Configurazione delle impostazioni di autenticazione utente Secure Shell (SSH) su uno switch Cisco Business serie 350

Obiettivo

In questo documento viene spiegato come configurare l'autenticazione dell'utente client sugli switch Cisco Business serie 350.

Introduzione

Secure Shell (SSH) è un protocollo che permette di connettersi in modo sicuro a dispositivi di rete remoti. Questa connessione offre una funzionalità simile a una connessione Telnet, con la differenza che è crittografata. SSH consente all'amministratore di configurare lo switch dalla riga di comando (CLI) con un programma di terze parti.

In modalità CLI tramite SSH, l'amministratore può eseguire configurazioni più avanzate in una connessione protetta. Le connessioni SSH sono utili per risolvere i problemi di una rete in remoto, nei casi in cui l'amministratore di rete non sia fisicamente presente sul sito di rete. Lo switch consente all'amministratore di autenticare e gestire gli utenti per connettersi alla rete tramite SSH. L'autenticazione viene effettuata tramite una chiave pubblica che l'utente può utilizzare per stabilire una connessione SSH a una rete specifica.

La funzionalità client SSH è un'applicazione che viene eseguita sul protocollo SSH per fornire l'autenticazione e la crittografia del dispositivo. Consente a un dispositivo di stabilire una connessione protetta e crittografata a un altro dispositivo che esegue il server SSH. Con l'autenticazione e la crittografia, il client SSH permette una comunicazione sicura su una connessione Telnet non protetta.

Dispositivi interessati | Versione software

- CBS350 (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)
- CBS350-2X (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)
- CBS350-4X (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)

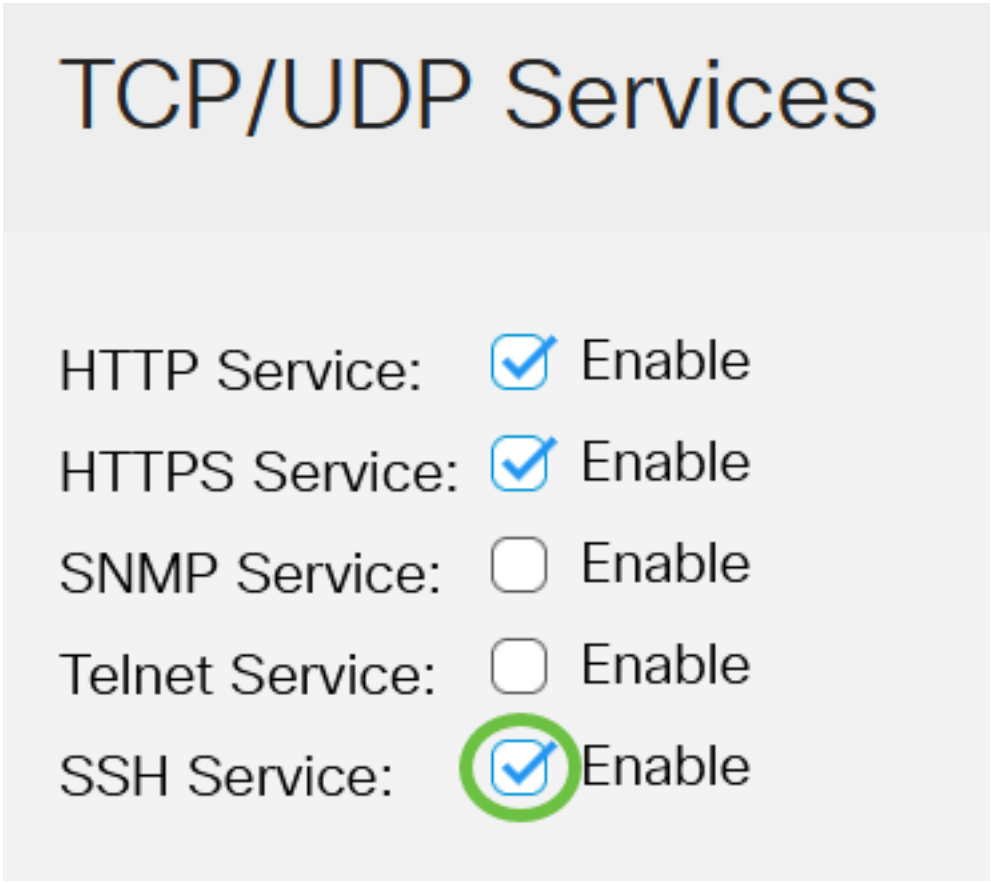
Configurazione delle impostazioni di autenticazione utente del client SSH

Abilitazione del servizio SSH

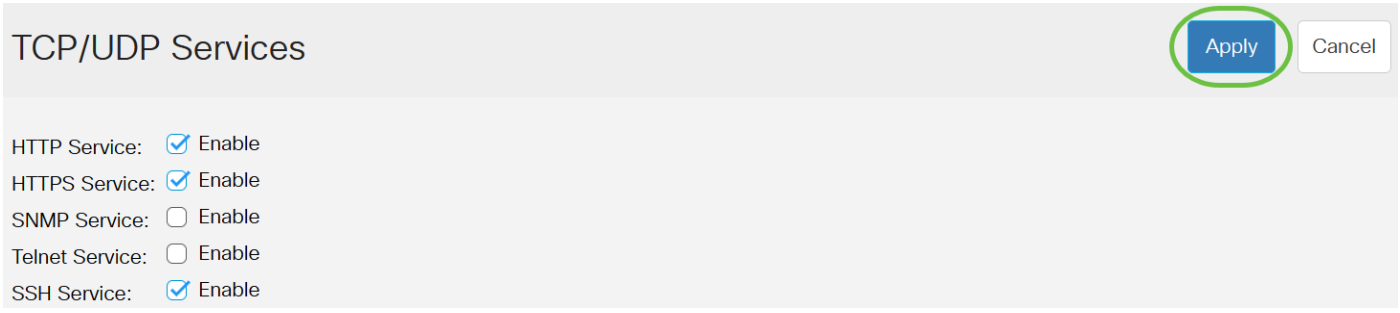
Per supportare la configurazione automatica di un dispositivo non incluso (dispositivo con configurazione predefinita), l'autenticazione del server SSH è disabilitata per impostazione predefinita.

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > Servizi TCP/UDP**

Passaggio 2. Selezionare la casella di controllo **Servizio SSH** per abilitare l'accesso del prompt dei comandi degli switch tramite SSH.



Passaggio 3. Fare clic su **Apply** (Applica) per abilitare il servizio SSH.

