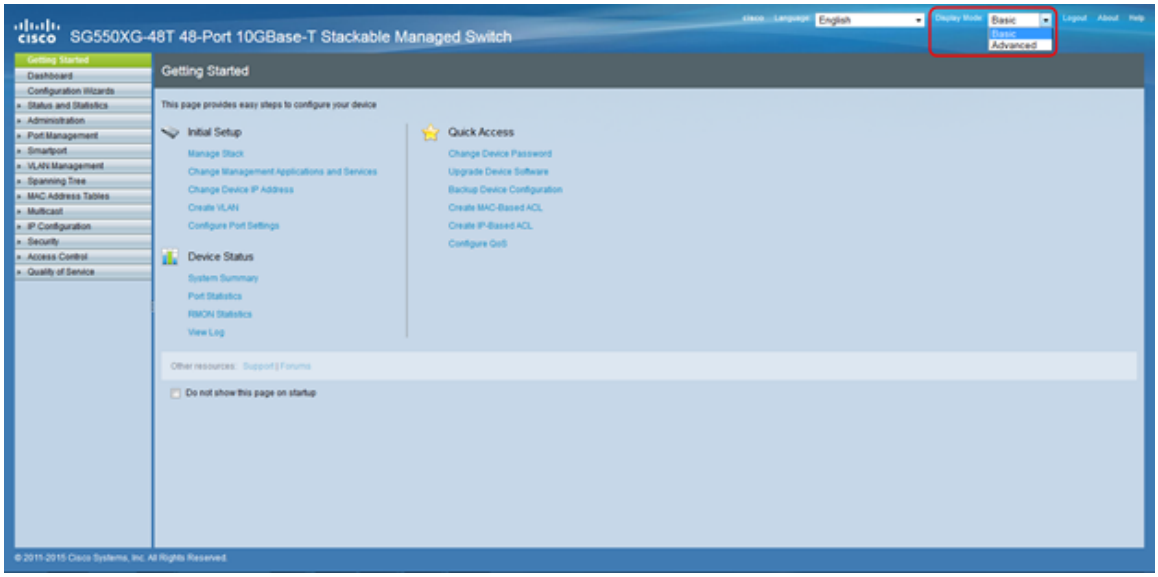
Versione del software

- v2.0.0.73

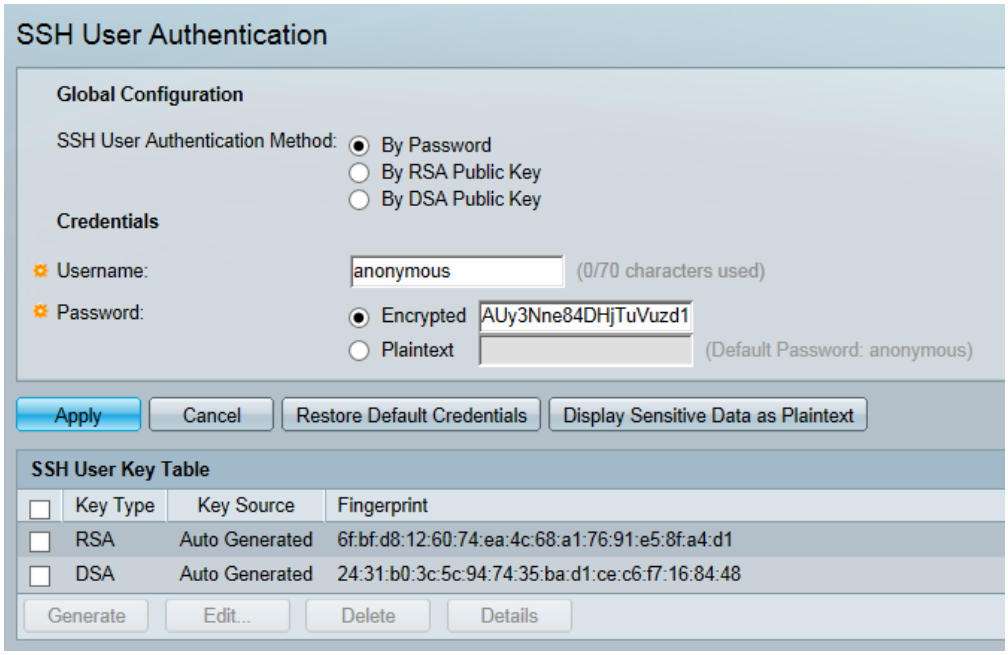
Configurazione del protocollo SSH Cliente Autenticazione

