Secure Shell (SSH) Client User Authentication-Einstellungen auf Stackable Switches der Serie Sx500

Ziel

Mit der SSH-Serverfunktion (Secure Shell) können Sie eine SSH-Sitzung mit den Stackable Switches der Serie Sx500 einrichten. Eine SSH-Sitzung ist wie eine Telnet-Sitzung, aber sie ist sicherer. Die Sicherheit wird vom Gerät abgerufen, wenn die öffentlichen und privaten Schlüssel automatisch generiert werden. Diese Schlüssel können auch vom Benutzer geändert werden. Eine SSH-Sitzung kann mithilfe der PuTTY-Anwendung geöffnet werden.

Dieser Artikel enthält Informationen zur Auswahl der Authentifizierungsmethode für einen SSH-Client. Außerdem wird erläutert, wie Sie auf Stackable Switches der Serie Sx500 einen Benutzernamen und ein Kennwort für den SSH-Client einrichten.

Anwendbare Geräte

·Stackable Switches der Serie Sx500

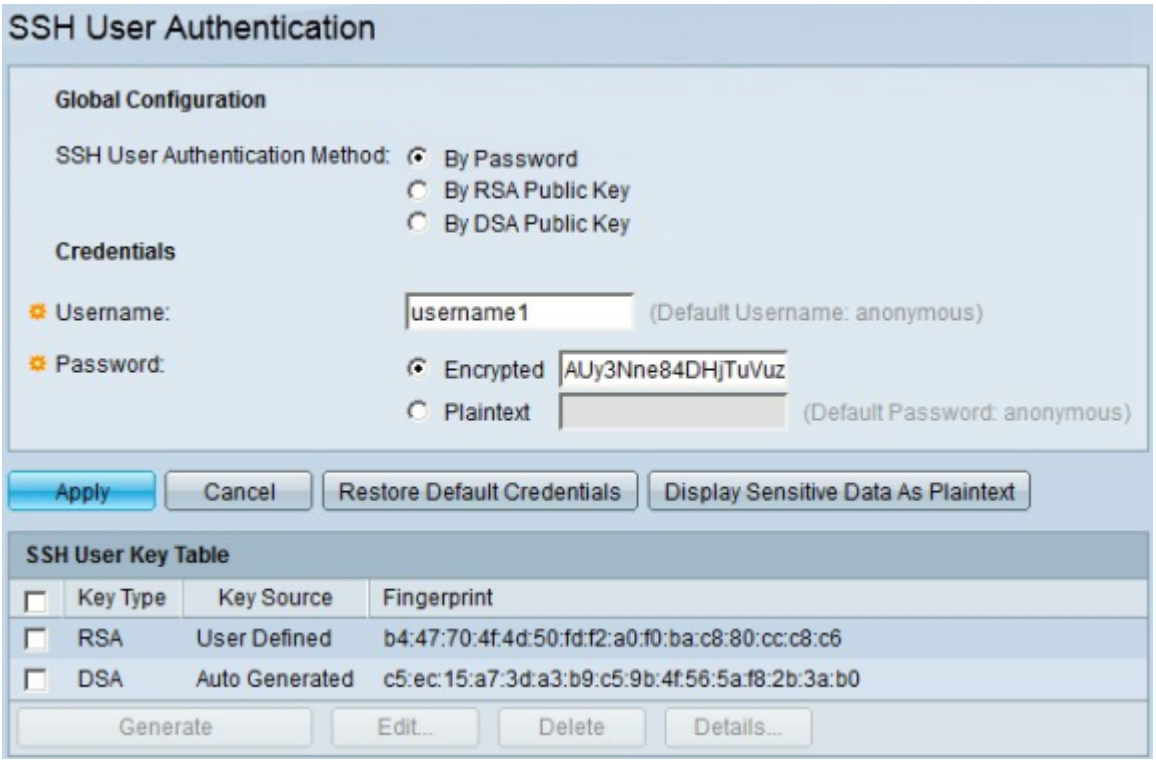
Softwareversion

·1.3.0.62

Client SSH-Benutzerauthentifizierungskonfiguration

In diesem Abschnitt wird erläutert, wie Sie die Benutzerauthentifizierung für die Stackable Switches der Serie Sx500 konfigurieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > SSH Client > SSH User Authentication aus**. Die Seite *SSH-Benutzerauthentifizierung* wird geöffnet:



Schritt 2: Klicken Sie im Bereich "Globale Konfiguration" auf das Optionsfeld für die gewünschte SSH-Benutzerauthentifizierungsmethode. Folgende Optionen stehen zur Verfügung:

·By Password (Kennwort): Mit dieser Option können Sie ein Kennwort für die Benutzerauthentifizierung konfigurieren.