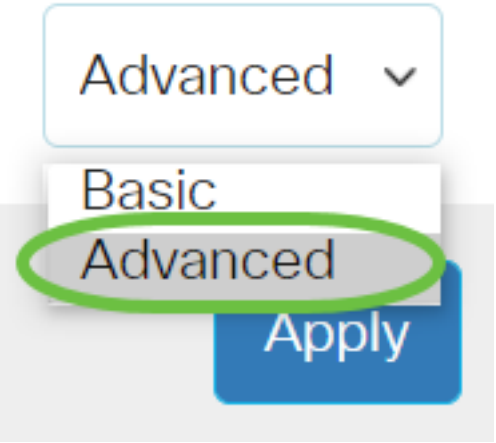


Configurazione delle impostazioni di autenticazione utente SSH

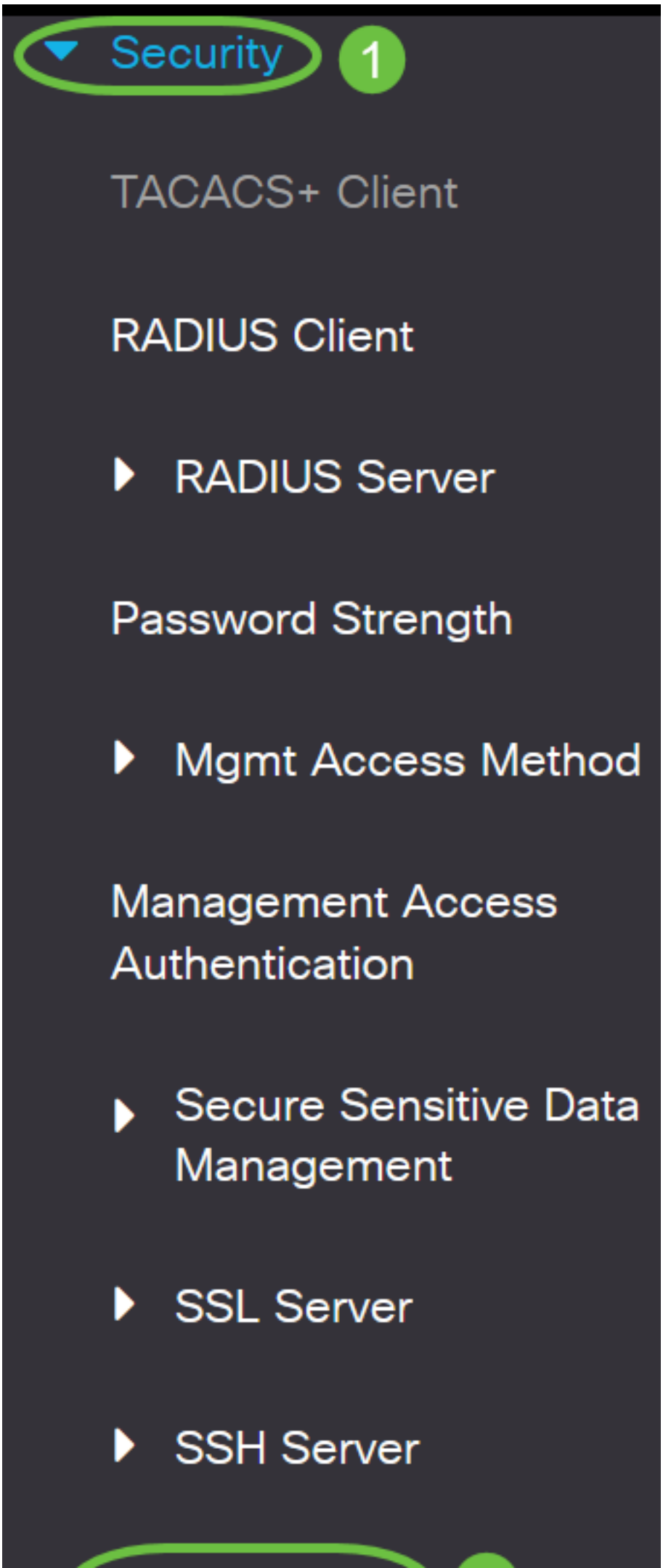
Utilizzare questa pagina per scegliere un metodo di autenticazione utente SSH. È possibile impostare un nome utente e una password sul dispositivo se si sceglie il metodo password. È inoltre possibile generare una chiave Ron Rivest, Adi Shamir e Leonard Adleman (RSA) o Digital Signature Algorithm (DSA) se è selezionato il metodo della chiave pubblica o privata.

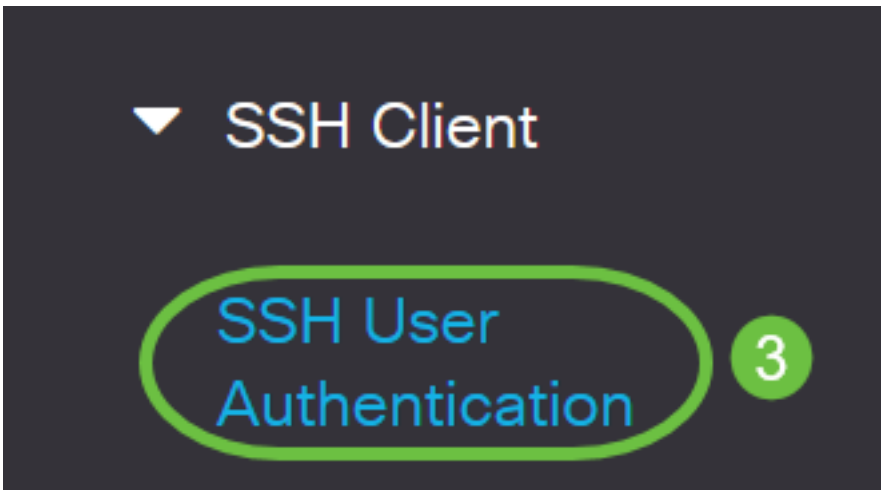
Le coppie di chiavi predefinite RSA e DSA vengono generate per il dispositivo all'avvio. Una di queste chiavi è utilizzata per crittografare i dati scaricati dal server SSH. La chiave RSA è utilizzata per impostazione predefinita. Se l'utente elimina una o entrambe queste chiavi, queste vengono rigenerate.

Passaggio 1. Accedere all'utility basata sul Web dello switch, quindi selezionare Advanced nell'elenco a discesa Display Mode (Modalità di visualizzazione).

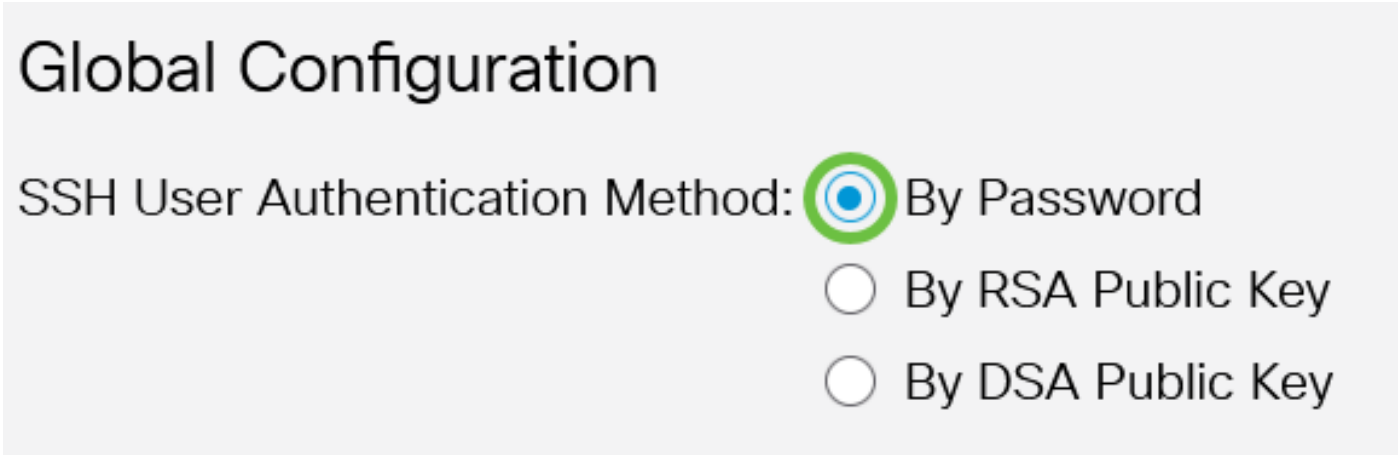


Passaggio 2. Selezionare **Security > SSH Client > SSH User Authentication** dal menu.


Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Passaggio 3. In Configurazione globale, fare clic sul metodo di autenticazione utente SSH desiderato.