Configurazione globale

Nota: Le seguenti schermate sono tratte da Advanced Display. È possibile alternare la visualizzazione facendo clic sull'elenco a discesa *Display Mode (Modalità di visualizzazione)* nella parte superiore destra dello schermo



Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Security > SSH Client > SSH User Authentication**. Viene visualizzata la pagina *SSH User Authentication*:



Passaggio 2. Nel campo *Metodo di autenticazione utente SSH*, fare clic sul pulsante di opzione corrispondente al metodo di autenticazione globale desiderato.

Le opzioni disponibili sono le seguenti:

- Per password: questa opzione consente di configurare una password per l'autenticazione utente. Immettere una password o mantenere l'impostazione predefinita "anonimo".
- Per chiave pubblica RSA: questa opzione consente di utilizzare una chiave pubblica RSA per l'autenticazione dell'utente. RSA viene utilizzato per la crittografia e la firma. Se questa opzione è selezionata, creare una chiave pubblica e privata RSA nel blocco della tabella della chiave utente SSH.
- Per chiave pubblica DSA: questa opzione consente di utilizzare una chiave pubblica DSA per l'autenticazione utente. DSA viene utilizzato solo per la firma. Se questa opzione è selezionata, creare una chiave DSA pubblica/privata nel blocco della tabella della chiave utente SSH.

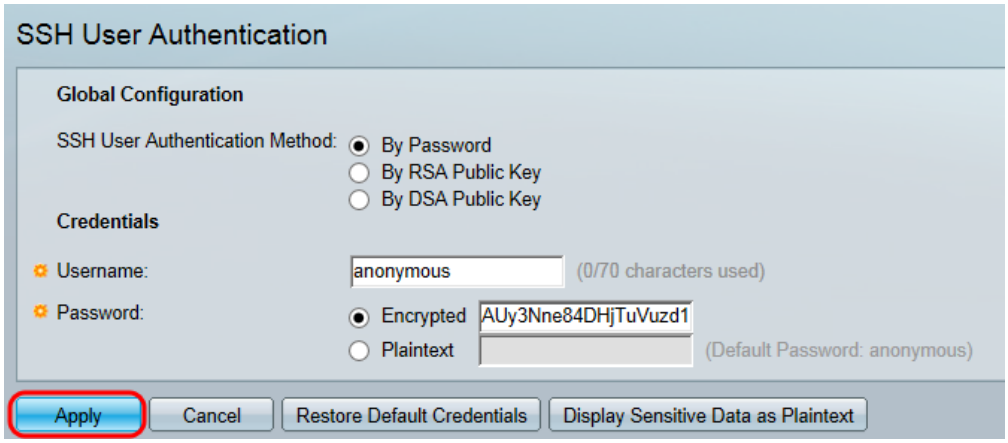
Passaggio 3. Individuare l'area *Credenziali*. Nel campo *Username* (Nome utente), immettere il nome utente.

Passaggio 4. Se nel Passaggio 2 è stata selezionata l'opzione **Per password**, fare clic sul pulsante di opzione relativo al metodo di password desiderato nel campo *Password*. La password predefinita è "anonimo".

