Impostazioni di autenticazione utente client Secure Shell (SSH) sugli switch impilabili serie Sx500

Obiettivo

La funzionalità server Secure Shell (SSH) permette di stabilire una sessione SSH con gli switch impilabili della serie Sx500. Una sessione SSH è proprio come una sessione telnet, ma è più sicura. La protezione viene ottenuta dal dispositivo quando genera automaticamente le chiavi pubbliche e private. Questi tasti possono anche essere modificati dall'utente. È possibile aprire una sessione SSH utilizzando l'applicazione PuTTy.

In questo documento viene spiegato come selezionare il metodo di autenticazione per un client SSH. Inoltre, viene spiegato come configurare un nome utente e una password per il client SSH sugli switch impilabili serie Sx500.

Dispositivi interessati

·Switch Stack Serie Sx500

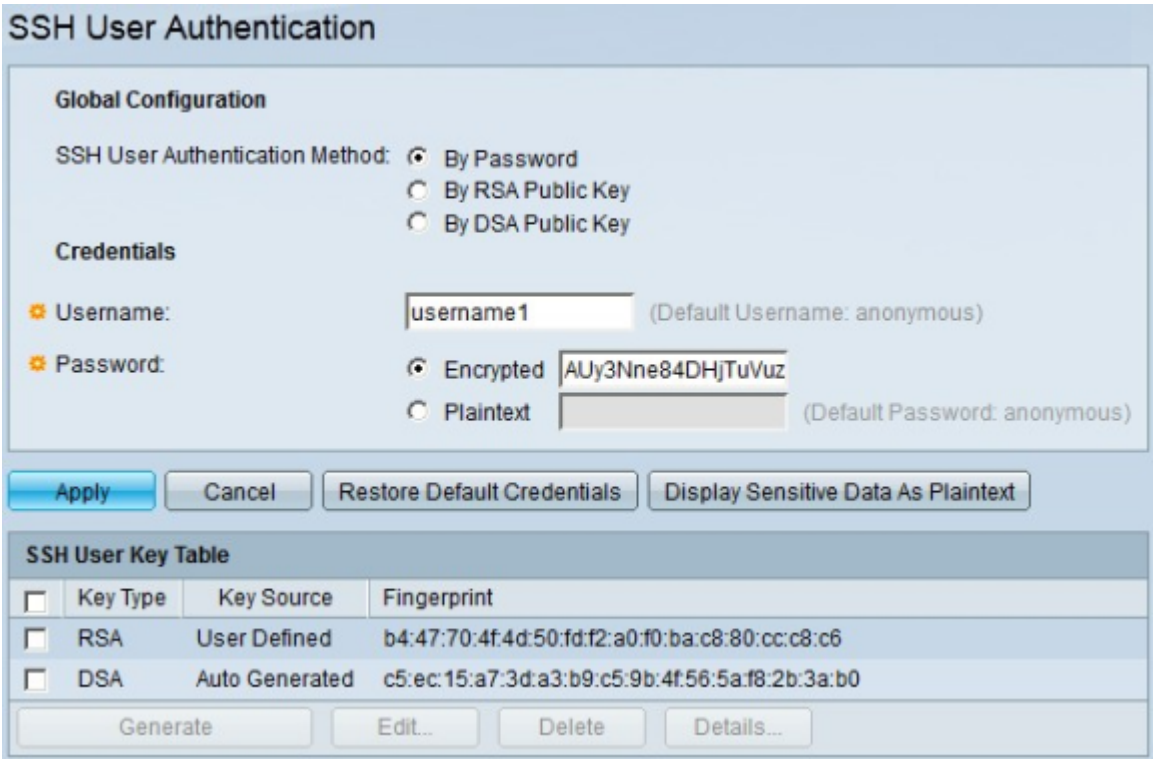
Versione del software

•1.3.0.62

Configurazione autenticazione utente SSH client

Questa sezione spiega come configurare l'autenticazione dell'utente sugli switch impilabili della serie Sx500.

Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Security > SSH Client > SSH User Authentication** (Sicurezza > Client SSH > Autenticazione utente SSH). Viene visualizzata la pagina *SSH User Authentication*:



Passaggio 2. Nell'area Global Configuration, fare clic sul pulsante di opzione per il metodo di autenticazione utente SSH desiderato. Le opzioni disponibili sono:

·Per password - Questa opzione consente di configurare una password per l'autenticazione utente

·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.

·Per chiave pubblica DSA: questa opzione consente di utilizzare una chiave pubblica DSA per l'autenticazione utente. DSA è solo per la firma.

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

Passaggio 4. Se nel Passaggio 2 è stato scelto Per password, nel campo Password fare clic sul metodo per immettere la password. Le opzioni disponibili sono:

·Crittografato - Questa opzione consente di immettere una password crittografata.