Quando un dispositivo (client SSH) tenta di stabilire una sessione SSH con il server SSH, questo utilizza uno dei seguenti metodi di autenticazione del client:

- Per password: questa opzione consente di configurare una password per l'autenticazione utente. Si tratta dell'impostazione predefinita e la password predefinita è anonima. Se si sceglie questa opzione, verificare che le credenziali di nome utente e password siano state stabilite sul server SSH.
- Per chiave pubblica RSA: questa opzione consente di utilizzare la chiave pubblica RSA per l'autenticazione dell'utente. Una chiave RSA è una chiave crittografata basata sulla fattorizzazione di numeri interi di grandi dimensioni. Questa chiave è la chiave più comune utilizzata per l'autenticazione dell'utente SSH.
- Per chiave pubblica DSA: questa opzione consente di utilizzare una chiave pubblica DSA per l'autenticazione utente. Una chiave DSA è una chiave crittografata basata su un algoritmo discreto ElGamal. Questa chiave non viene in genere utilizzata per l'autenticazione dell'utente SSH in quanto richiede più tempo.

Nell'esempio, viene scelto Per password.

Passaggio 4. Nell'area Credenziali, immettere il nome utente nel campo *Nome utente*.

nell'esempio viene usato ciscosbuser1.

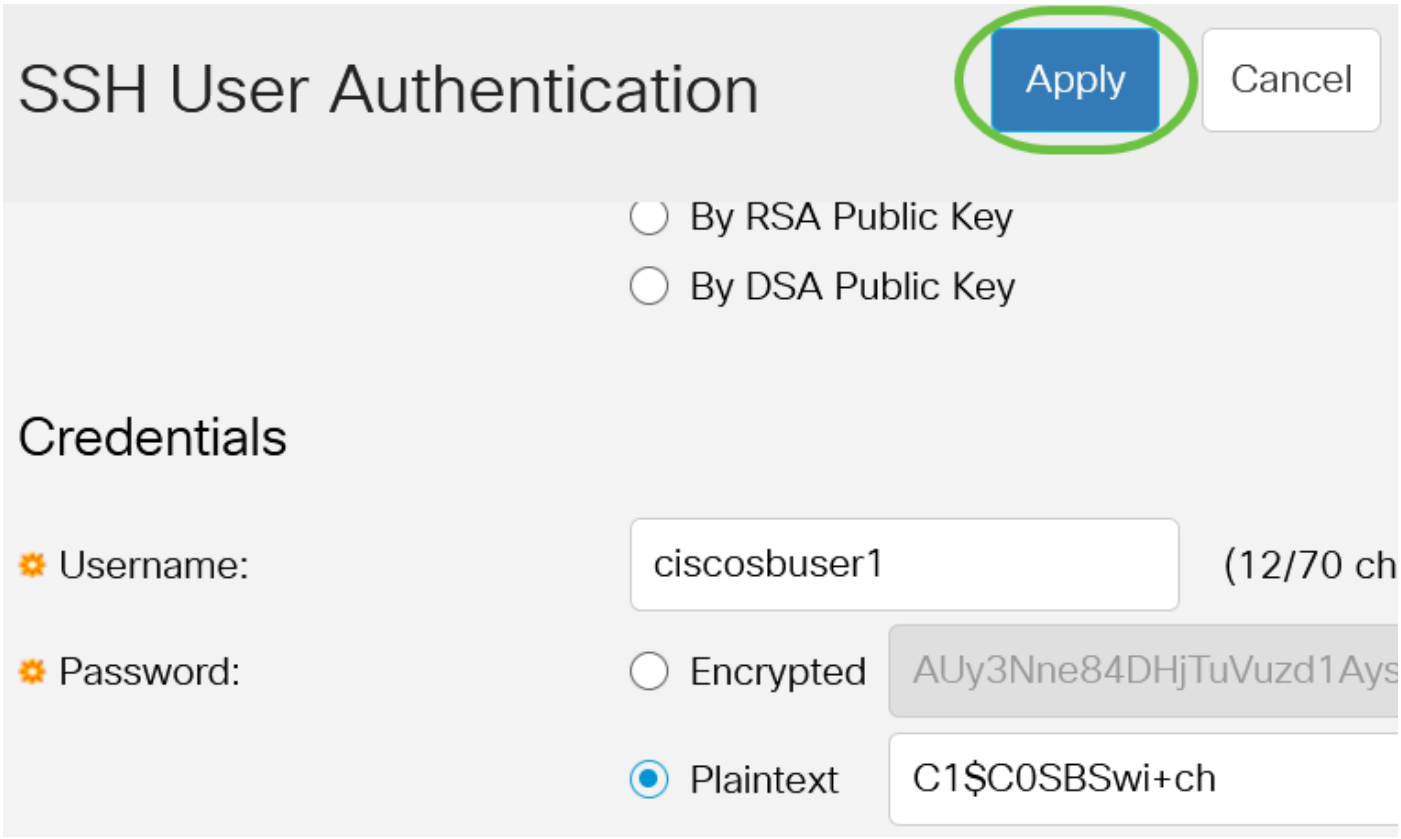
Passaggio 5. (Facoltativo) Se si sceglie Per password al passaggio 2, fare clic sul metodo e immettere la password nel campo *Crittografato* o *Testo normale*.

Le opzioni sono:

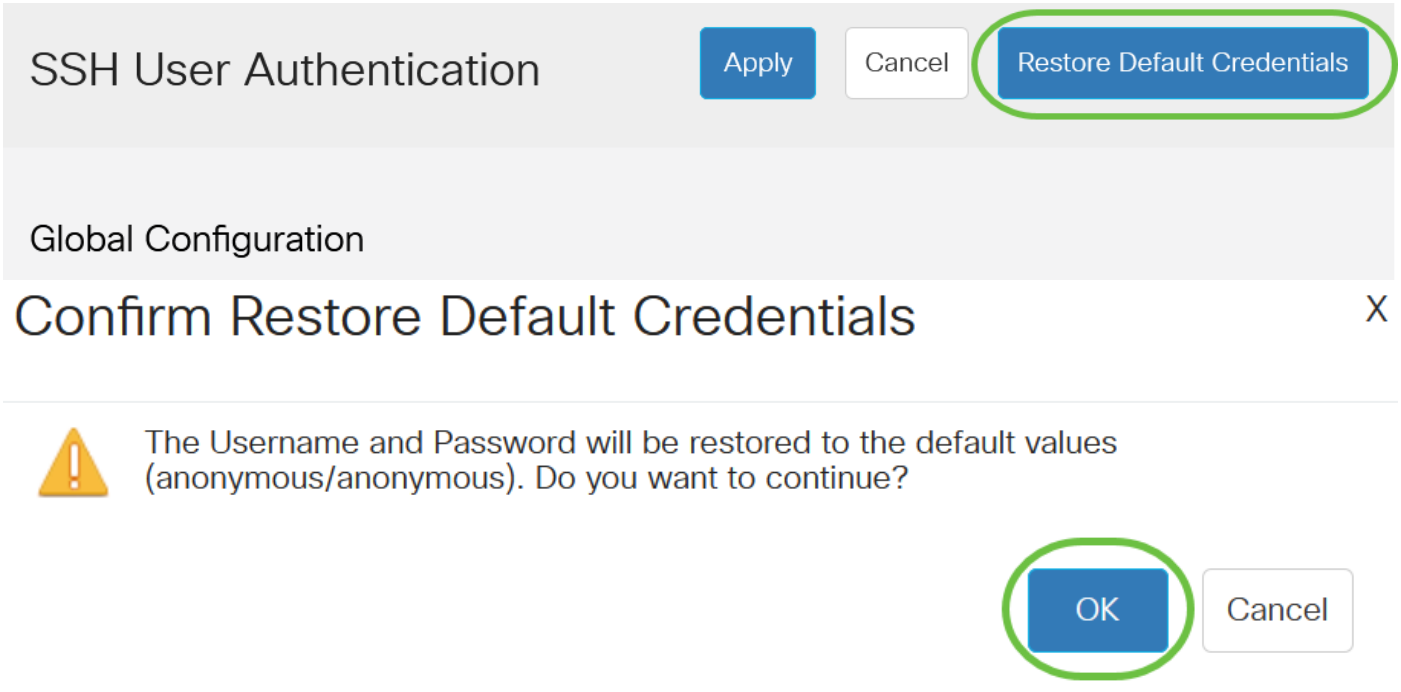
- Crittografata - Questa opzione consente di immettere una versione crittografata della password.
- Testo normale - Questa opzione consente di immettere una password in testo normale.