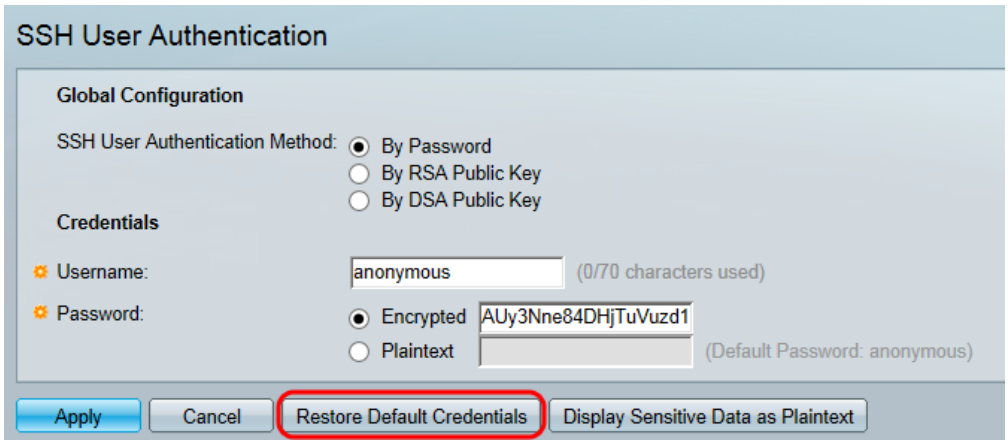
Le opzioni disponibili sono descritte come segue:

- Encrypted - Immettere una password crittografata.
- Testo normale - Immettere una password come testo normale.

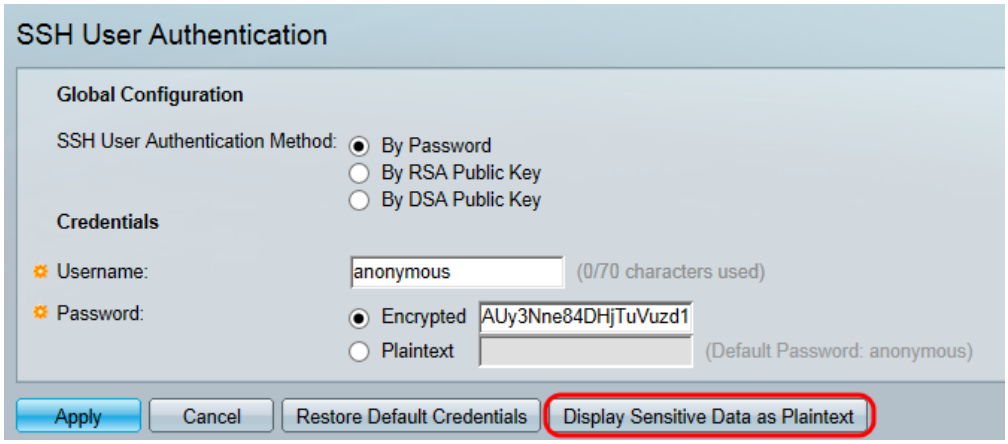
Passaggio 5. Fare clic su **Apply** (Applica) per salvare la configurazione dell'autenticazione.



Passaggio 6. (Facoltativo) Per ripristinare il nome utente e la password predefiniti, fare clic su **Ripristina credenziali predefinite**. La password predefinita è "anonima".



Passaggio 7. (Facoltativo) Per visualizzare i dati sensibili come testo normale o crittografato, fare clic su **Visualizza dati sensibili come testo normale/crittografato.**

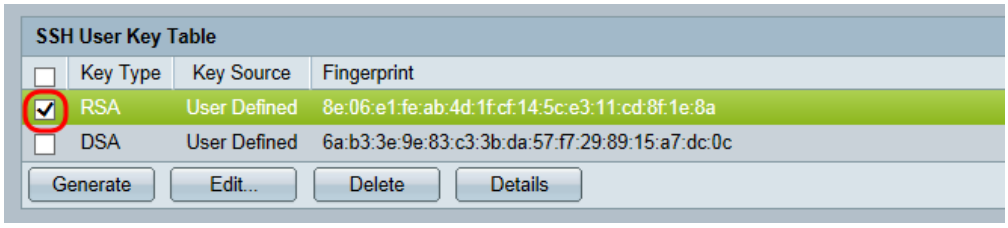


Nota: Il nome del pulsante cambia a seconda dell'impostazione corrente. Il pulsante consente di attivare e disattivare sempre la visualizzazione dei dati.