·By RSA Public Key (Öffentlicher RSA-Schlüssel): Mit dieser Option können Sie einen öffentlichen RSA-Schlüssel für die Benutzerauthentifizierung verwenden. RSA wird für Verschlüsselung und Signierung verwendet.

·By DSA Public Key (Öffentlicher DSA-Schlüssel): Mit dieser Option können Sie einen öffentlichen DSA-Schlüssel für die Benutzerauthentifizierung verwenden. DSA dient nur zur Signierung.

Schritt 3: Geben Sie im Bereich Anmeldeinformationen im Feld Benutzername den Benutzernamen ein.

Schritt 4: Wenn Sie in Schritt 2 die Option By Password (Kennwort) ausgewählt haben, klicken Sie im Feld Password (Kennwort) auf die Methode zur Eingabe des Kennworts. Folgende Optionen stehen zur Verfügung:

·Encrypted (Verschlüsselt) - Mit dieser Option können Sie ein verschlüsseltes Kennwort eingeben.

·Plaintext: Mit dieser Option können Sie ein Passwort im Klartext eingeben. Einfach Text wird eingegeben, damit Sie sich beim Gerät anmelden und das Passwort anzeigen können, wenn Sie es vergessen.

Schritt 5: Klicken Sie auf **Apply**, um die Authentifizierungskonfiguration zu speichern.

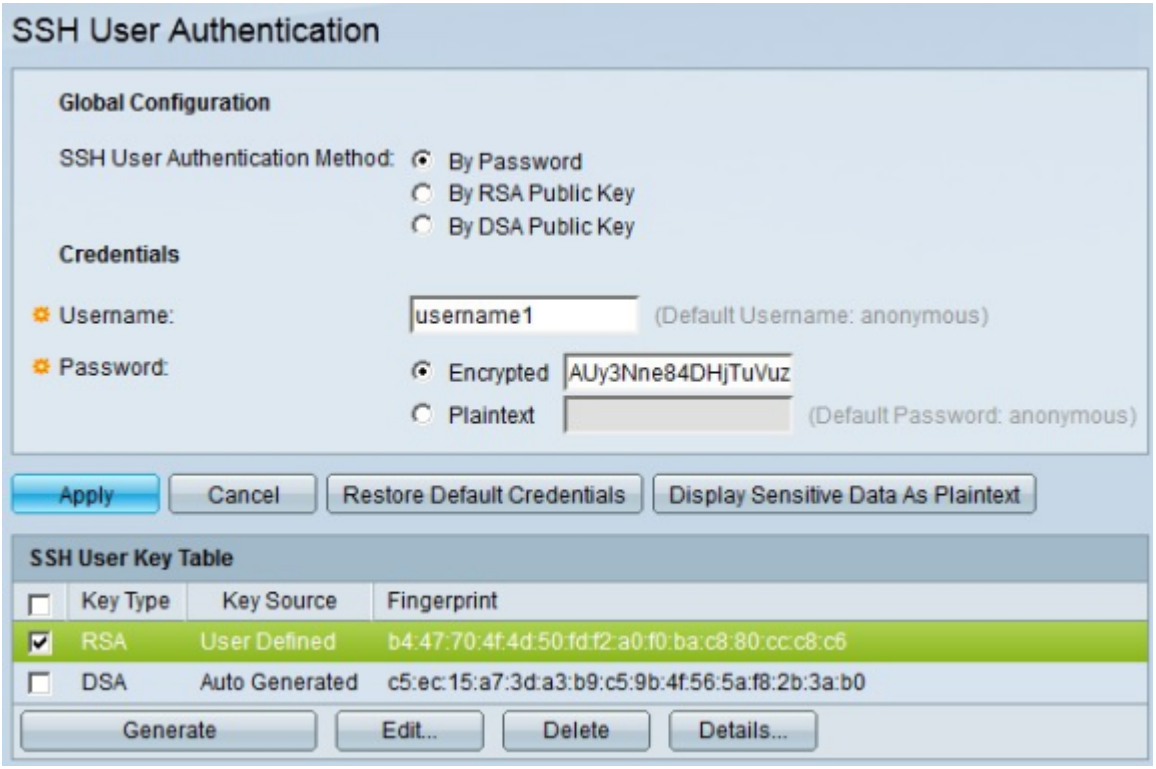
Schritt 6: (Optional) Um den Standardbenutzernamen und das Standardkennwort wiederherzustellen, klicken Sie auf **Standardanmeldeinformationen wiederherstellen.**

