Configure Secure Shell (SSH) User Authentication Settings on a Switch

Objective

Secure Shell (SSH) is a protocol that provides a secure remote connection to specific network devices. This connection provides functionality that is similar to a Telnet connection, except that it is encrypted. SSH allows the administrator to configure the switch through the command line interface (CLI) with a third party program.

In CLI mode via SSH, the administrator can execute more advanced configurations in a secure connection. SSH connections are useful in troubleshooting a network remotely, in cases where the network administrator is not physically present at the network site. The switch lets the administrator authenticate and manage users to connect to the network via SSH. The authentication occurs via a public key that the user can use to establish an SSH connection to a specific network.

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. It enables a device to make a secure and encrypted connection to another device that runs the SSH server. With authentication and encryption, the SSH client allows for a secure communication over an unsecure Telnet connection.

This article provides instructions on how to configure client user authentication on a managed switch.

Applicable Devices

- Sx200 Series
- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Software Version

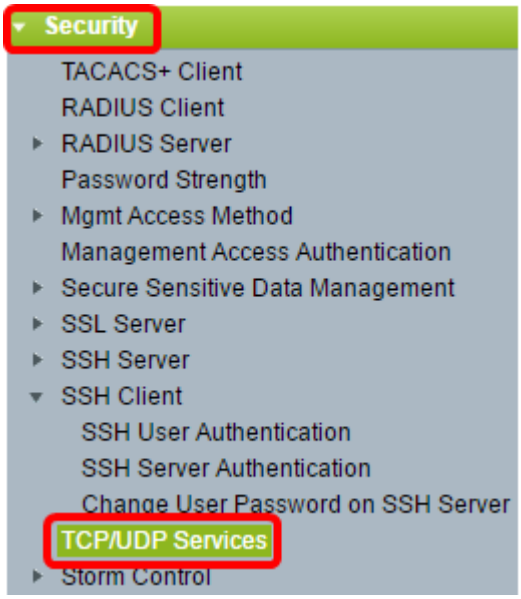
- 1.4.5.02 – Sx200 Series, Sx300 Series, Sx500 Series
- 2.2.0.66 – Sx350 Series, SG350X Series, Sx550X Series

Configure SSH Client User Authentication Settings

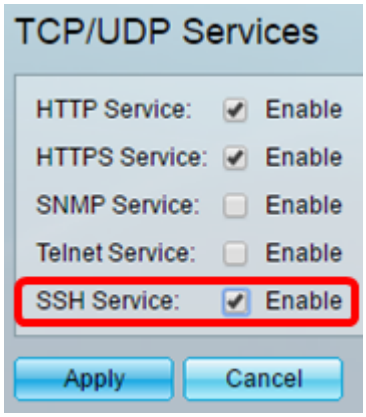
Enable SSH Service

Note: In order to support auto configuration of an out-of-box device (device with factory default configuration), SSH server authentication is disabled by default.

Step 1. Log in to the web-based utility and choose **Security > TCP/UDP Services**



Step 2. Check the **SSH Service** check box to enable access of switches command prompt through SSH.



Step 3. Click **Apply** to enable the SSH service.

Configure SSH User Authentication Settings

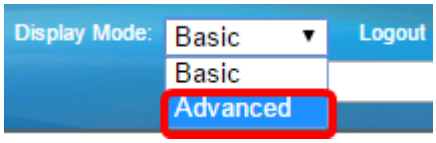
Use this page to choose an SSH user authentication method. You can set a username and password on the device if the password method is chosen. You can also generate a Ron Rivest, Adi Shamir and Leonard Adleman (RSA) or Digital Signature Algorithm (DSA) key if the public or private key method is selected.

RSA and DSA default key pairs are generated for the device when it is booted. One of these keys is used to encrypt the data being downloaded from the SSH server. The RSA key is used by default. If the user deletes one or both of these keys, they are regenerated.

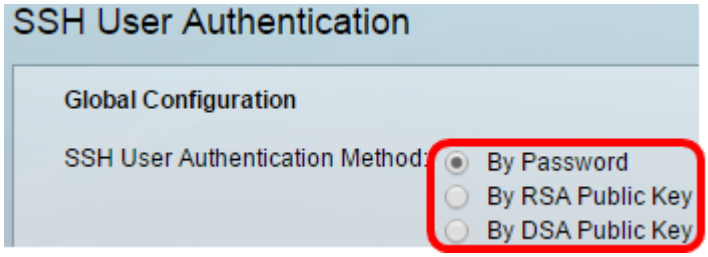
Step 1. Log in to the web-based utility and choose **Security > SSH Client > SSH User Authentication**.