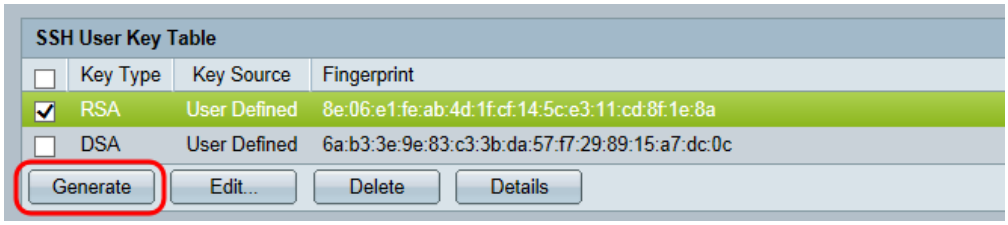
Tabella chiavi utente SSH

Questa sezione spiega come gestire la tabella utenti SSH.

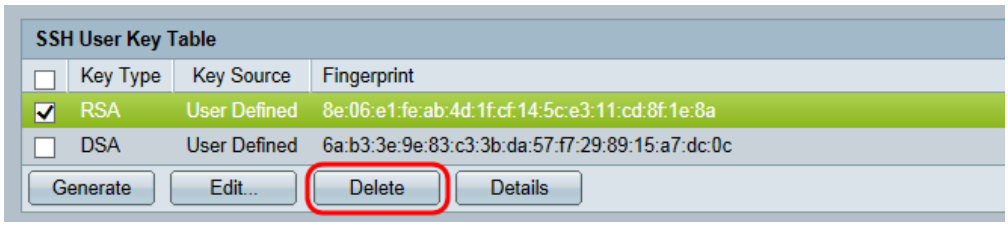
Passaggio 1. Passare alla *tabella della chiave utente SSH*. Nell'elenco visualizzato selezionare le caselle di controllo a sinistra della chiave che si desidera gestire.



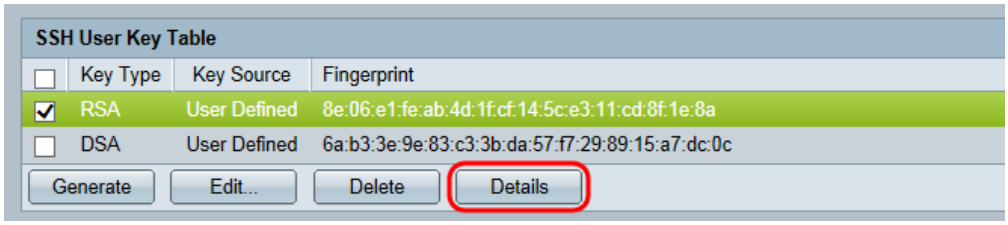
Passaggio 2. (Facoltativo) Fare clic su **Genera** per generare una nuova chiave. La nuova chiave sostituisce la chiave selezionata. Viene visualizzata una finestra di conferma. Fare clic su **OK** per continuare.



