Secure Shell (SSH) Client User Authentication Settings on Sx500 Series Stackable Switches

Objective

The Secure Shell (SSH) server feature enables you to establish an SSH session with the Sx500 Series Stackable Switches. An SSH session is just like a telnet session but it 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 through the use of the PuTTY application.

This article provides information on how to select the authentication method for a SSH client. It also explains how to set up a username and password for the SSH client on Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

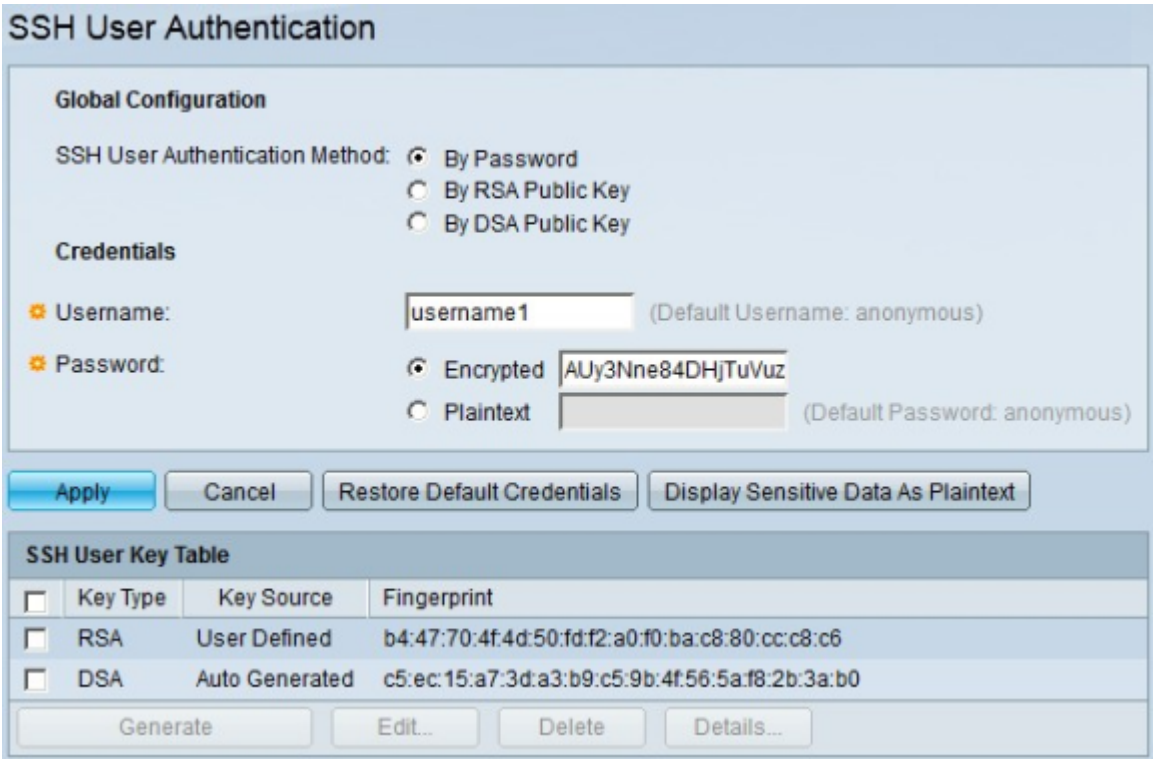
Software Version

- 1.3.0.62

Client SSH User Authentication Configuration

This section explains how to configure user authentication on the Sx500 Series Stackable Switches.

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



Step 2. In the Global Configuration area, click the radio button for the desired SSH User Authentication Method. The available options are:

- By Password — This option lets you configure a password for user authentication
- By RSA Public Key — This option lets you use an RSA public key for user authentication. RSA is used for encryption and signing.
- By DSA Public Key — This option lets you use a DSA public key for user authentication. DSA is for only signing.

Step 3. In the Credentials area, in the Username field, enter the user name.

Step 4. If you chose By Password in Step 2, then in the Password field, click the method to enter the password. The available options are:

- Encrypted — This option lets you enter an encrypted password.
- Plaintext — This option lets you enter a plain text password. Plain text is entered so that you can log in to the device and view the password if you forget.

Step 5. Click **Apply** to save your authentication configuration.