Note: If you have an Sx350, SG300X, or Sx500X, switch to Advanced mode by choosing **Advanced** from the Display Mode drop-down list.



Step 2. Under Global Configuration, click the desired SSH User Authentication Method.

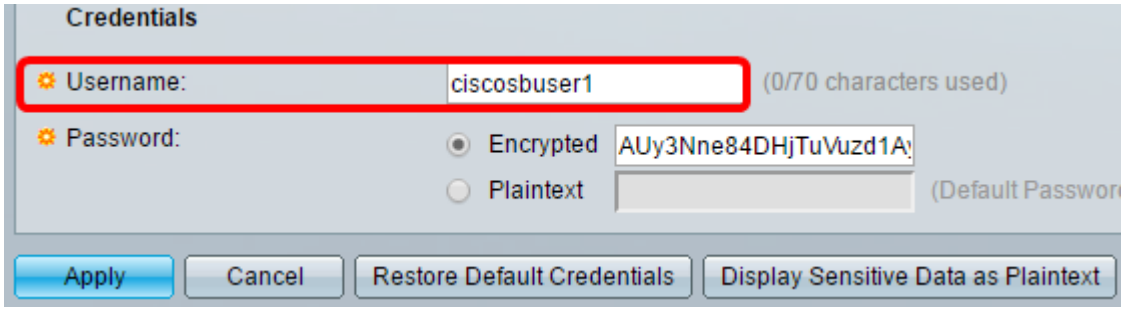


Note: When a device (SSH client) attempts to establish an SSH session to the SSH server, the SSH server uses one of the following methods for client authentication:

- By Password — This option lets you configure a password for user authentication. This is the default setting and the default password is anonymous. If this option is chosen, make sure that the username and password credentials have been established on the SSH Server.
- By RSA Public Key — This option lets you use RSA public key for user authentication. An RSA key is an encrypted key based on factorization of large integers. This key is the most common type of key used for SSH user authentication.
- By DSA Public Key — This option lets you use a DSA public key for user authentication. A DSA key is an encrypted key based on ElGamal discrete algorithm. This key is not commonly used for SSH user authentication as it takes more time in the authentication process.

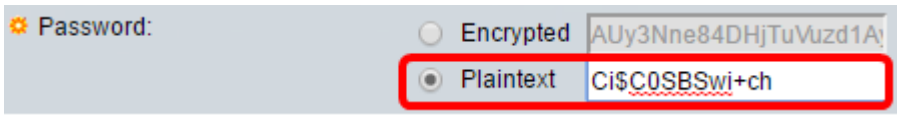
Note: In this example, By Password is chosen.

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



Note: In this example, ciscosbuser1 is used.

Step 4. (Optional) If you chose By Password in Step 2, click the method then enter the password in the *Encrypted* or *Plaintext* field.



The options are:

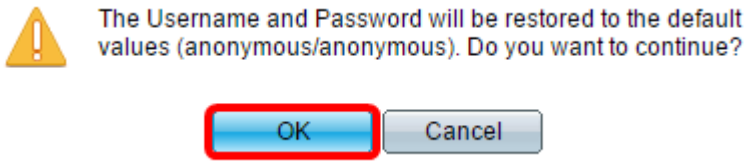
- Encrypted — This option lets you enter an encrypted version of the password.
- Plaintext — This option lets you enter a plain text password.

Note: In this example, Plaintext is chosen and a plain text password is entered.

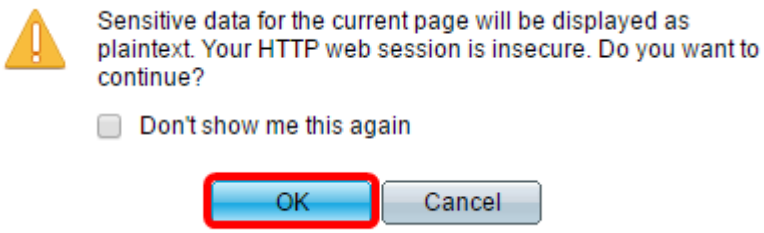
Step 5. Click **Apply** to save your authentication configuration.