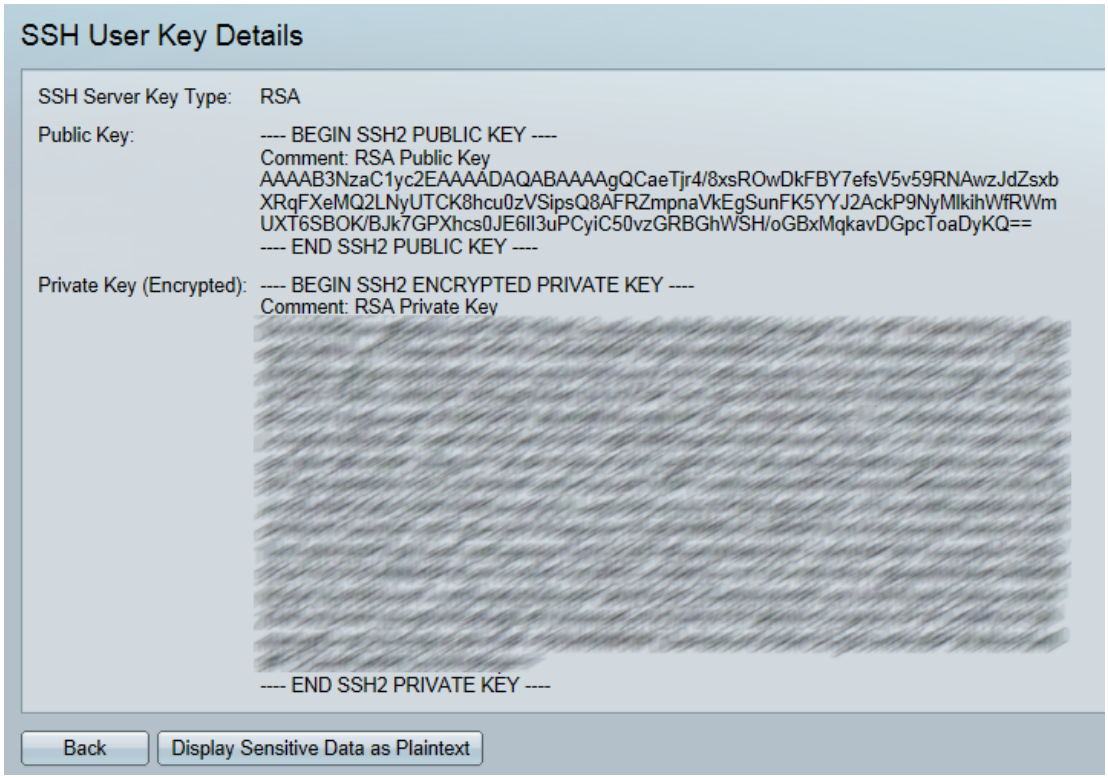
Passaggio 3. (Facoltativo) Fare clic su **Elimina** per eliminare la chiave selezionata. Viene visualizzata una finestra di conferma. Fare clic su **OK** per continuare.



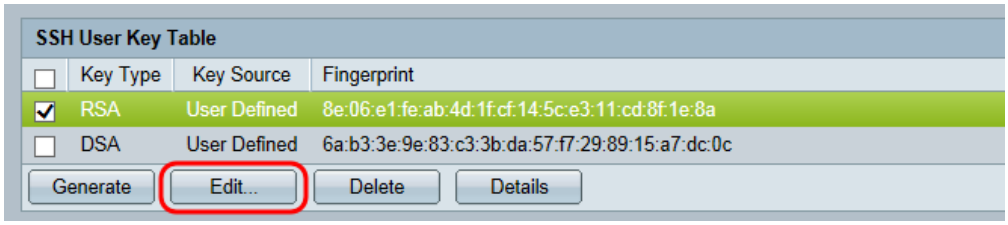
Passaggio 4. (Facoltativo) Fare clic su **Dettagli** per visualizzare i dettagli della chiave selezionata.



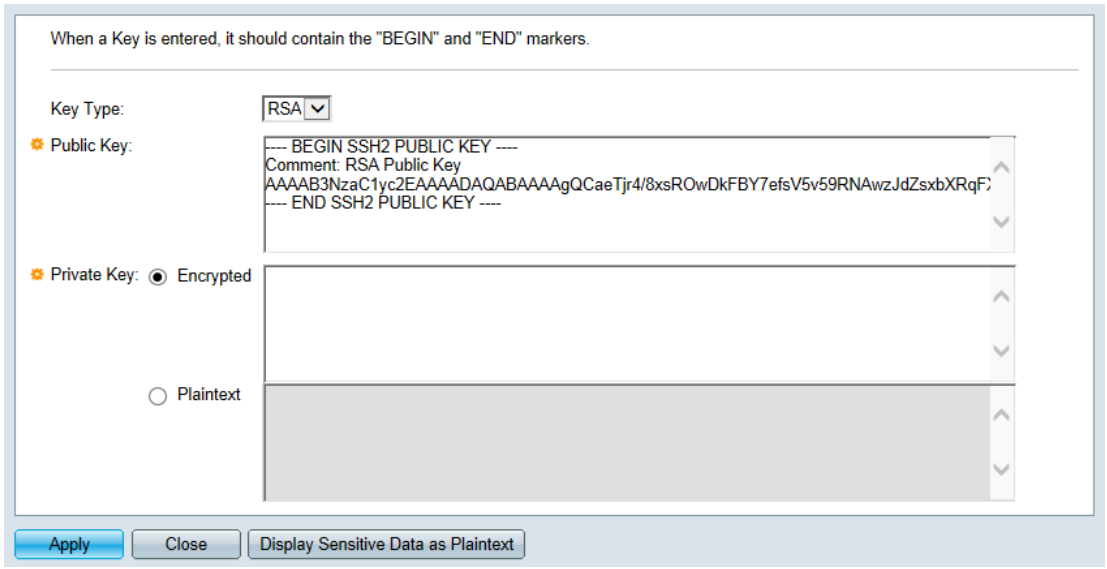
Viene visualizzata la pagina SSH User Key Details (Dettagli chiave utente SSH). Fare clic su **Indietro** per tornare alla tabella delle chiavi utente SSH.