Schritt 7: (Optional) Um die vertraulichen Daten der Seite im Textformat anzuzeigen, klicken Sie auf **Sensitive Daten als Nur-Text anzeigen**.

SSH-Benutzerschlüsseltabelle

In diesem Abschnitt wird erläutert, wie die SSH-Benutzertabelle auf den Stackable Switches der Serie Sx500 verwaltet wird.

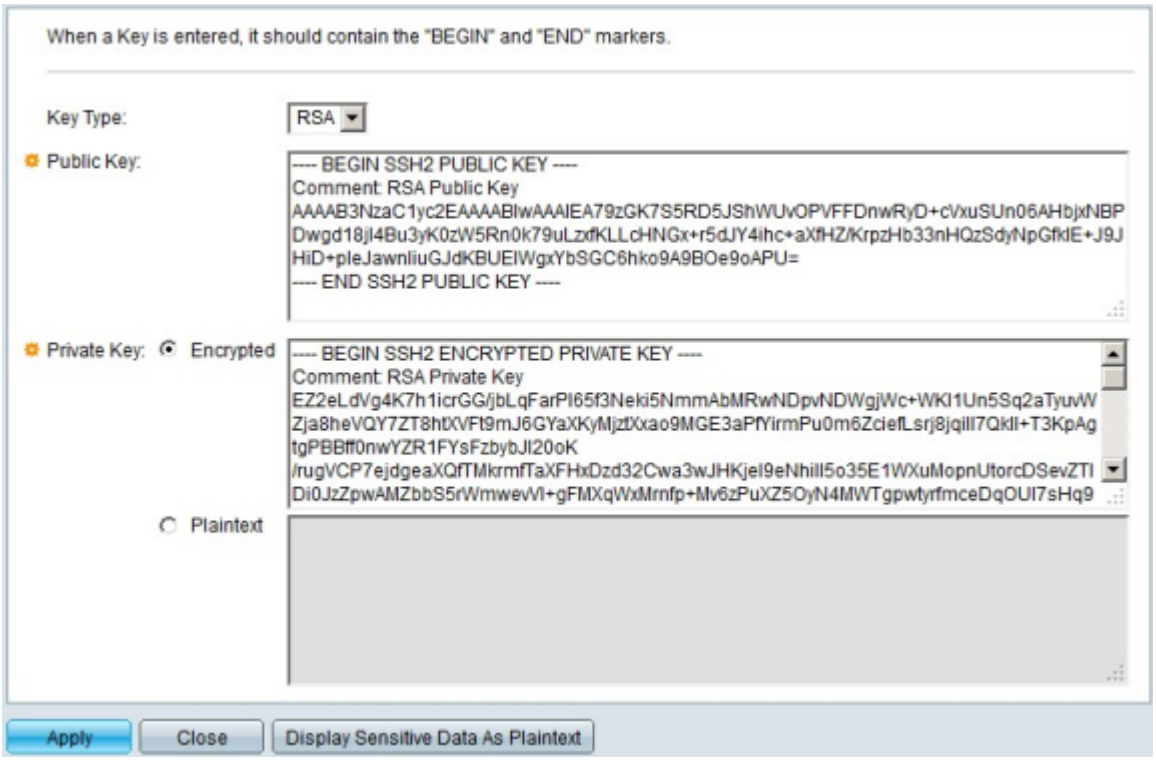
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > SSH Client > SSH User Authentication aus**. Die Seite *SSH-Benutzerauthentifizierung* wird geöffnet:



Schritt 2: Aktivieren Sie das Kontrollkästchen des Schlüssels, den Sie verwalten möchten.