Step 6. (Optional) Click **Restore Default Credentials** to restore the default user name and password then click **OK** to proceed.

Note: The username and password will be restored to the default values: anonymous/anonymous.

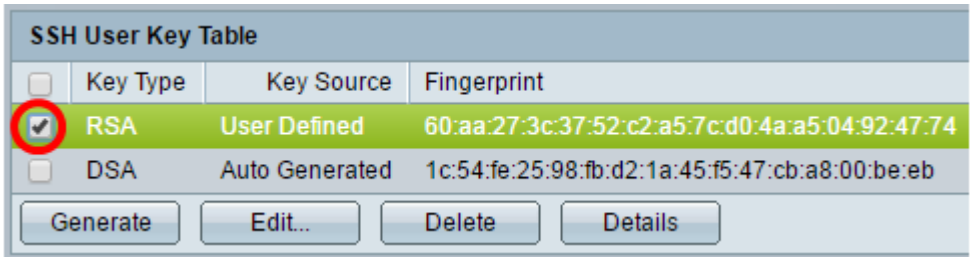


Step 7. (Optional) Click **Display Sensitive Data as Plaintext** to show the sensitive data of the page in plain text format then click **OK** to proceed.



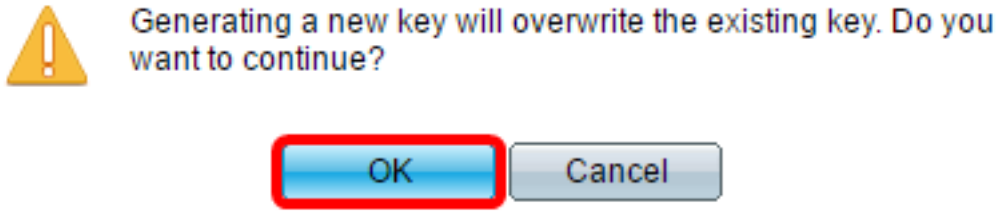
Configure SSH User Key Table

Step 8. Check the check box of the key you wish to manage.

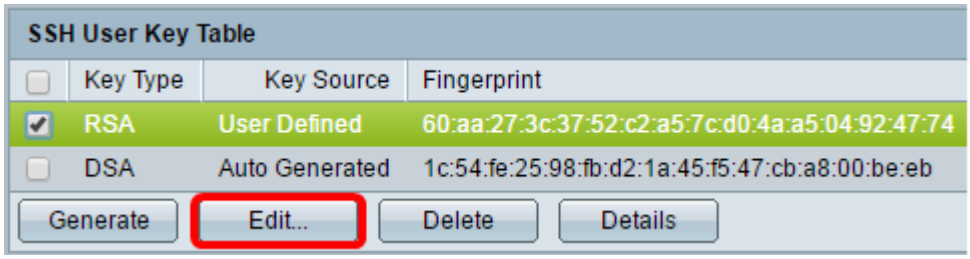


Note: In this example, RSA is chosen.

Step 9. (Optional) Click **Generate** to generate a new key. The new key will override the checked key then click **OK** to proceed.



Step 10. (Optional) Click **Edit** to edit a current key.

