

Secure Shell (SSH) Server Authentication Configuration for SSH Clients on Sx500 Series Stackable Switches

Objective

The Secure Shell (SSH) server feature allows the user to establish a SSH session with the Sx500 Series Stackable Switches. An SSH session is just like a telnet session, but an SSH session is more secure. The security is obtained by the device when it generates the public and private keys automatically. These keys can also be changed by the user. An SSH session can be opened with the use of the PuTTY application.

This article provides information on how to enable SSH server authentication for SSH clients and define the trusted servers on Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

Software Version

- v1.2.7.76

SSH Server Authentication Configuration

Step 1. Log in to the web configuration utility and choose **Security > SSH Client > SSH Server Authentication**. The *SSH Server Authentication* page opens:



SSH Server Authentication

SSH Server Authentication: ☒ Enable

Apply Cancel

Trusted SSH Servers Table		
<input type="checkbox"/>	Server IP Address/Name	Fingerprint
<input type="checkbox"/>	192.168.1.10	fe:b8:c3:de:e0:ff:a7:f0:c3:8b:3d:ee:0f:34:ee:0e
<input type="checkbox"/>	192.168.20.1	94:3c:9e:2b:23:df:bd:53:b4:ad:f1:5f:4e:2f:9d:ba

Add... Delete

Step 2. Check **Enable** to enable the SSH server authentication.

SSH Server Authentication: ☒ Enable

Apply **Cancel**

Server IP Address/Name	Fingerprint
192.168.1.10	fe:b8:c3:de:e0:ff:a7:f0:c3:8b:3d:ee:0f:34:ee:0e
192.168.20.1	94:3c:9e:2b:23:df:bd:53:b4:ad:f1:5f:4e:2f:9d:ba

Add... **Delete**

Step 3. Click **Apply** to save the configuration.

Add Trusted SSH Server

SSH Server Authentication: ☒ Enable

Apply **Cancel**

Server IP Address/Name	Fingerprint
192.168.1.10	fe:b8:c3:de:e0:ff:a7:f0:c3:8b:3d:ee:0f:34:ee:0e
192.168.20.1	94:3c:9e:2b:23:df:bd:53:b4:ad:f1:5f:4e:2f:9d:ba

Add... **Delete**

Step 1. In the Trusted SSH Servers Table the IP address and the finger print of the SSH server can be found. Click **Add** to add the trusted ssh server. The *Add Trusted SSH Server* window appears.

Server Definition: ☒ By IP address ☐ By name

IP Version: ☐ Version 6 ☒ Version 4

IPv6 Address Type: ☐ Link Local ☐ Global

Link Local Interface: **None**

Server IP Address/Name: 192.168.1.10

Fingerprint: FE:B8:C3:DE:E0:FF:A7:F0:C3:8B:3D:EE:0F:34:EE:0E (16 pairs of hexadecimal characters)

Apply **Close**

Step 2. Click the **By IP Address** radio button to enter an IP address in the Server IP Address/Name field. Click the **By name** radio button to enter the name of the server in the Server IP Address/Name field.

Step 3. Click the **Version 4** or **Version 6** radio button to enter an IPv4 or IPv6 IP address, respectively, in the Server IP Address/Name field. IP Version 6 can only be selected if an

IPv6 address has been configured on the device.



The screenshot shows a configuration window for an SSH server. The 'Server Definition' section has 'By IP address' selected. The 'IP Version' section has 'Version 4' selected. The 'IPv6 Address Type' section has 'Link Local' and 'Global' options, both unselected. The 'Link Local Interface' dropdown is set to 'None'. The 'Server IP Address/Name' field contains '192.168.1.10' and is highlighted with a red circle. The 'Fingerprint' field contains 'FE:B8:C3:DE:E0:FF:A7:F0:C3:8b:3D:EE:0F:34:EE:0E' and is followed by the text '(16 pairs of hexadecimal characters)'. At the bottom are 'Apply' and 'Close' buttons.

Step 4. Enter an IPv4 or IPv6 IP address of the trusted SSH user in the Server IP Address/Name field.



The screenshot shows the same configuration window as before. The 'Server IP Address/Name' field still contains '192.168.1.10'. The 'Fingerprint' field now contains 'FE:B8:C3:DE:E0:FF:A7:F0:C3:8b:3D:EE:0F:34:EE:0E' and is highlighted with a red circle. The text '(16 pairs of hexadecimal characters)' is still present. The 'Apply' and 'Close' buttons are at the bottom.

Step 5. Enter 16 pairs of hexadecimal values for the fingerprint of the SSH server in the Fingerprint field. To obtain the fingerprint value of the SSH server, navigate to **Security > SSH Server > SSH Server Authentication**. This is a feature of SSH to protect against an attack where a malicious user guides the client to a different server or computer to learn the username and password of the trusted SSH server. The client is advised to check the fingerprint of the server and then enter their credentials.

Step 6. Click **Apply** to save the configuration.