Configurazione delle impostazioni di autenticazione utente Secure Shell (SSH) su uno switch

Obiettivo

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.

In questo documento viene spiegato come configurare l'autenticazione degli utenti client su uno switch gestito.

Dispositivi interessati

- Serie Sx200
- Serie Sx300
- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

Versione del software

- 1.4.5.02 - Serie Sx200, Serie Sx300, Serie Sx500
- 2.2.0.66 - Serie Sx350, Serie SG350X, Serie Sx550X

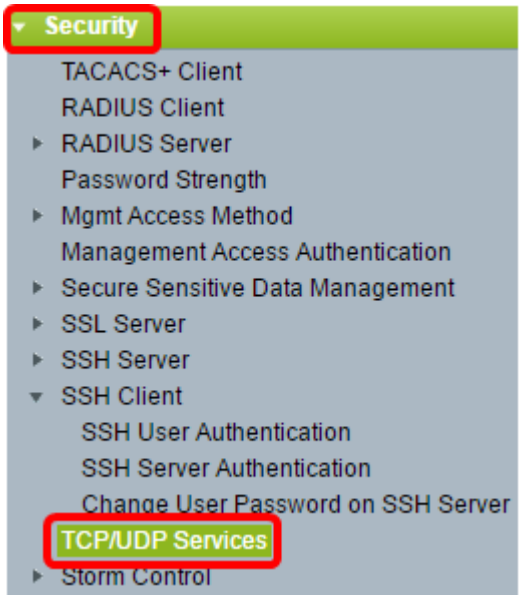
Configurazione delle impostazioni di autenticazione utente del client SSH

Abilitazione del servizio SSH

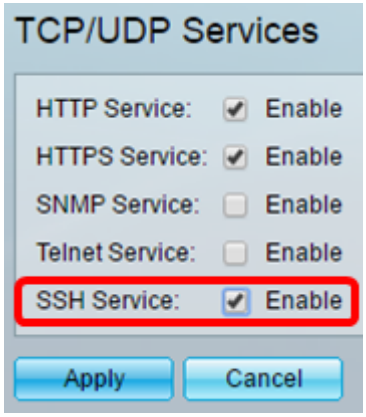
Nota: per supportare la configurazione automatica di un dispositivo out-of-box (dispositivo

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 **SSH Service** per abilitare l'accesso del prompt dei comandi degli switch tramite SSH.



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

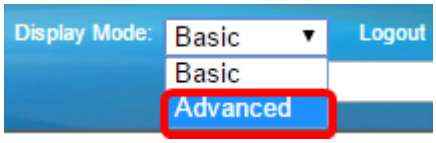
Configurazione delle impostazioni di autenticazione utente SSH

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.

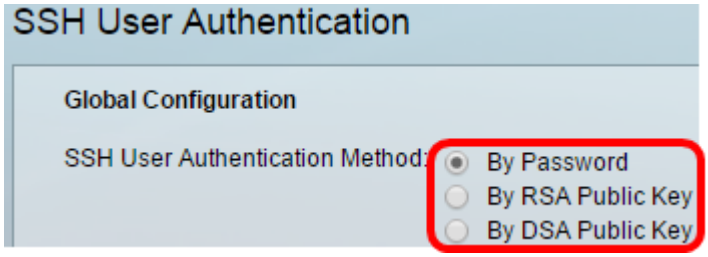
Le coppie di chiavi predefinite RSA e DSA vengono generate per il dispositivo al momento dell'avvio. Una di queste chiavi è utilizzata per crittografare i dati scaricati dal server SSH. La chiave RSA è utilizzata per impostazione predefinita. Se l'utente elimina una o entrambe queste chiavi, queste vengono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

Passaggio 1. Accedere all'utility basata sul Web e selezionare **Security > SSH Client > SSH User Authentication** (Sicurezza > Client SSH > Autenticazione utente SSH).

Nota: se si dispone di un Sx350, SG300X o Sx500X, passare alla modalità avanzata scegliendo **Avanzate** dall'elenco a discesa Display Mode (Modalità di visualizzazione).



Passaggio 2. In Configurazione globale, fare clic sul metodo di autenticazione utente SSH desiderato.