In questo esempio viene scelto Testo normale e viene immessa una password in testo normale.

Passaggio 6. Fare clic su **Applica** per salvare la configurazione di autenticazione.

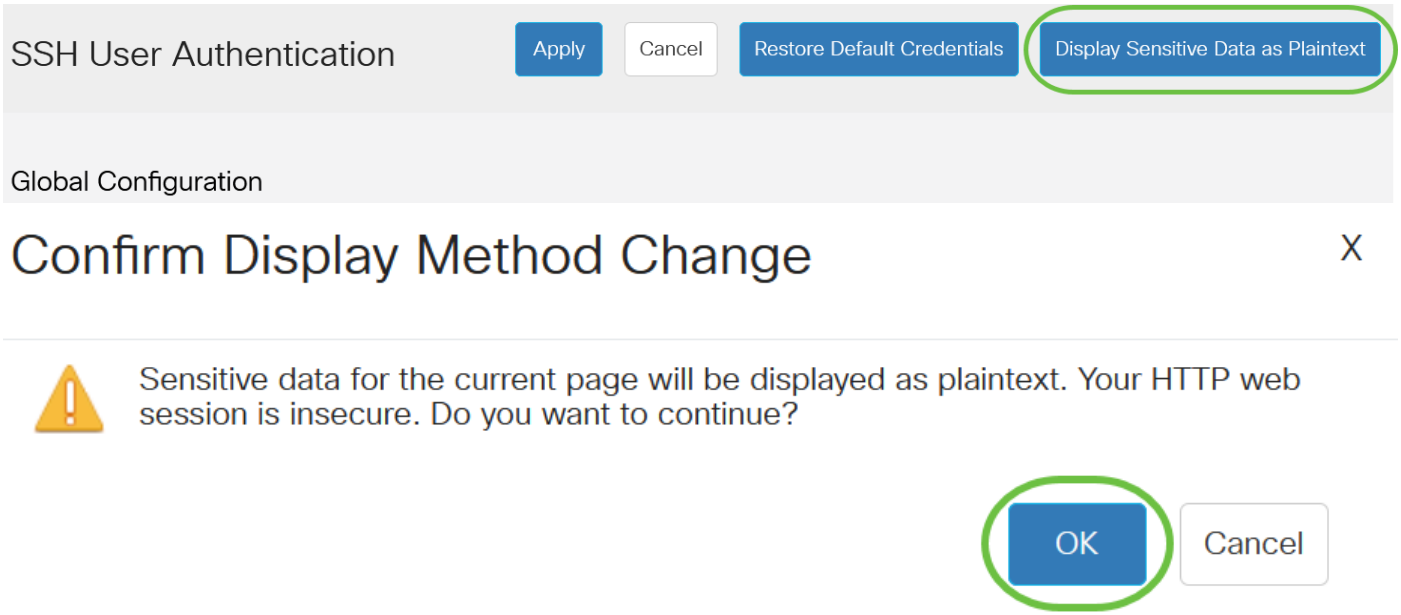


Passaggio 7. (Facoltativo) Fare clic su **Ripristina credenziali predefinite** per ripristinare il nome utente e la password predefiniti, quindi fare clic su **OK** per continuare.



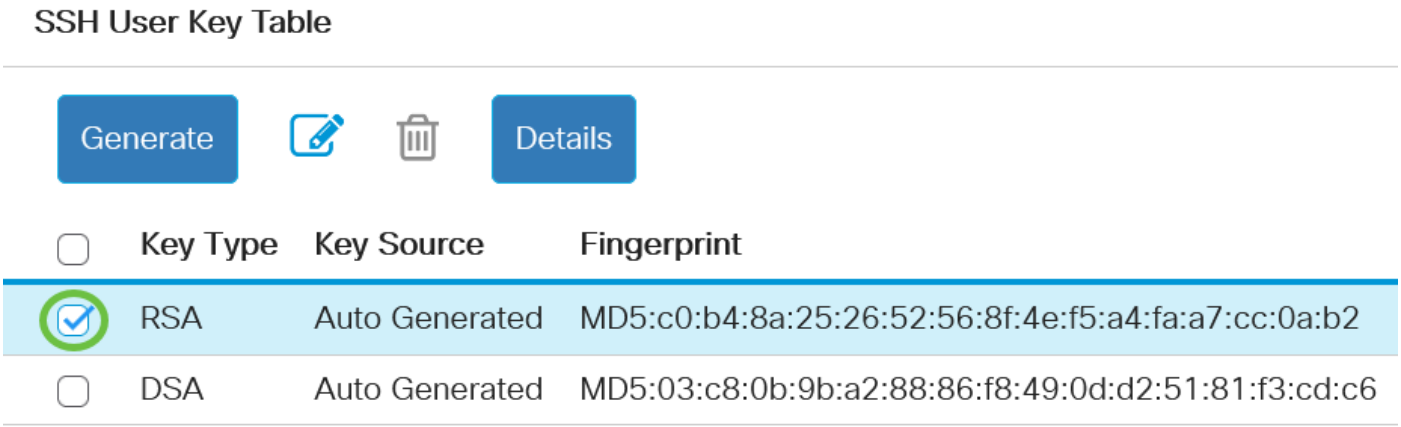
Il nome utente e la password verranno ripristinati ai valori predefiniti: anonimo/anonimo.

Passaggio 8. (Facoltativo) Fare clic su **Visualizza dati sensibili come testo normale** per visualizzare i dati sensibili della pagina in formato testo normale, quindi fare clic su **OK** per continuare.



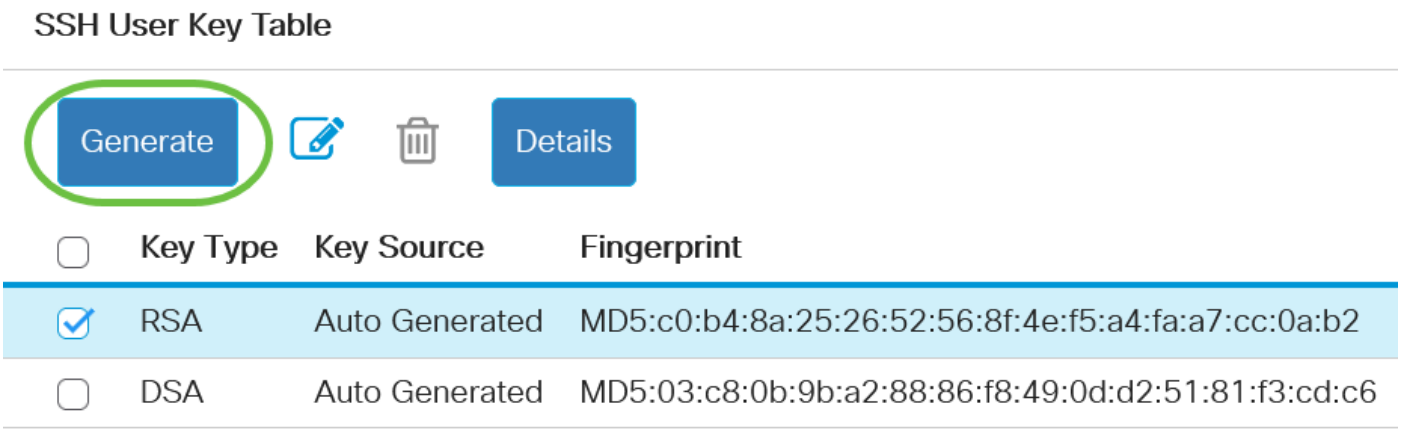
Configurazione della tabella delle chiavi utente SSH