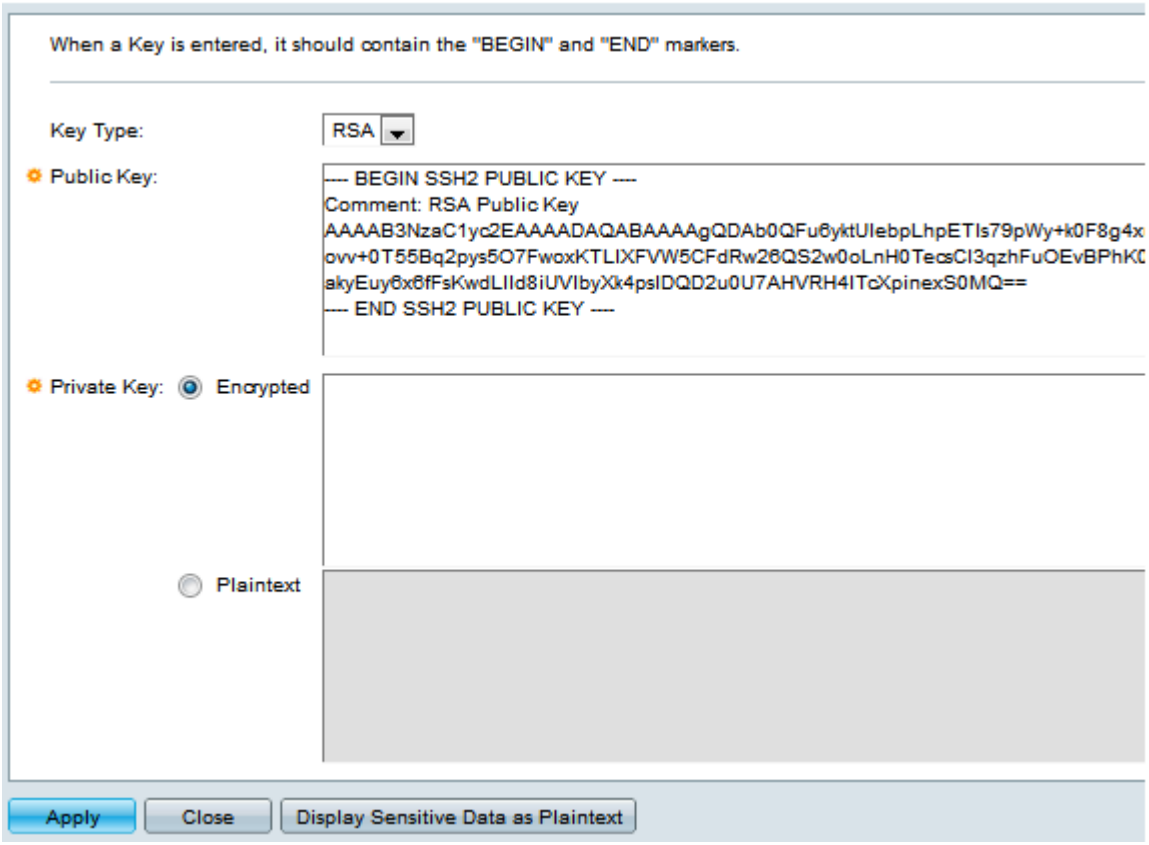


Step 11. (Optional) Choose a key type from the Key Type drop-down list.



Note: In this example, RSA is chosen.

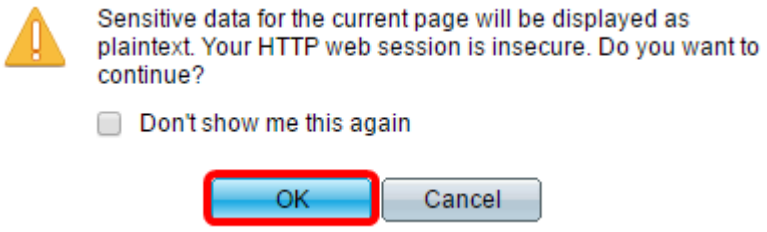
Step 12. (Optional) Enter the new public key in the *Public Key* field.



Step 13. (Optional) Enter the new private key in the *Private Key* field.

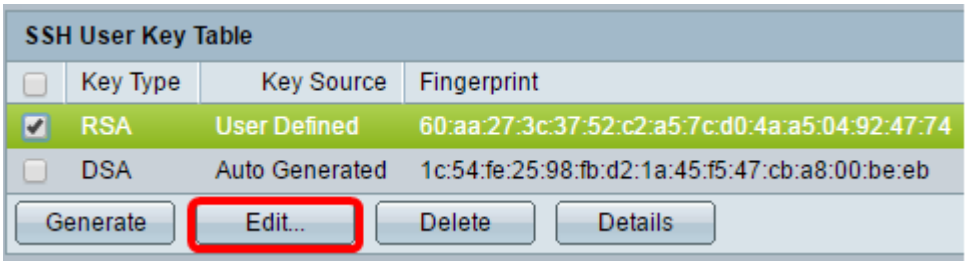
Note: You can edit the private key and you can click Encrypted to see the current private key as an encrypted text, or Plaintext to see the current private key in plain text.

Step 14. (Optional) Click **Display Sensitive Data as Plaintext** to show the encrypted data of the page in plain text format then click **OK** to proceed.