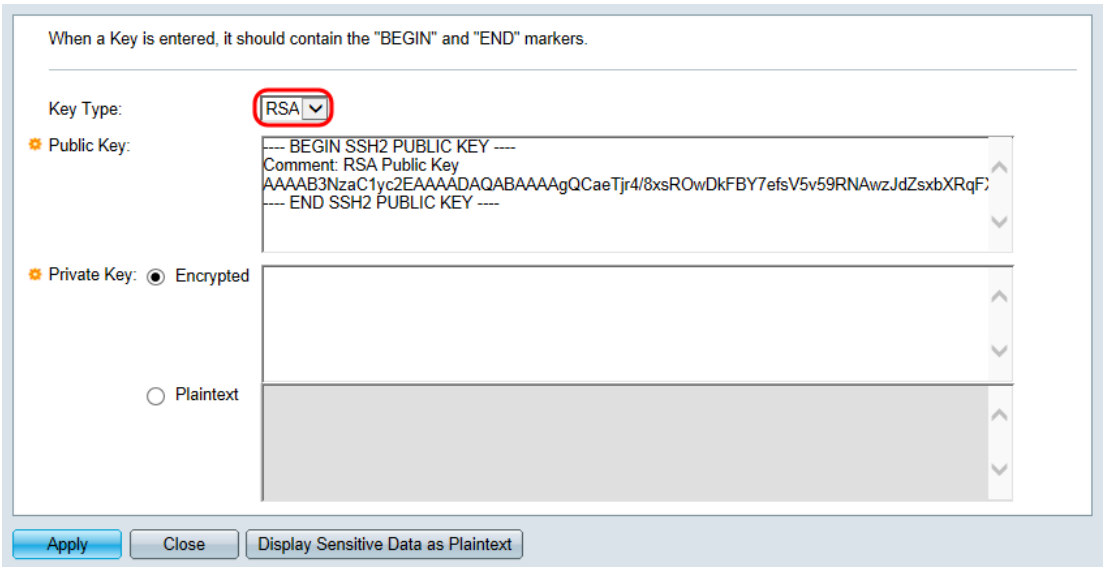
Passaggio 5. Fare clic su **Modifica** per modificare la chiave scelta.



Viene visualizzata la finestra *Edit SSH Client Authentication Settings*:



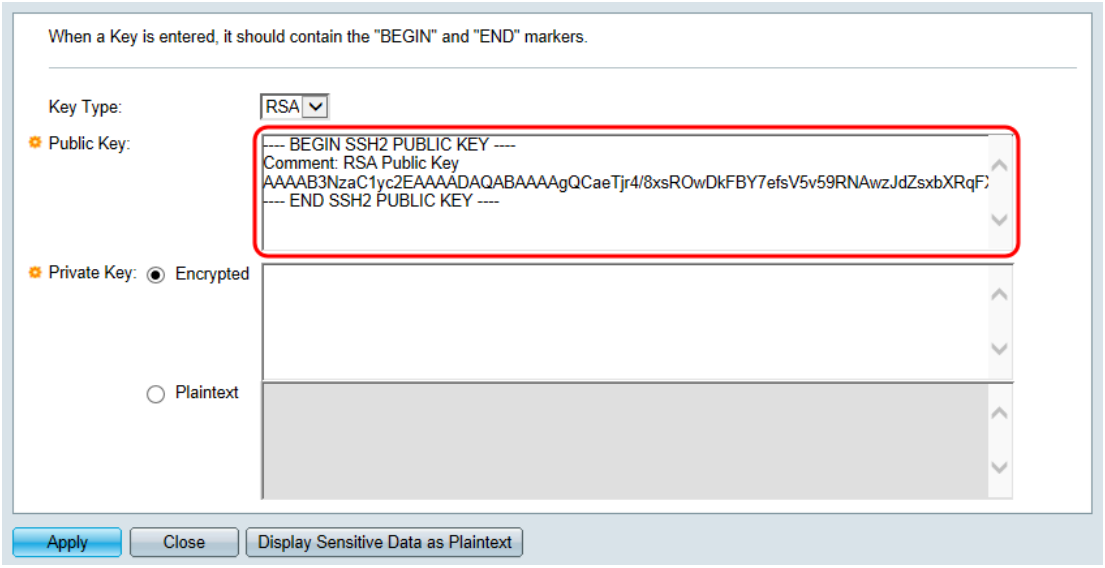
Passaggio 6. Selezionare il tipo di chiave desiderato dall'elenco a discesa *Tipo di chiave*.



Le opzioni disponibili sono le seguenti:

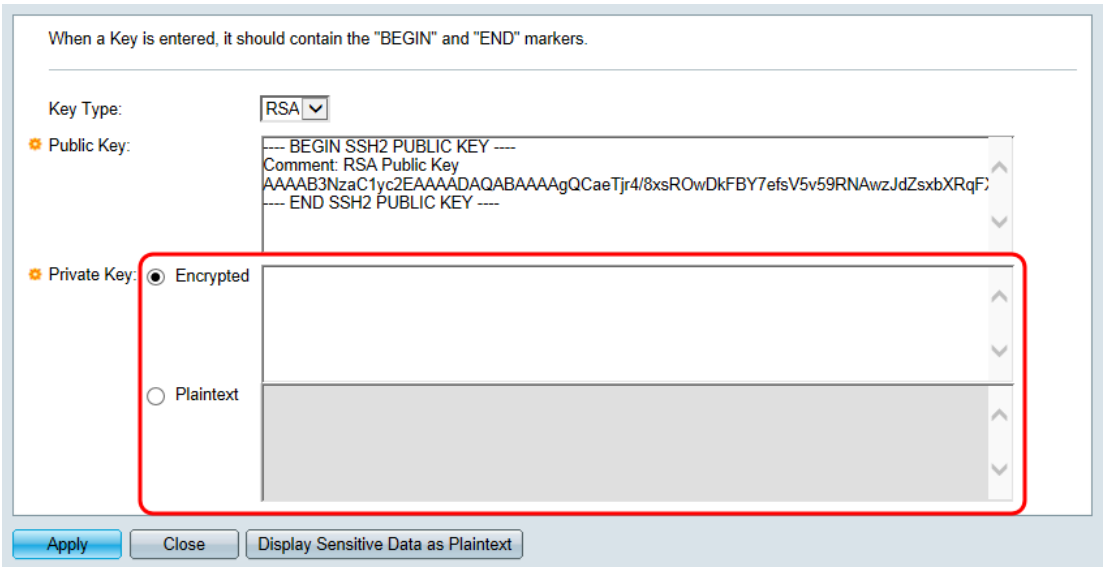
- RSA - RSA viene utilizzato per la crittografia e la firma.
- DSA: DSA viene utilizzato solo per la firma.

Passaggio 7. Nel campo *Chiave pubblica* è possibile modificare la chiave pubblica corrente.



Passaggio 8. Nel campo *Chiave privata* è possibile modificare la chiave privata corrente. Fare clic sul pulsante

Pulsante di opzione **Crittografato** per visualizzare la chiave privata corrente come crittografata. In caso contrario, fare clic sul pulsante di opzione **Testo normale** per visualizzare la chiave privata corrente come testo normale.



Passaggio 9. Fare clic su **Apply** (Applica) per salvare le modifiche.