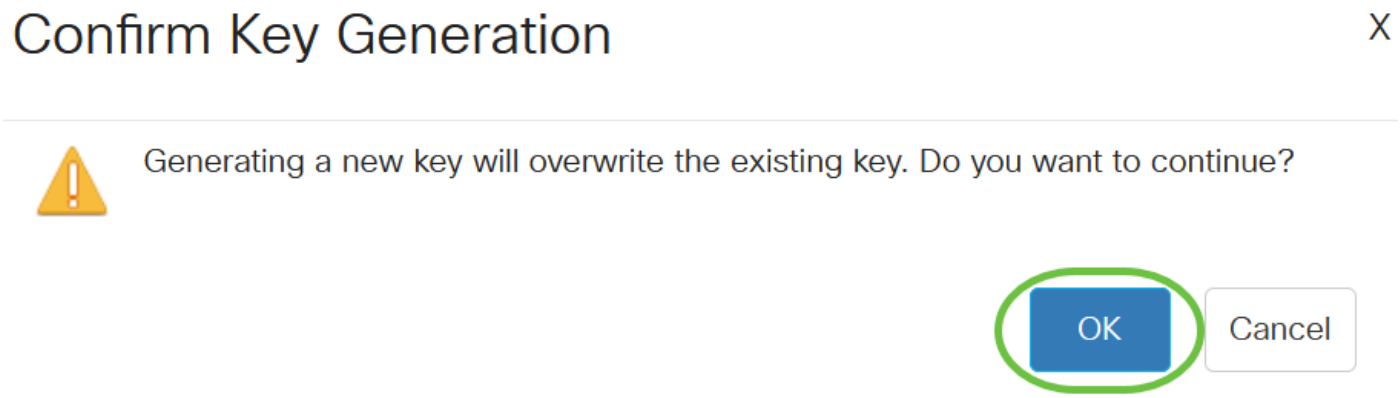
Passaggio 9. Selezionare la casella di controllo della chiave che si desidera gestire.



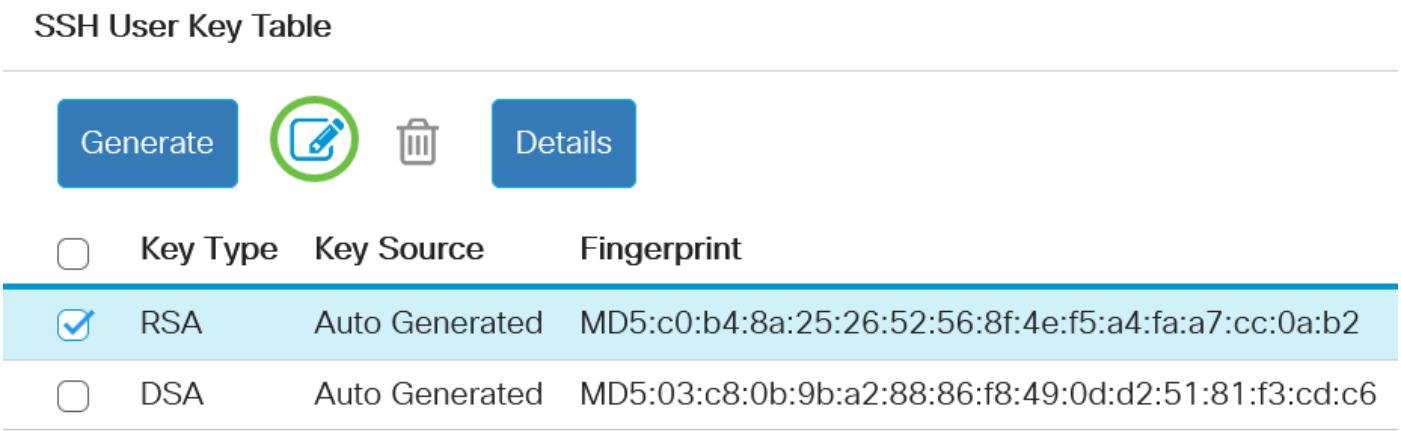
Nell'esempio, viene scelto RSA.

Passaggio 10. (Facoltativo) Fare clic su **Genera** per generare una nuova chiave. La nuova chiave sostituirà la chiave selezionata, quindi fare clic su **OK** per continuare.

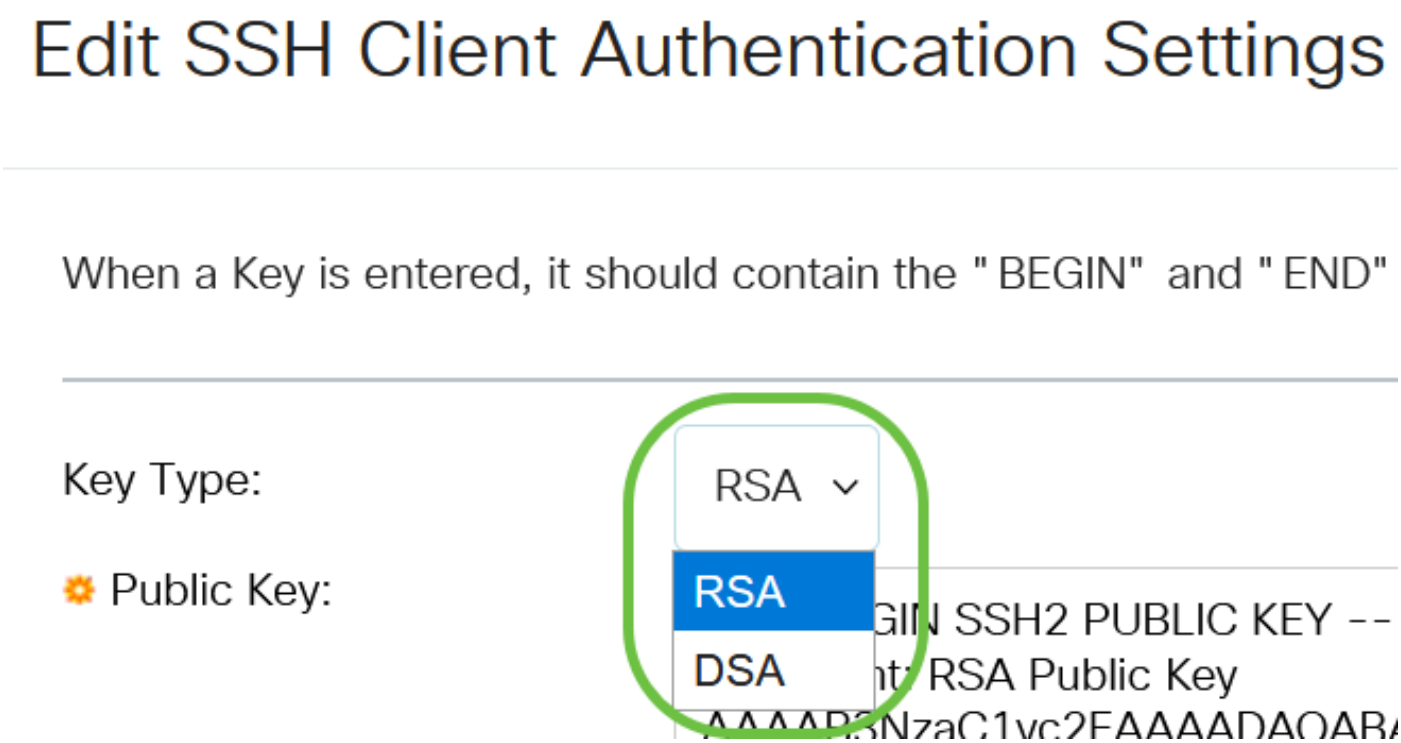




Passaggio 11. (Facoltativo) Fare clic su **Modifica** per modificare una chiave corrente.