·Testo normale - Questa opzione consente di immettere una password in testo normale. Viene immesso testo normale che consente di accedere al dispositivo e visualizzare la password se si dimentica.

Passaggio 5. Fare clic su **Applica** per salvare la configurazione di autenticazione.

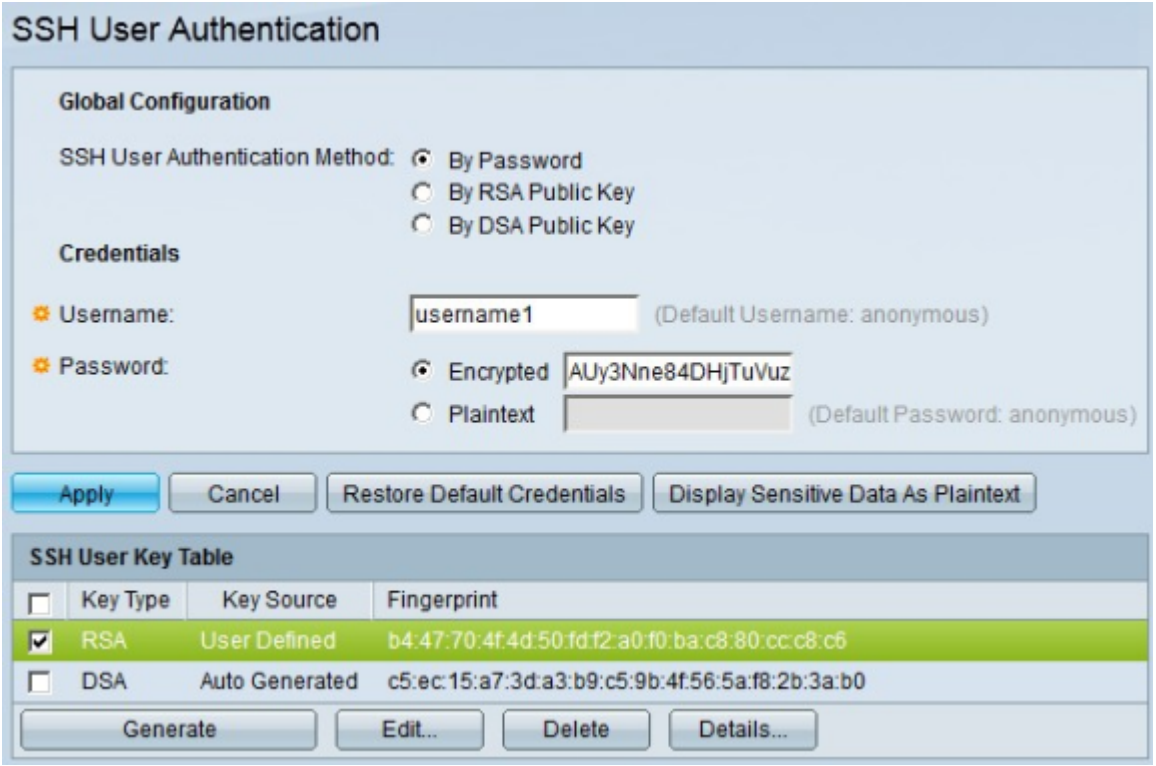
Passaggio 6. (Facoltativo) Per ripristinare il nome utente e la password predefiniti, fare clic su **Ripristina credenziali predefinite.**

Passaggio 7. (Facoltativo) Per visualizzare i dati riservati della pagina in formato testo normale, fare clic su **Visualizza dati riservati come testo normale**.

Tabella chiavi utente SSH

Questa sezione spiega come gestire la tabella utenti SSH sugli switch impilabili serie Sx500.