Schritt 3: (Optional) Klicken Sie auf **Generieren**, um einen neuen Schlüssel zu generieren. Der neue Schlüssel überschreibt den aktivierten Schlüssel.

Schritt 4: (Optional) Um einen aktuellen Schlüssel zu bearbeiten, klicken Sie auf **Bearbeiten**. Das Fenster *Einstellungen für die SSH-Client-Authentifizierung bearbeiten* wird angezeigt.



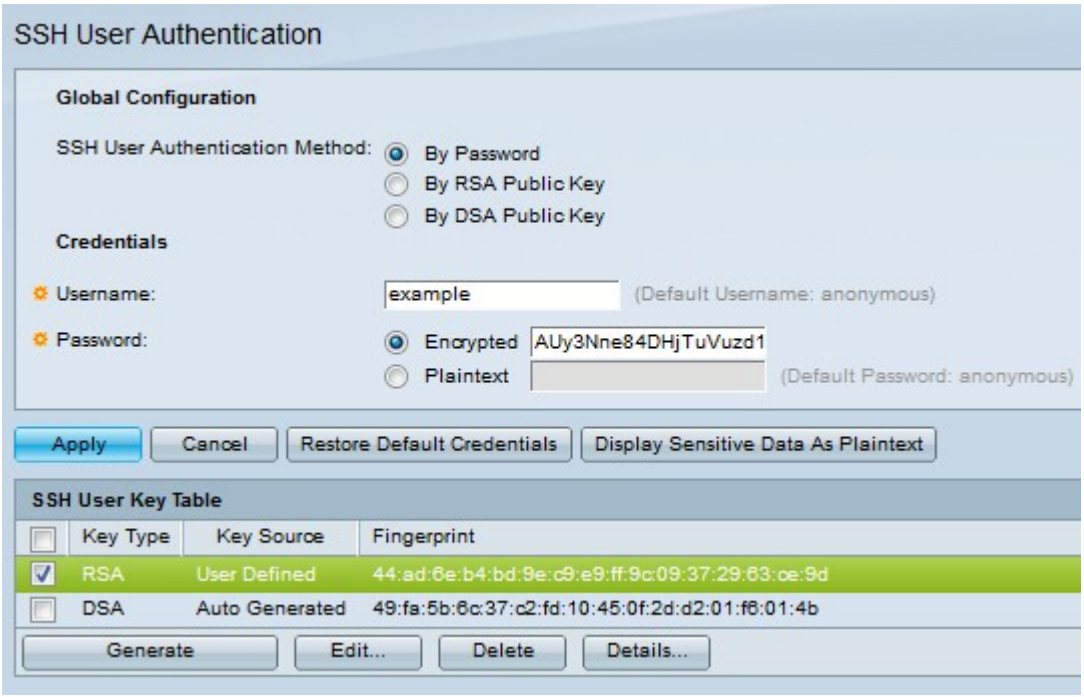
Sie können folgende Optionen bearbeiten:

·Key Type (Schlüsseltyp): Mit dieser Option können Sie in der Dropdown-Liste Key Type (Schlüsseltyp) den Schlüsseltyp Ihrer Präferenz auswählen. Sie können RSA oder DSA als Schlüsseltyp auswählen. RSA wird für die Verschlüsselung und Signierung verwendet, während DSA nur für die Signierung verwendet wird.

·Öffentlicher Schlüssel: In diesem Feld können Sie den aktuellen öffentlichen Schlüssel bearbeiten.

·Privater Schlüssel - In diesem Feld können Sie den privaten Schlüssel bearbeiten und auf **Verschlüsselt** klicken, um den aktuellen privaten Schlüssel als verschlüsselten Text anzuzeigen, oder **Nur-Text**, um den aktuellen privaten Schlüssel im Klartext anzuzeigen.

Schritt 5: Klicken Sie auf **Apply**, um die Änderungen zu speichern.



Schritt 6: (Optional) Um den aktivierten Schlüssel zu löschen, klicken Sie auf **Löschen**.

Schritt 7: (Optional) Klicken Sie auf **Details**, um die Details des aktivierten Schlüssels anzuzeigen. Unten sehen Sie ein Bild der Details des Benutzerschlüssels.