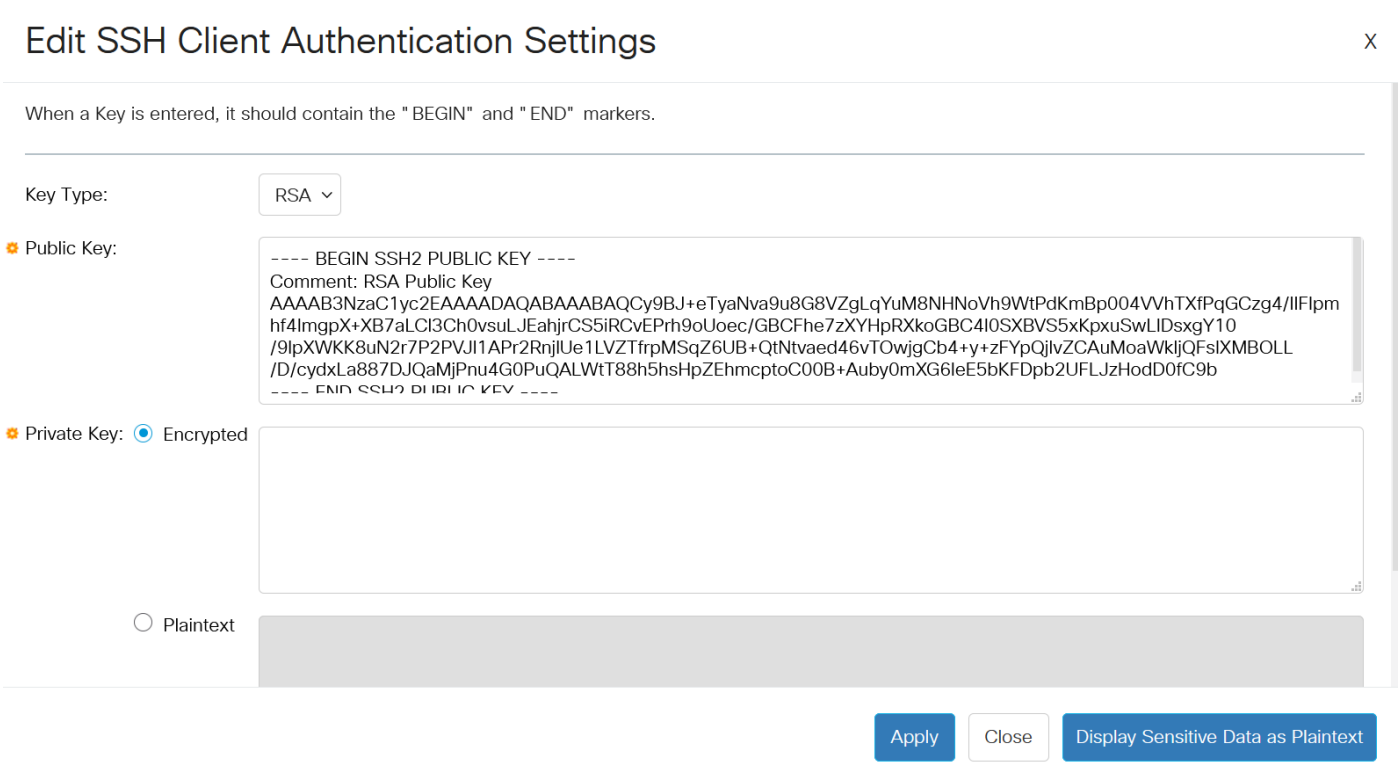


Passaggio 12. (Facoltativo) Scegliere un tipo di chiave dall'elenco a discesa Tipo di chiave.



Nell'esempio, viene scelto RSA.

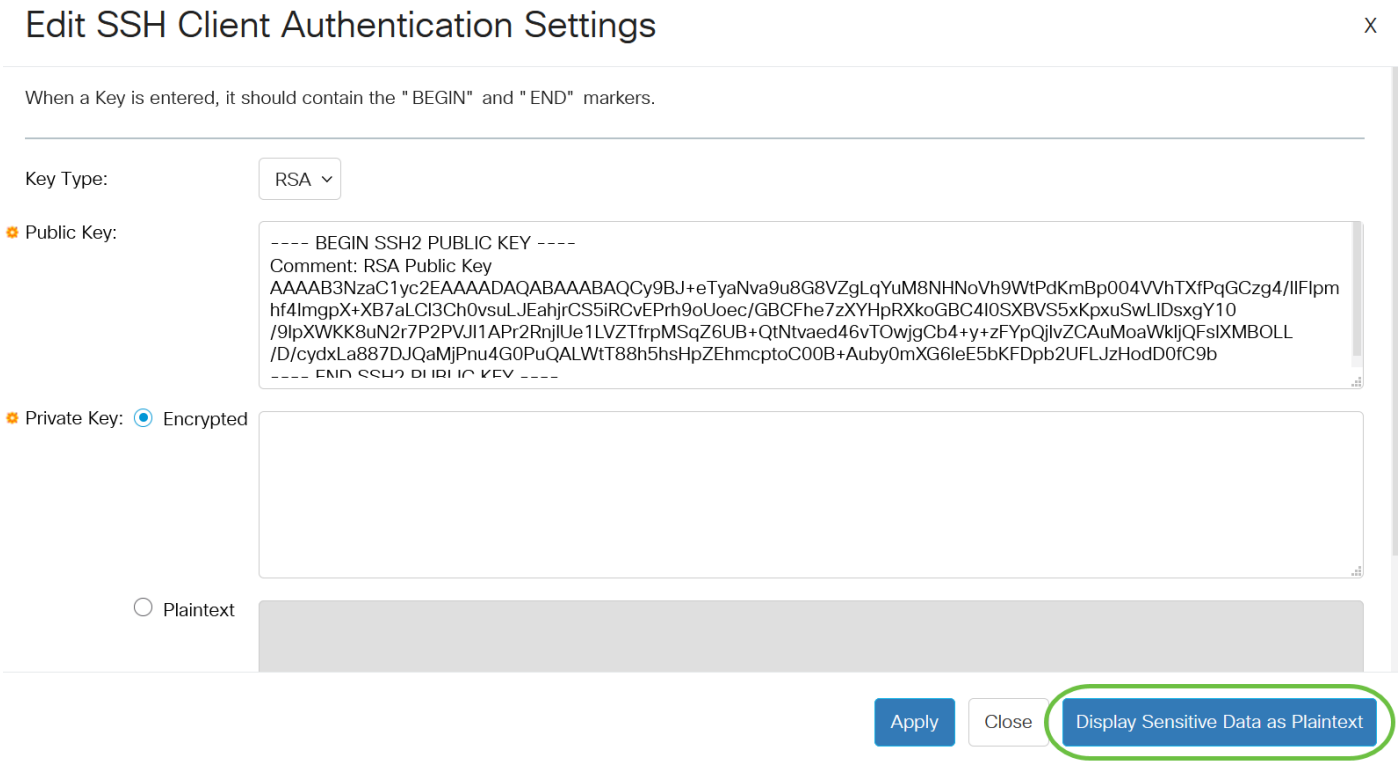
Passaggio 13. (Facoltativo) Immettere la nuova chiave pubblica nel campo *Chiave pubblica*.

