

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:

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (Default Username: anonymous)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	b4:47:70:4f:4d:50:fd:f2:a0:f0:ba:c8:80:cc:c8:c6
<input type="checkbox"/>	DSA	Auto Generated	c5:ec:15:a7:3d:a3:b9:c5:9b:4f:56:5a:f8:2b:3a:b0

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:

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (Default Username: anonymous)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	b4:47:70:4f:4d:50:fd:f2:a0:f0:ba:c8:80:cc:c8:c6
<input type="checkbox"/>	DSA	Auto Generated	c5:ec:15:a7:3d:a3:b9:c5:9b:4f:56:5a:f8:2b:3a:b0

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.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEA79zGK7S5RD5JShWUvOPVFFDnwRyD+cVxuSUn06AHbjxNBP
Dwgd18Jl4Bu3yK0zW5Rn0k79uLzdfKLLcHNGx+r5dJY4ihc+aXfHZKrpzHb33nHQzSdyNpGfkiE+J9J
HiD+pleJawnliuGJdKBUEIWgxYbSGC6hko9A9BOe9oAPU=
---- END SSH2 PUBLIC KEY ----

```

Private Key: Encrypted

```

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
EZ2eLdVg4K7h1icrGGjblqFarPI65f3Neki5NmmAbMRwNDpvNDWgjWc+WkI1Un5Sq2aTyuvW
Zja8heVQY7ZT8h0vF19mJ6GYaXkYmJztXxao9MGE3aPYirmPu0m6ZciefLsrj8jqill7QkII+T3KpAg
tgPBBff0nwYZR1FYsFzbybJI20oK
/rugVCP7ejdgeaXQfTMkrmfTaXFHxDzd32Cwa3wJHKjel9eNhill5o35E1WxuMopnUtorcDSevZTI
Di0JzZpwAMZbbS5rWmwewVI+gFMXqWxMrnfp+Mv6zPuXZ5OyN4MWTgpwtyrfmceDqOUI7sHq9

```

Plaintext

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.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (Default Username: anonymous)
Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply

Cancel

Restore Default Credentials

Display Sensitive Data As Plaintext

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	44:ad:6e:b4:bd:9e:c9:e9:ff:9c:09:37:29:63:ce:9d
<input type="checkbox"/>	DSA	Auto Generated	49:fa:5b:6c:37:c2:fd:10:45:0f:2d:d2:01:f8:01:4b

Generate Edit... Delete Details...

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.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: --- BEGIN SSH2 PUBLIC KEY ---
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzzGyPuoBcoaNa32Pk2ELNnt7UaGR5xFEPoH7
JdGj3Lto7UfkRAM9XlvaI9Xua/B4pU1fCL
/I2ZFjGVgTs7UUsNOjjuOTRSopHR8udhUGqgdzA4hHQyovCGy8OIuRYNIU0q6UHWW7
6NX+jnD4WphJxeYCKx2AIWzmsu14p6GQ2Eo=
--- END SSH2 PUBLIC KEY ---

Private Key (Encrypted): --- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---
Comment: RSA Private Key
mF32KmMsoyqrru/46gXYvYHa8i4GpPchdlzh7fQDyx5+zAXxJ6skn3bAo
/brX7Nshm5zf0SPgbRGmdWXAfo3o0AZUaE/pHcPfpTE3Ilyu6QtjfoB64S
/kJKYwfvZhrVU4g6hIBfZnCDXz0H1mgXvzoYBpkqxq8ZldTdYOIRW+3W25z8+ez2r
/LycEtNyEziv0RGhCfSZat3PGCpNX9IH1DY9asfNAnIKDcRvqOnIO4hcBY+aCirtSs3wS
xtYPS1m3rBUdhUBOX4m/bzH1qJJP6dLuxZAVsrNRY1Xmk3WGjxxyNGsUgC
/2dEmPZodIstKtV4xg13hux78rzd3u072ofCSRmEuO166S2JNNR1IRLcVOI
/PKVv1pfuuZUDDm0qmegr8sDvWFxkDbeWPisOvRQXO3Yk2D94TiW1sFpW0B4zB9nN
QMsO4/dQnl/Qa5ofk/ObzwVNmmaNhXdK
/TYPXRQGEz9McLc641VNYmKWpBELTqS
/vujygonYqDpgUw2XJlxZ9nmhp1mYteqINTUNVv4QNnssc9no5YoffPdyNEuox9L0rmT
LgNaIpdo5R6CP7hyN0Ao9wGgBMwnq6dz2fUSplhu2vqNULmaRgUIKR2bVtmSBWuX
S8CRtDFnt3qB3UMRLouMssWWEuGfCJaAA7zhDbeqDRuct
/EiPWLgzYBqGbcvTB4EZtbbIQebmFphnqxc3X7CuxmU9klwUrkZTVhjoQb7rjySbCybP
w47xpxi5/6u6A6kyhC+/wpWBld6C4UO2u/9C7zDJSnho5w+anL6
/1tl6p06lkwn+hCsQZJA9kphmaq5NjUscQadZqQtz4w5s8kvpjT3lfy5NZr2KB030Qi9CsP
O+ao1vhnfBSPfu8Rt/8fPXVQyfhXvYG
/RI6aDIho3+pL7VUdqZ7u4CyYB+pnrZ5psX9I6qRuGfqiTDMSiZyWY
/p+J6lhLfYwKfl3Lj2wpeggRwl4HUiZpGr+0S5O51ot8+1ItIkFhoqA1+Z3C9Sh7TvnYBGI
gbLqLPsXxz2xAHizH8
/NK7EquMs0Ob52DPJ79vNeJjtfnAvPjwDkCunkEzjoo3LYxliE3DtMCBAcVPUEGndKK
hCA==
--- END SSH2 PRIVATE KEY ---

Back

Display Sensitive Data As Plaintext