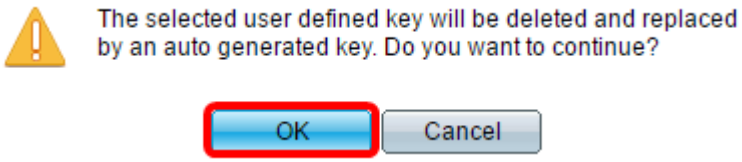


Step 15. Click **Apply** to save your changes then click **Close**.

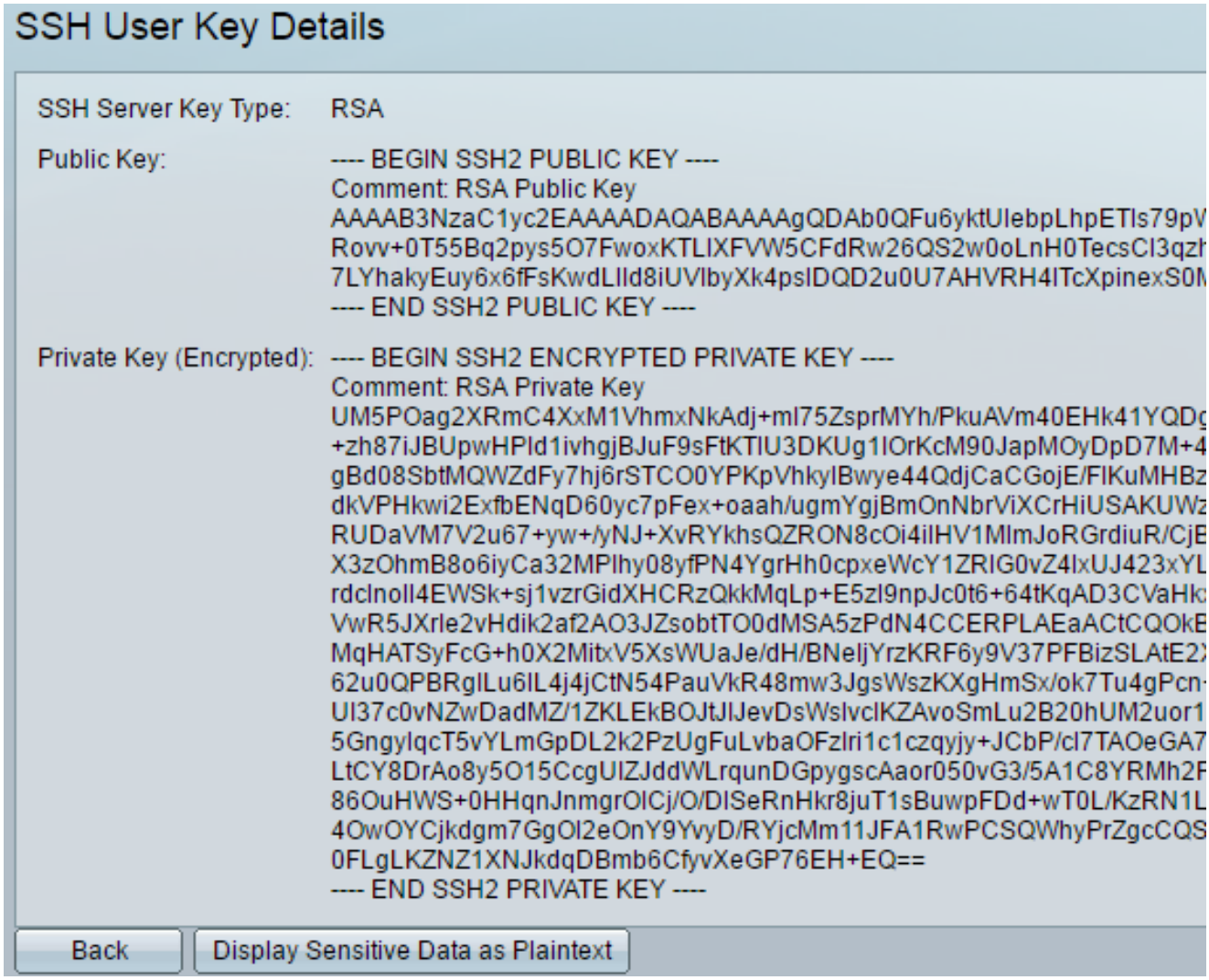
Step 16. (Optional) Click **Delete** to delete the checked key.