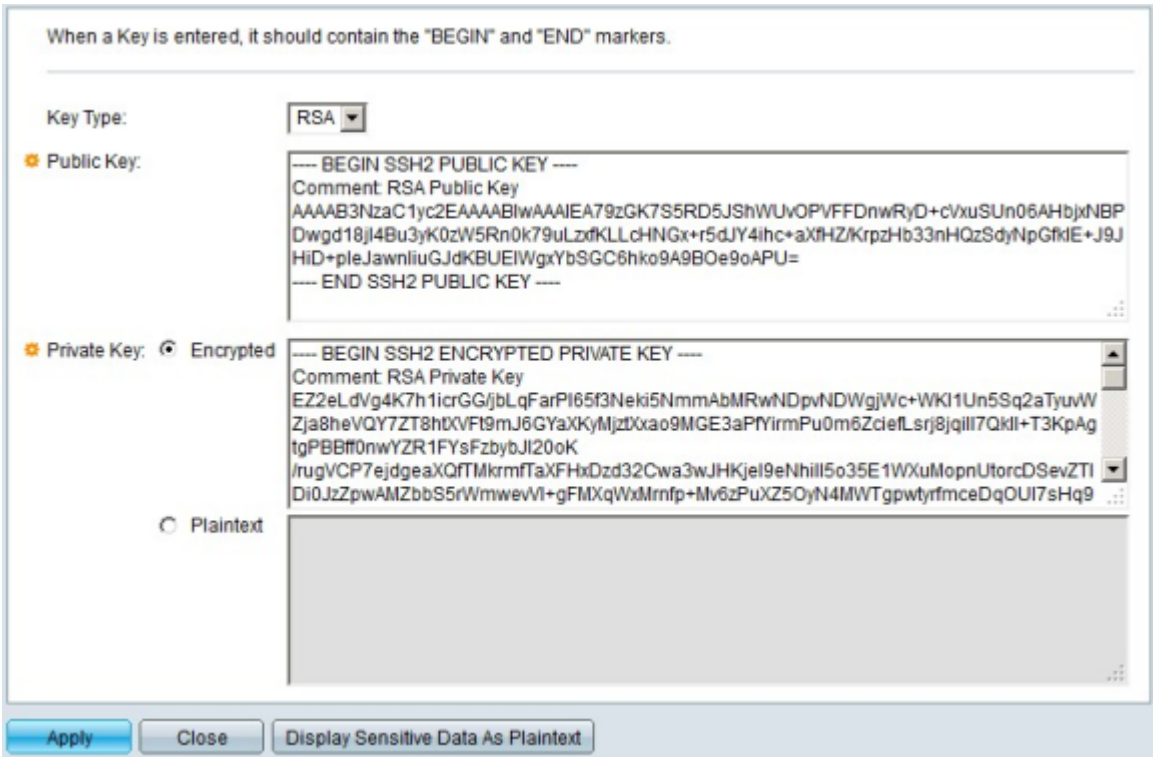
Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Security > SSH Client > SSH User Authentication** (Sicurezza > Client SSH > Autenticazione utente SSH). Viene visualizzata la pagina *SSH User Authentication*:



Passaggio 2. Selezionare la casella di controllo della chiave che si desidera gestire.

Passaggio 3. (Facoltativo) Per generare una nuova chiave, fare clic su **Genera**. La nuova chiave sostituisce la chiave selezionata.

Passaggio 4. (Facoltativo) Per modificare una chiave corrente, fare clic su **Modifica**. Viene visualizzata la finestra *Edit SSH Client Authentication Settings*.



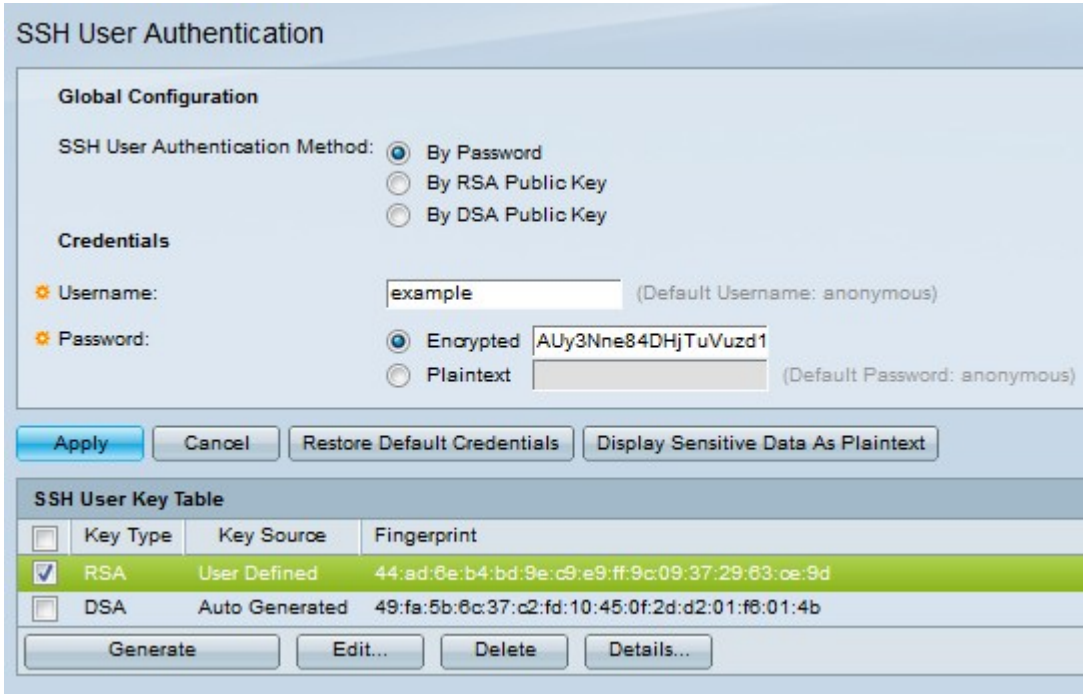
Le opzioni che è possibile modificare sono:

·Tipo di chiave: questa opzione consente di scegliere dall'elenco a discesa Tipo di chiave il tipo di chiave desiderato. È possibile scegliere RSA o DSA come tipo di chiave. RSA è utilizzato per la crittografia e la firma, mentre DSA è utilizzato solo per la firma.