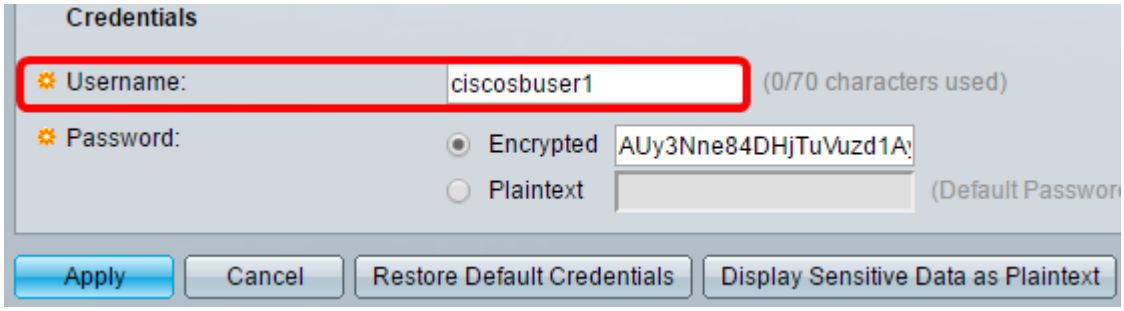


Nota: quando un dispositivo (client SSH) tenta di stabilire una sessione SSH con il server SSH, questo utilizza uno dei seguenti metodi di autenticazione del client:

- 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.

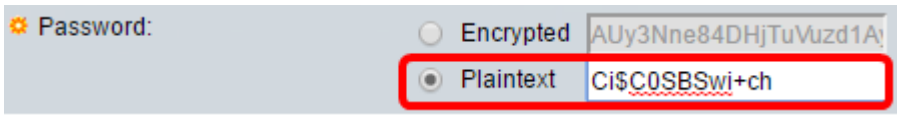
Nota: in questo esempio, è selezionato Per password.

Passaggio 3. Nell'area Credenziali, immettere il nome utente nel campo *Nome utente*.



Nota: nell'esempio viene usato ciscosbuser1.

Passaggio 4. (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:

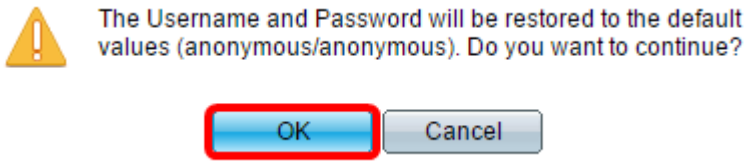
- Crittografata - questa opzione consente di immettere una versione crittografata della password.
- Testo normale — questa opzione consente di immettere una password in testo normale.

Nota: in questo esempio, viene scelto Testo normale e viene immessa una password in testo normale.

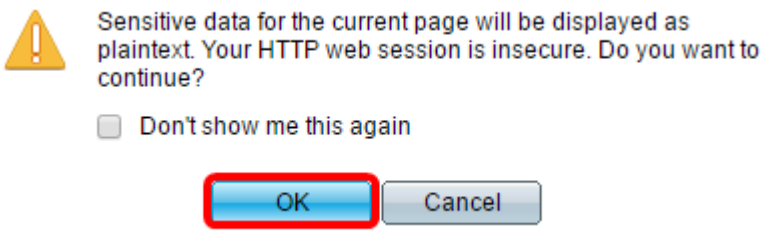
Passaggio 5. Fare clic su **Apply** (Applica) per salvare la configurazione dell'autenticazione.

Passaggio 6. (Facoltativo) Fare clic su **Ripristina credenziali predefinite** per ripristinare il nome utente e la password predefiniti, quindi fare clic su **OK** per continuare.

Nota: il nome utente e la password verranno ripristinati ai valori predefiniti anonimi.