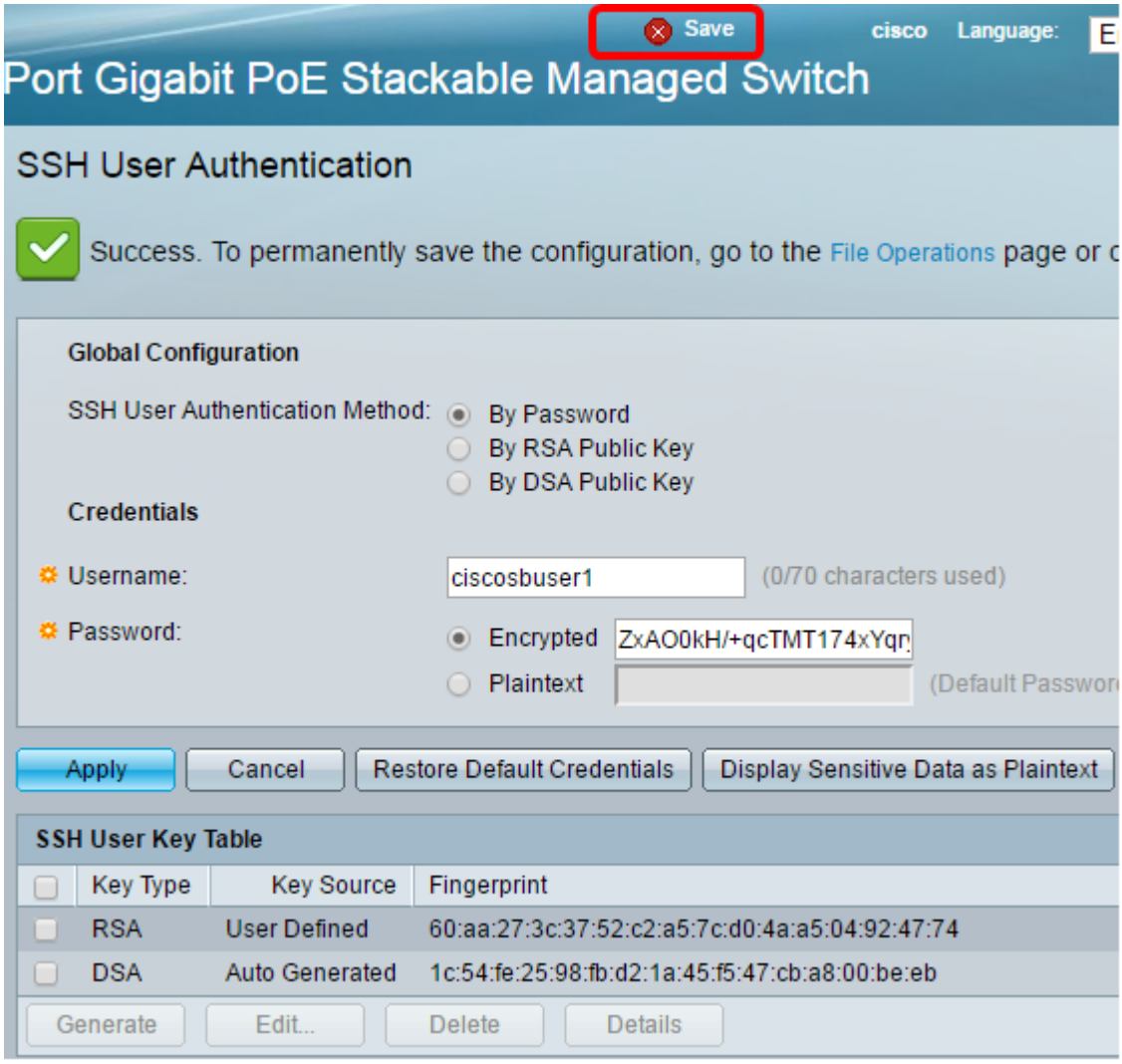
Step 17. (Optional) Once prompted by a confirmation message as shown below, click **OK** to delete the key.



Step 18. (Optional) Click **Details** to see the details of the checked key.



Step 19. (Optional) Click the **Save** button at the top portion of the page to save the changes to the startup configuration file.



You should now have configured the client user authentication settings on your managed switch.