·Chiave pubblica: in questo campo è possibile modificare la chiave pubblica corrente.

·Chiave privata: in questo campo 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 5. Fare clic su **Applica** per salvare le modifiche.



Passaggio 6. (Facoltativo) Per eliminare il tasto selezionato, fare clic su **Elimina**.

Passaggio 7. (Facoltativo) Per visualizzare i dettagli della chiave selezionata, fare clic su **Dettagli**. Di seguito è riportata un'immagine con i dettagli del codice utente.

SSH User Key Details

SSH Server Key Type:	RSA
Public Key:	---- BEGIN SSH2 PUBLIC KEY ---- Comment: RSA Public Key AAAAB3NzaC1yc2EAAAABIwAAAIEAzzGyPuoBcoaNa32Pk2ELNNt7UaGR5xFEPoH7 JdGj3Lto7UfkRAM9XIvai9Xua/B4pU1fCL /I2ZFjGVgTs7UUsNOjjuOtRSopHR8udhUGqgdzA4hHQycvCGy8OIuRYNIU0q6UHWW7 6NX+jnD4WphJxeYCKx2AIWzmsu14p6GQ2Ec= ---- END SSH2 PUBLIC KEY ----
Private Key (Encrypted):	---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---- Comment: RSA Private Key mF32KmMsoyqrru/46gXYvYHa8i4GpPchdIzh7fQDyx5+zAXxJ8skn3bAo /brrX7Nshm5zf0SPgbRGmdWXAfO3o0AZUaE/pHcPfpTE3Ilyu6Qtjfob64S /kJKYwfvZhRvU4g6hIBfZnCDXz0H1mgXvzoYBpkqxq8ZIdTdYOIRW+3W25z8+ez2r /LycEtNyEziv0RGhCfSZzat3PGCpNX9IH1DY9asfNAnIKDcRvqOnIO4hcBY+aCirtSs3wS xtYPS1m3rBUdhUB0X4m/bzH1qJJP6dLuxZAVsrNRY1XmK3WGjxsyNGsUgC /2dEmPZodIstKTv4xg13hux78rzd3u072ofCSRmEuO166S2JNNR1IRLcVOI /PKVv1pfuuZUDDm0qmegr8sDvWFXkDbeWPisOvRQXO3Yk2D94TiW1sFpW0B4zB9nN QMsO4/dQnI/Qa5ofk/ObzwVNmmaNhXdK /TYPXRQGJEz9McLc641VNYmKWpBELTqS /vujygonYqDpgUw2XJlxZ9nmhp1mYteqINTUNVv4QNnssc9no5YoffPdyNEuox9L0rmT LgNaIpdo5R6CP7hyN0Ao9wGgBMwnq6dz2fUSpIhu2vqNULmaRgUIKR2bVtmSBWuX S8CRtDFnt3qB3UMRLouMssWWEuGfCJaAA7zhDbeqDRuct /EiPWLgzYBqGbCvTB4EZtbbIQebmFphnqxc3X7CuxmU9klwUrkZTVhjoQb7rjySbCybP w47xpxi5/6u6A6kyhC+/wpWBId6C4UO2u/9C7zDJSnho5w+anL6 /1tl6p06lkwn+hCsqZJA9kphmaq5NjUscQadZqQtz4w5s8kVpjT3Ify5NZr2KB030Qi9ICsP O+ao1vhnfBSPfu8Rt/8fPXVQyfhXvYG /RI6aDIho3+pL7VUdqZ7u4CyYB+pnrZ5psX9I6qRuGfqiTDMSiZyWY /p+J6IhLfYwKfI3Lj2wpeggRwI4HUiZpGr+0S5O51ot8+1ItlkFhcqA1+Z3C9Sh7TvNyBGI gbLqLPsXxz2xAHIzH8 /NK7EquMs0Ob52DPJ79vNeJjtjfNAvPjwDkCunkEzjoo3LYxIiE3DtMCBAcVPUEGncKK hCA== ---- END SSH2 PRIVATE KEY ----

Back | Display Sensitive Data As Plaintext