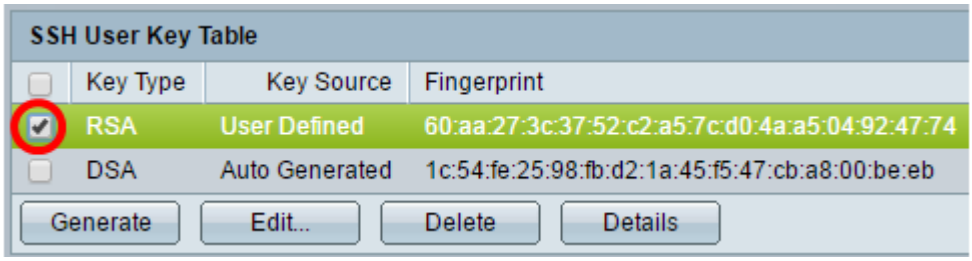


Passaggio 7. (Facoltativo) Fare clic su **Visualizza dati sensibili come testo normale** per visualizzare i dati sensibili della pagina in formato testo normale, quindi fare clic su **OK** per continuare.



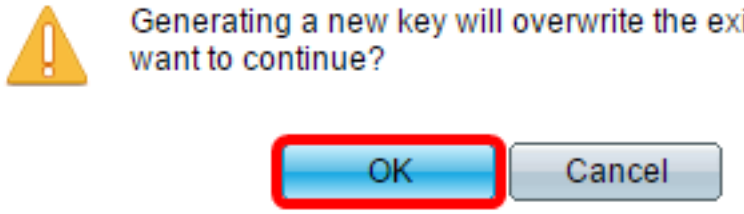
Configurazione della tabella delle chiavi utente SSH

Passaggio 8. Selezionare la casella di controllo della chiave che si desidera gestire.

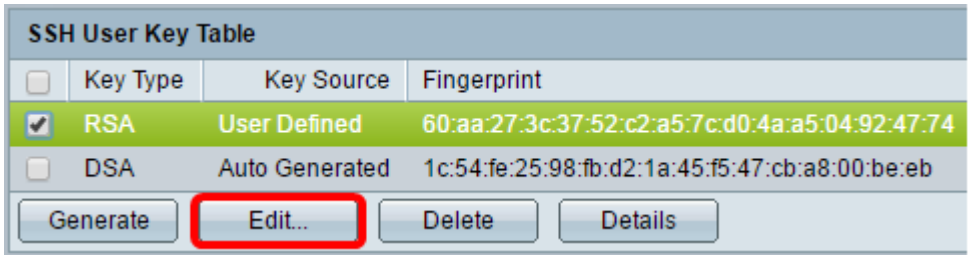


Nota: nell'esempio riportato viene scelto RSA.

Passaggio 9. (Facoltativo) Fare clic su **Genera** per generare una nuova chiave. La nuova chiave sostituirà la chiave selezionata, quindi fare clic su **OK** per continuare.



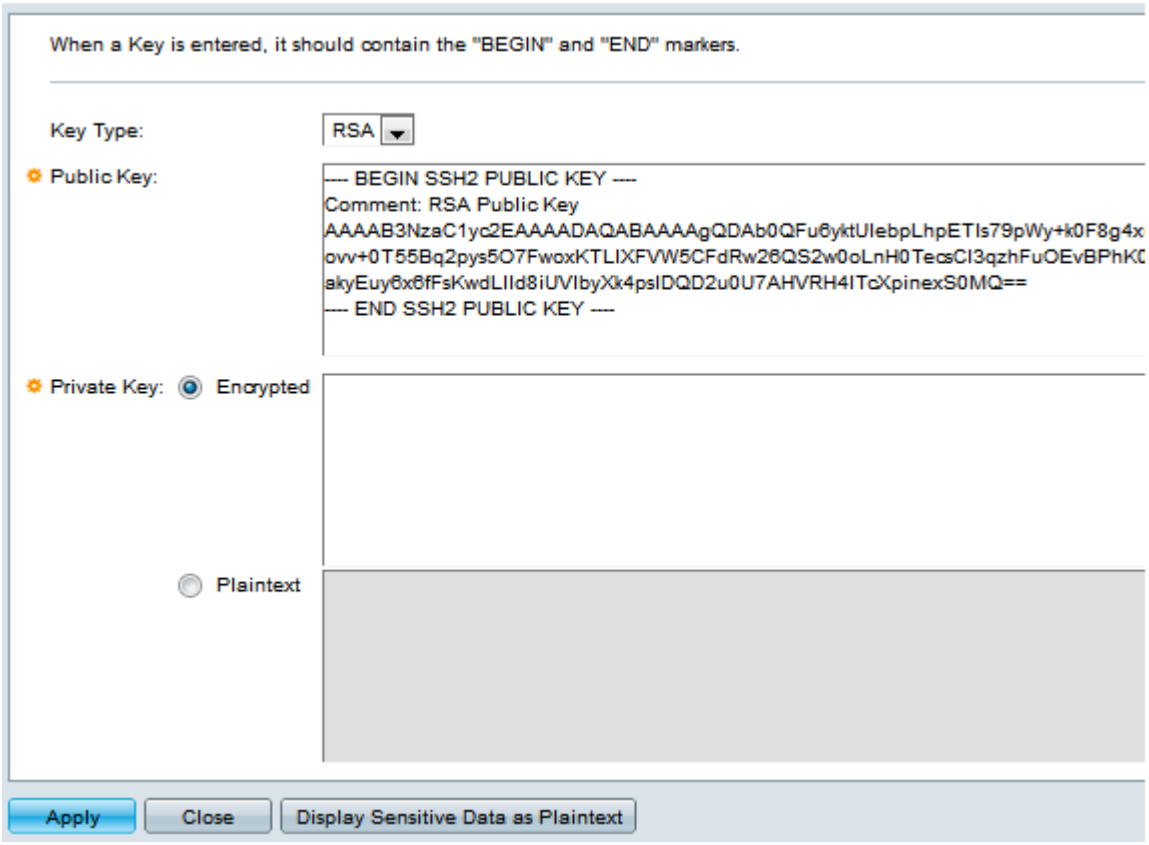
Passaggio 10. (Facoltativo) Fare clic su **Modifica** per modificare una chiave corrente.