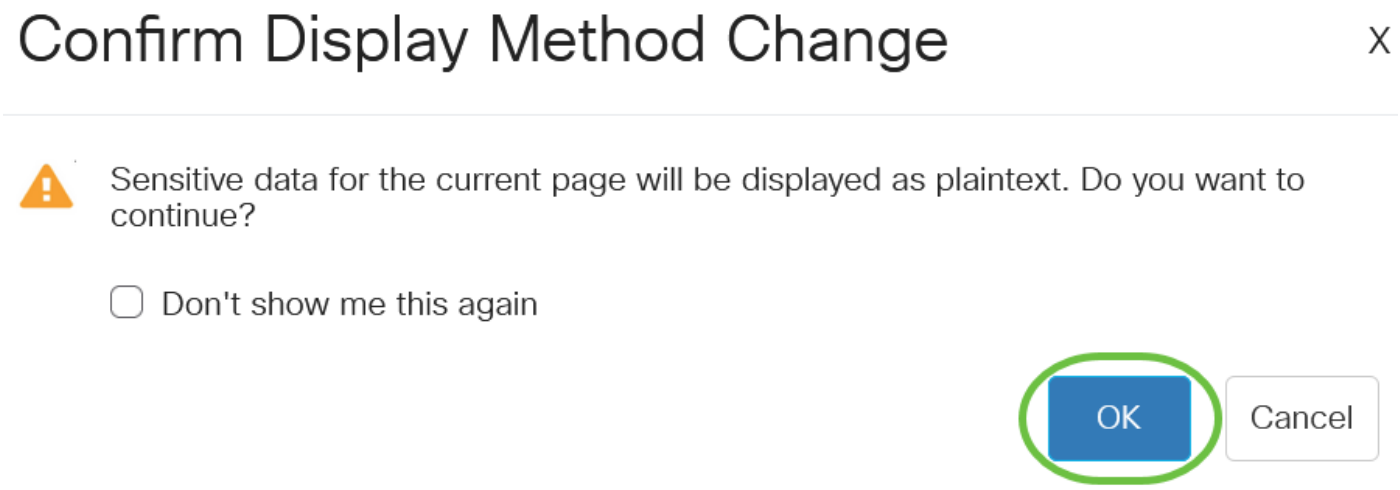


Passaggio 14. (Facoltativo) Immettere la nuova chiave privata nel campo *Chiave privata*.

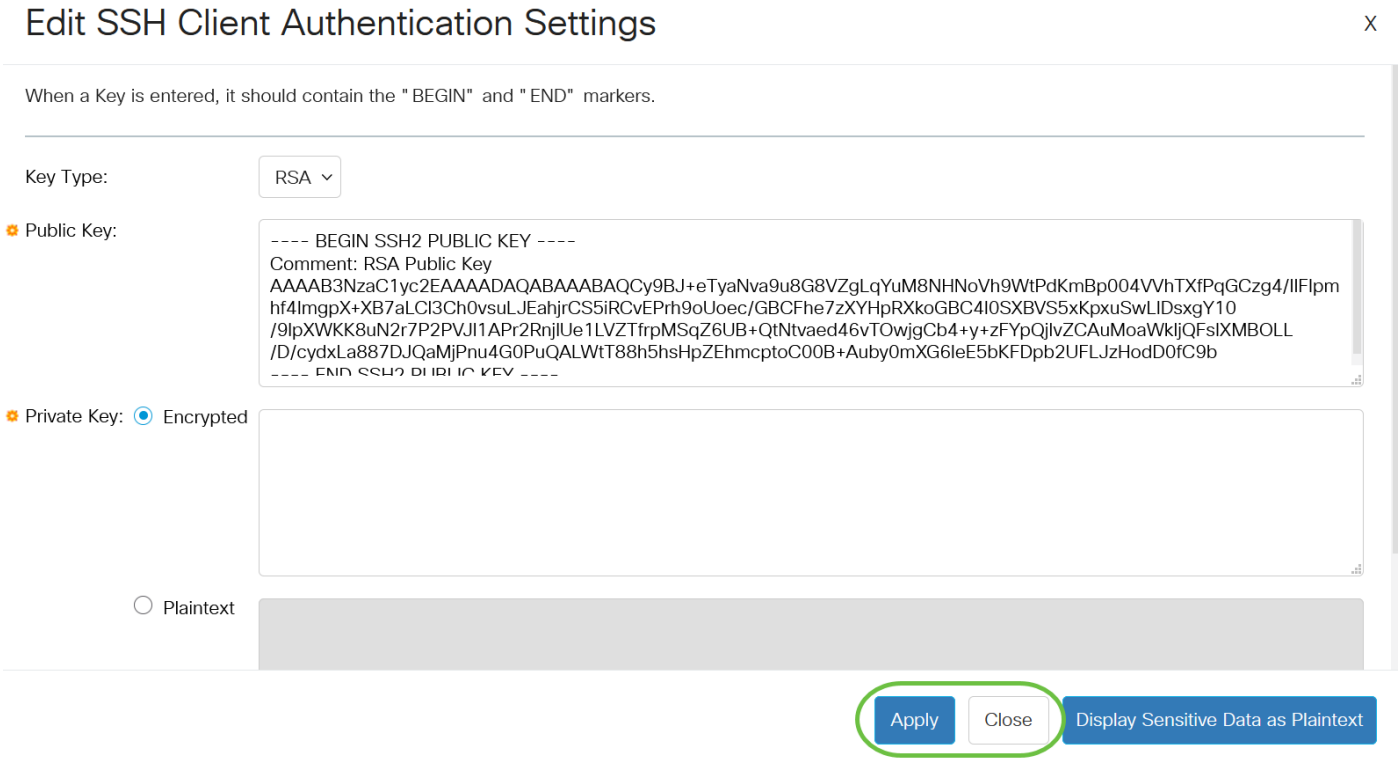
Èpossibile modificare la chiave privata e fare clic su Crittografata per visualizzare la chiave privata corrente come testo crittografato oppure su Testo normale per visualizzare la chiave privata corrente in testo normale.

Passaggio 15. (Facoltativo) Fare clic su **Visualizza dati sensibili come testo normale** per visualizzare i dati crittografati della pagina in formato testo normale, quindi fare clic su **OK** per continuare.