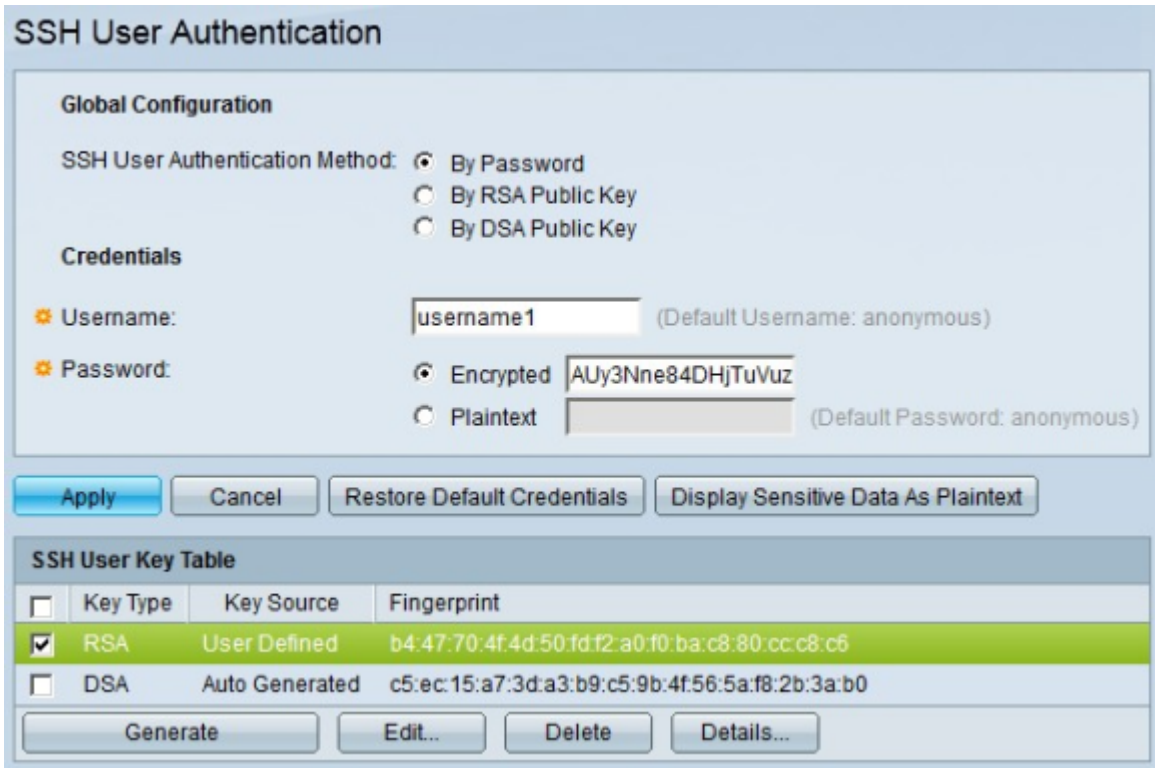
Step 6. (Optional) To restore the default username and password, click **Restore Default Credentials.**

Step 7. (Optional) To show the sensitive data of the page in plain text format, click **Display Sensitive Data as Plaintext**.

SSH User Key Table

This section explains how to manage the SSH User Table on the Sx500 Series Stackable Switches.

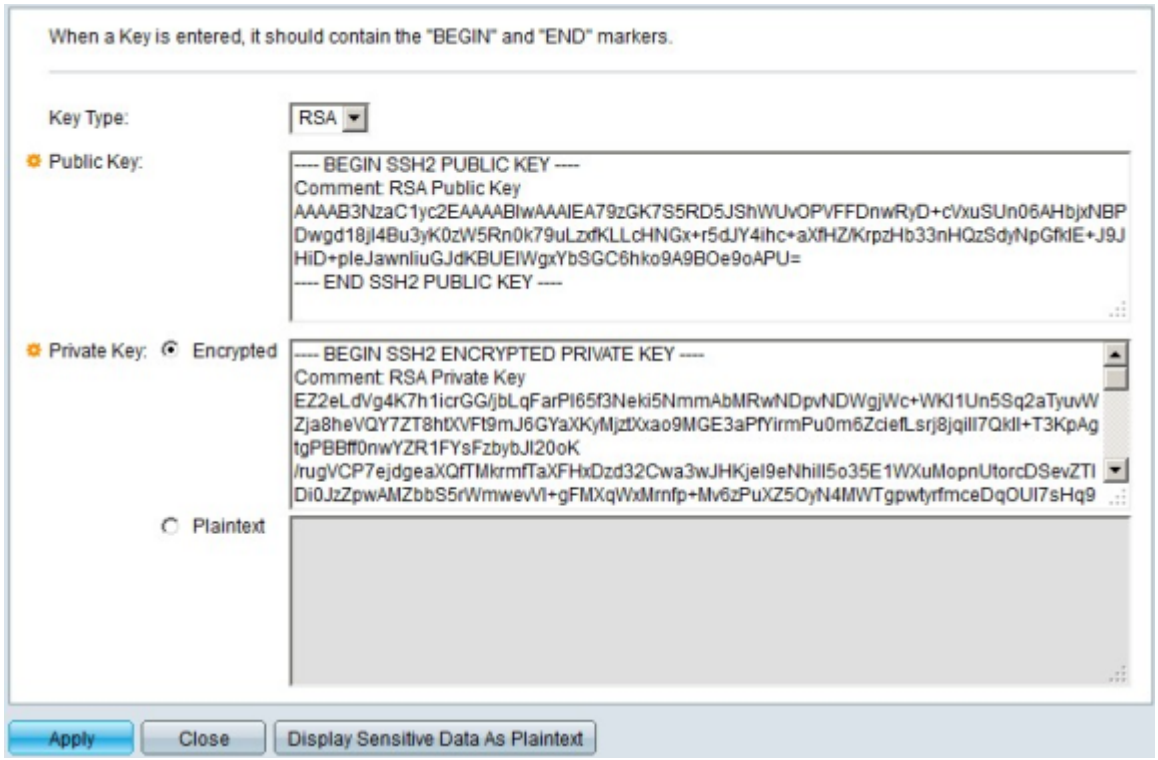
Step 1. Log in to the web configuration utility and choose **Security > SSH Client > SSH User Authentication**. The *SSH User Authentication* page opens:



Step 2. Check the check box of the key you wish to manage.

Step 3. (Optional) To generate a new key , click **Generate**. The new key overrides the checked key.

Step 4. (Optional) To edit a current key, click **Edit**. The *Edit SSH Client Authentication Settings* window appears.



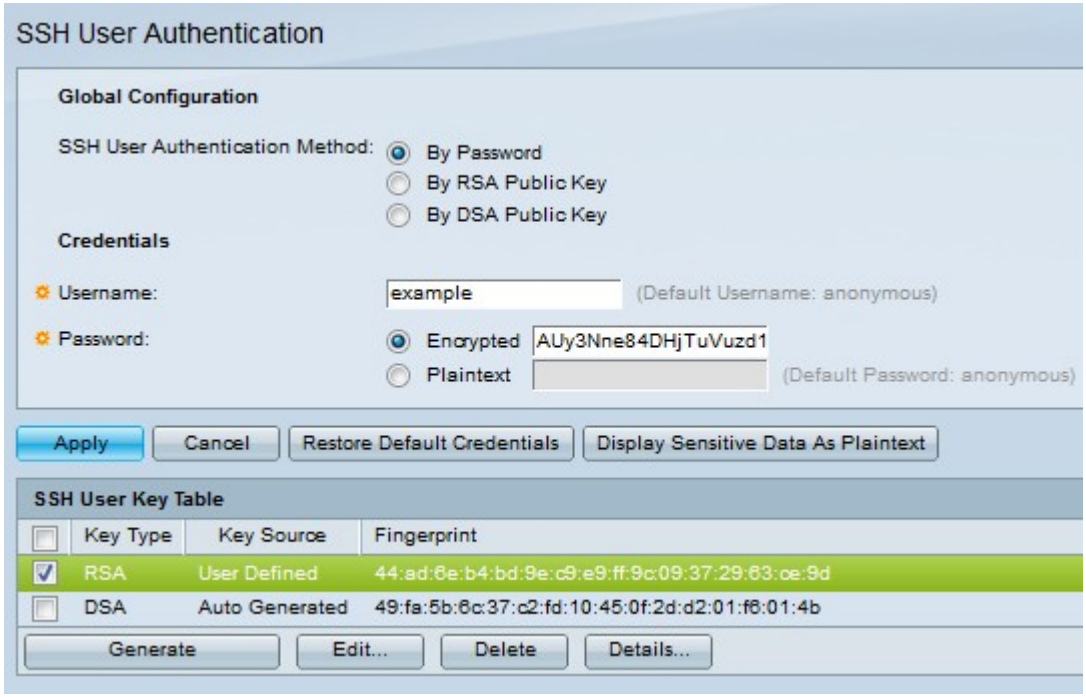
The options you can edit are:

• Key Type — This option lets you choose from the Key Type drop-down list the key type of your preference. You can choose RSA or DSA as the key type. RSA is used for encryption and signing, while DSA is for only signing.

• Public Key — In this field, you can edit the current public key.

• Private Key — In this field, you can edit the private key, and you can click **Encrypted** to see the current private key as an encrypted text, or **Plaintext** to see the current private key in plain text.

Step 5. Click **Apply** to save your changes.



Step 6. (Optional) To delete the checked key, click **Delete**.

Step 7. (Optional) To view the details of the checked key, click **Details**. Below is an image of the user key details.

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