Passaggio 11. (Facoltativo) Scegliere un tipo di chiave dall'elenco a discesa Tipo di chiave.

Nota: nell'esempio riportato viene scelto RSA.

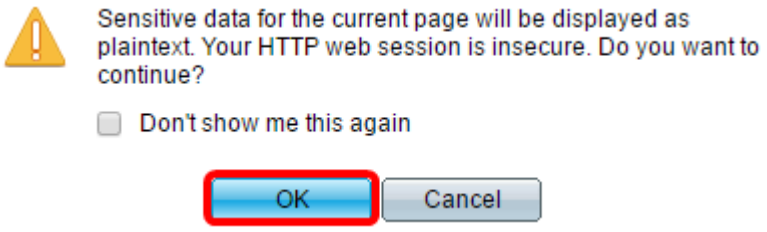
Passaggio 12. (Facoltativo) Immettere la nuova chiave pubblica nel campo *Chiave pubblica*.



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

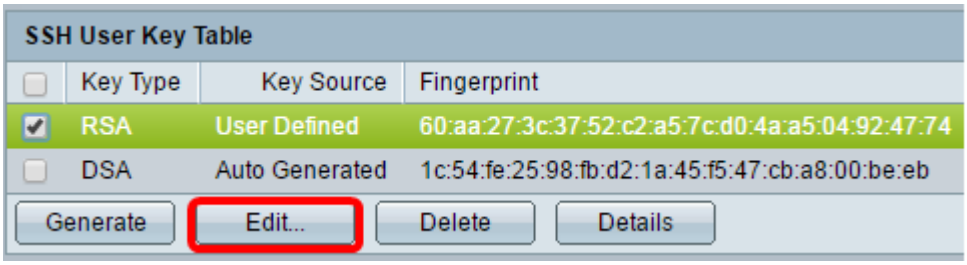
Nota: è possibile modificare la chiave privata e fare clic su Crittografata per visualizzare la chiave privata corrente come testo crittografato oppure su Testo normale per visualizzare la chiave privata corrente in testo normale.

Passaggio 14. (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.

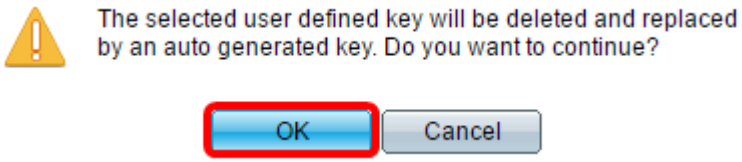


Passaggio 15. Fare clic su **Apply** (Applica) per salvare le modifiche, quindi su **Close** (Chiudi).