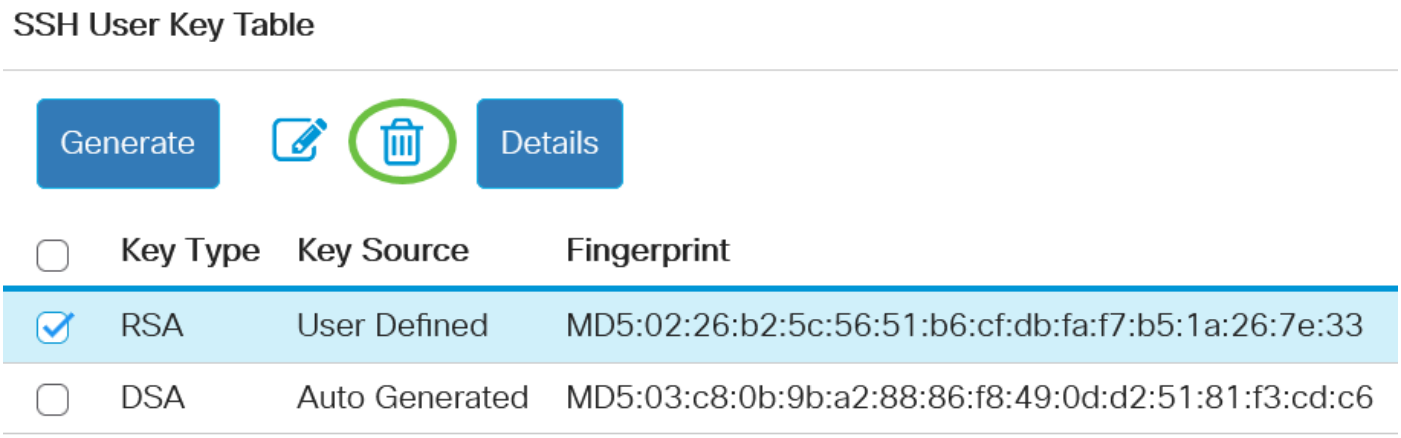




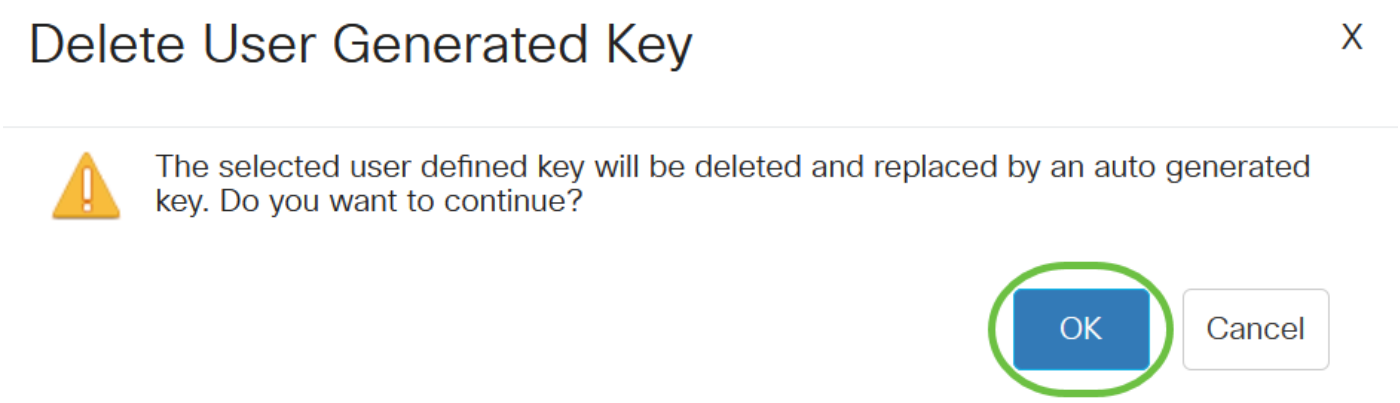
Passaggio 16. Fare clic su **Apply** per salvare le modifiche, quindi su **Close**.



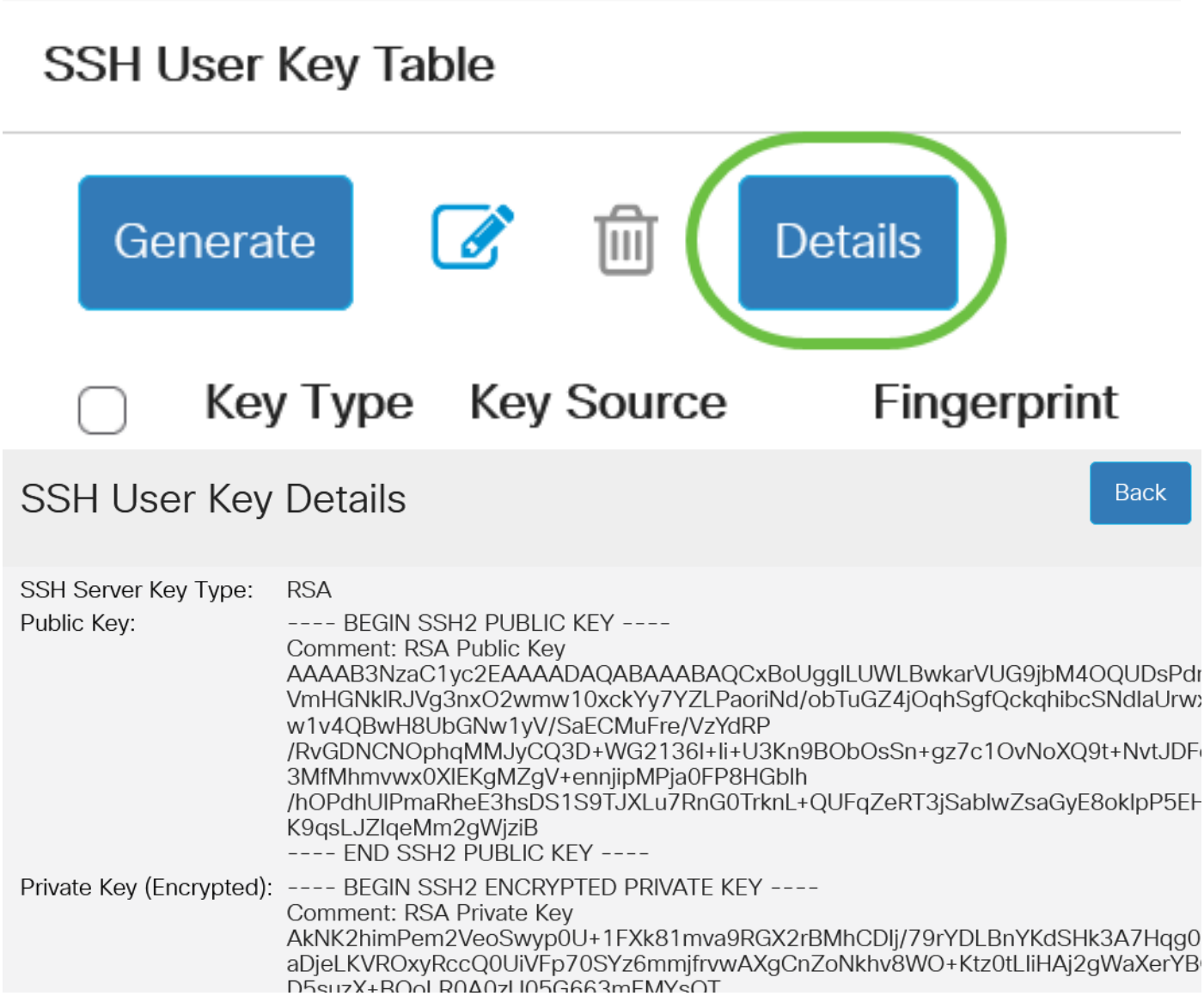
Passaggio 17. (Facoltativo) Fare clic su **Elimina** per eliminare la chiave selezionata.



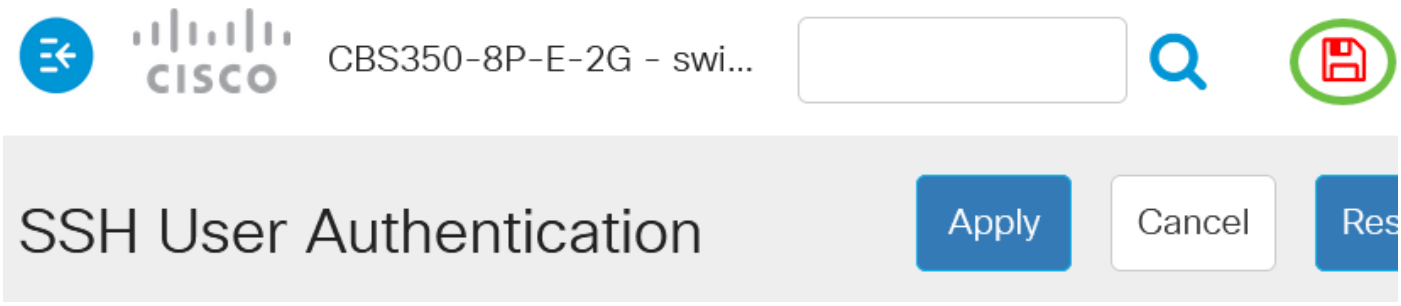
Passaggio 18. (Facoltativo) Quando richiesto da un messaggio di conferma, come mostrato di seguito, fare clic su **OK** per eliminare la chiave.



Passaggio 19. (Facoltativo) Fare clic su **Dettagli** per visualizzare i dettagli della chiave selezionata.



Passaggio 20. (Facoltativo) Fare clic sul pulsante **Save** nella parte superiore della pagina per salvare le modifiche nel file della configurazione di avvio.



A questo punto, sono state configurate le impostazioni di autenticazione dell'utente client sullo switch Cisco Business serie 350.