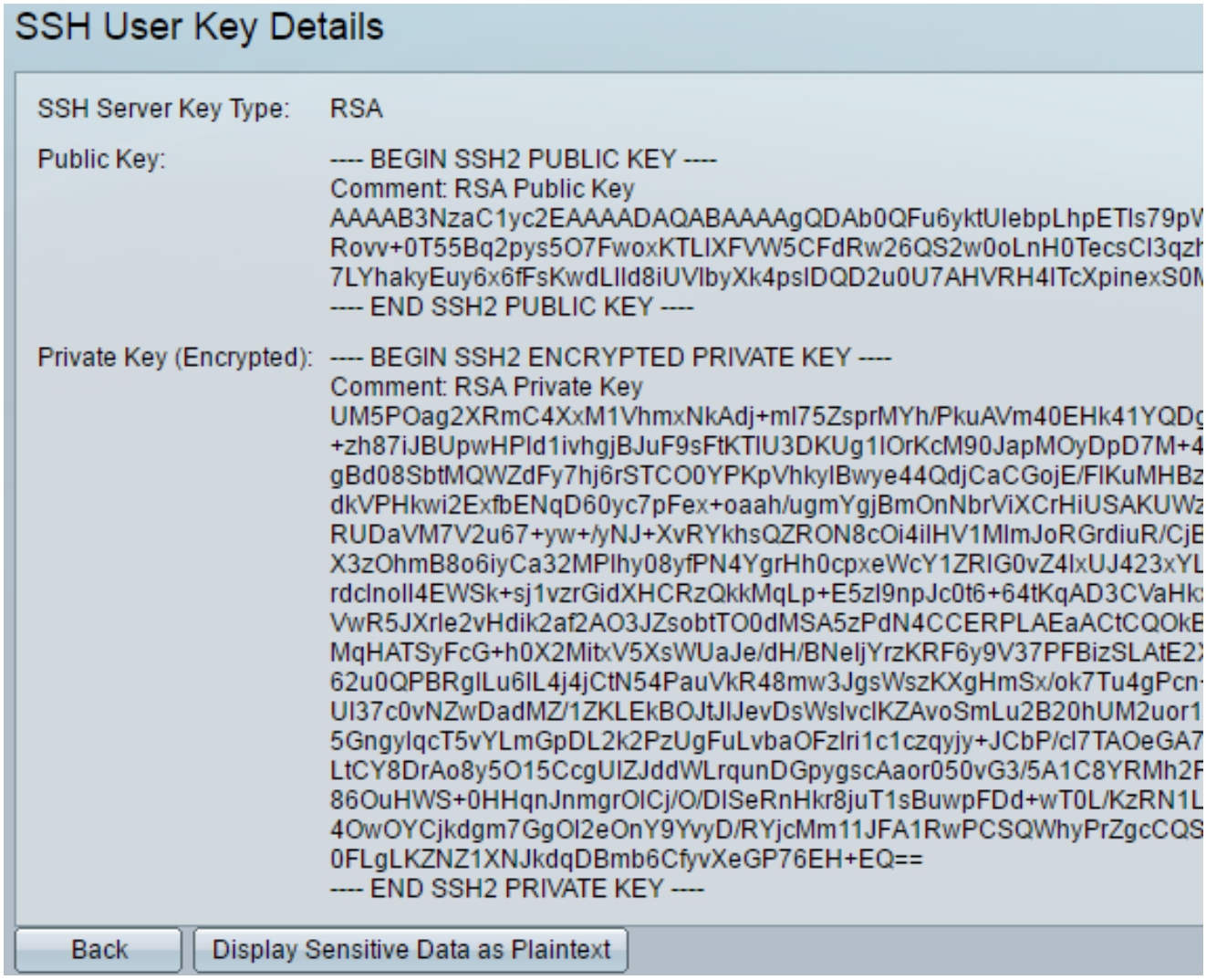
Passaggio 16. (Facoltativo) Fare clic su **Elimina** per eliminare la chiave selezionata.



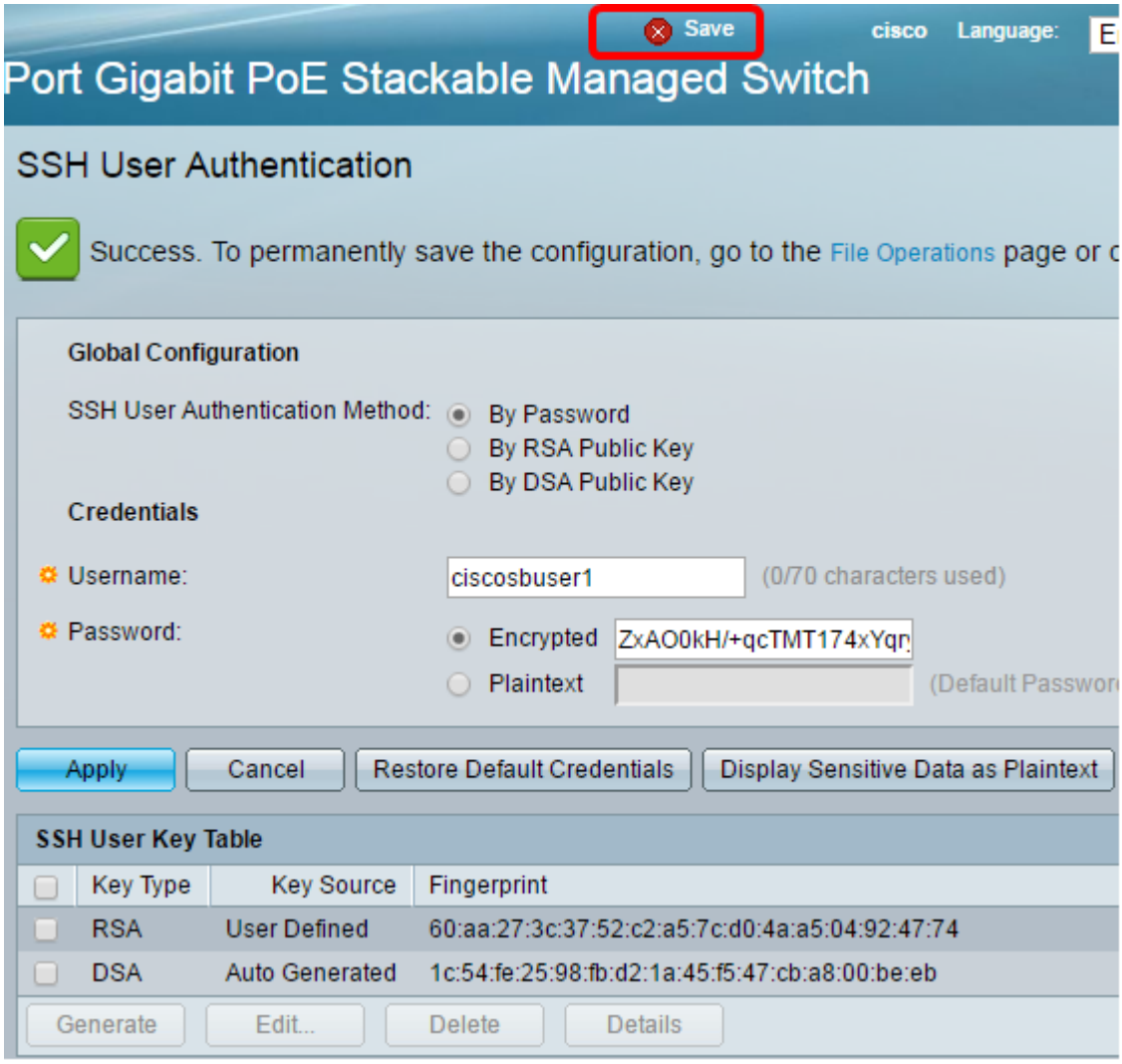
Passaggio 17. (Facoltativo) Quando richiesto da un messaggio di conferma, come mostrato di seguito, fare clic su **OK** per eliminare la chiave.



Passaggio 18. (Facoltativo) Fare clic su **Dettagli** per visualizzare i dettagli della chiave selezionata.



Passaggio 19. (Facoltativo) Fare clic sul pulsante **Save** nella parte superiore della pagina per salvare le modifiche nel file della configurazione di avvio.



A questo punto, è necessario configurare le impostazioni di autenticazione degli utenti client sullo switch gestito.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).