# Client Secure Shell (SSH) User Authentication for the SG350XG and SG550XG Switches

## Objective

Secure Shell (SSH) is a protocol that provides a secure remote connection to a specific device. The 350XG and 550XG Series Managed Switches let you authenticate and manage users to connect to the device via SSH. The authentication occurs via a public key, so the user can use this key to establish a SSH connection to a specific device. SSH connections are useful to troubleshoot a network remotely, in the case that the network administrator is not at the network site.

This article explains how to configure client user authentication on the SG350XG and SG550XG Series Managed Switches.

## Applicable Devices

- SG350XG
- SG550XG

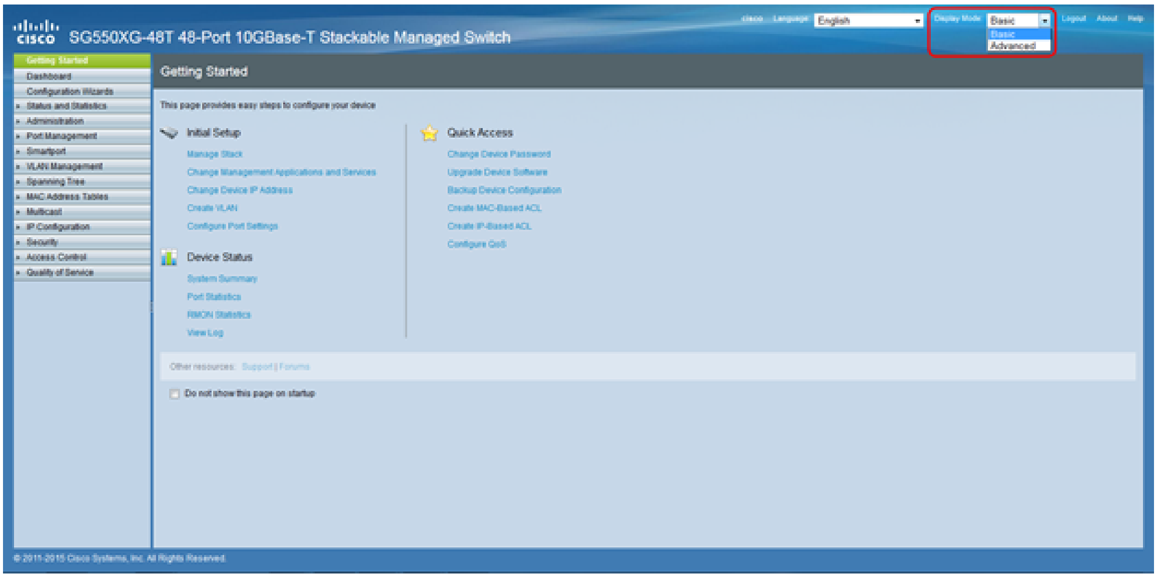
## Software Version

- v2.0.0.73

## Configure SSH Client Authentication

### Global Configuration

**Note:** The following screenshots are from the Advanced Display. This can be toggled by clicking the *Display Mode* drop-down list located in the top right of the screen



Language: English

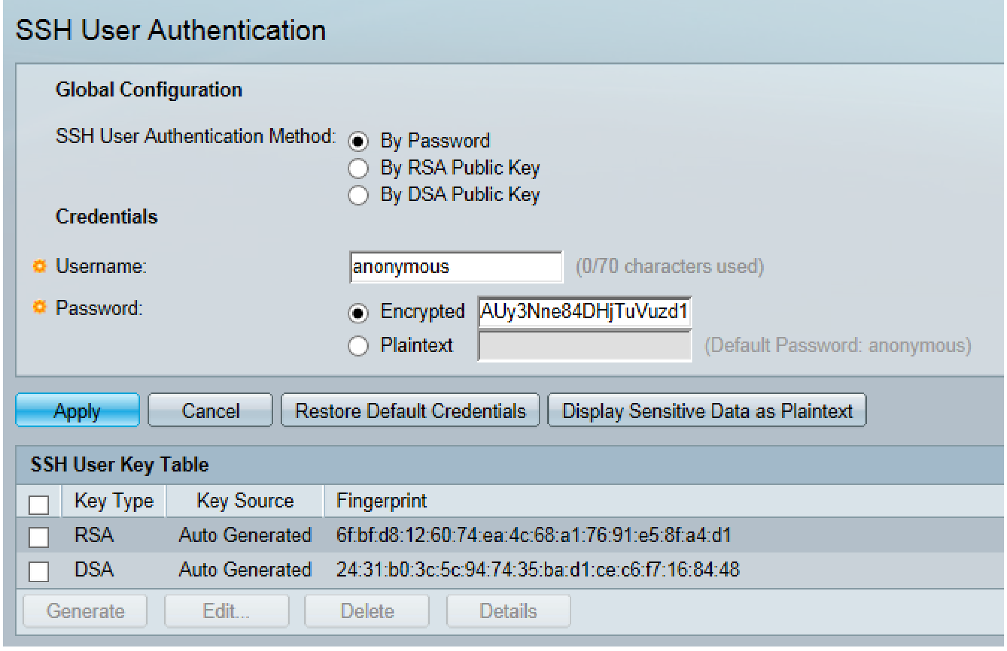
Display Mode: Basic (Basic / Advanced)

Getting Started

This page provides easy steps to configure your device

□ Do not show this page on startup

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



SSH User Authentication

Global Configuration

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

Credentials

Username: anonymous (0/70 characters used)

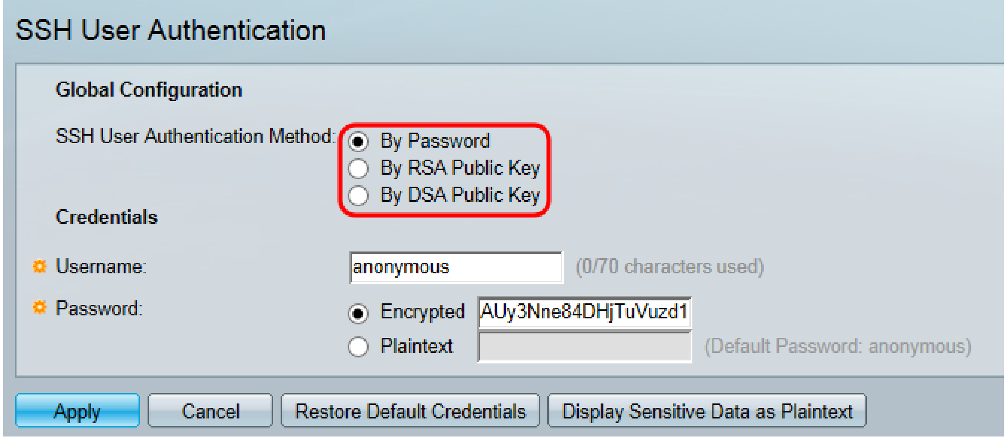
Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

SSH User Key Table

| □ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| □ | RSA | Auto Generated | 6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1 |
| □ | DSA | Auto Generated | 24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48 |

Step 2. In the *SSH User Authentication Method* field, click on the radio button for the desired global authentication method.



SSH User Authentication

Global Configuration

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

Credentials

Username: anonymous (0/70 characters used)

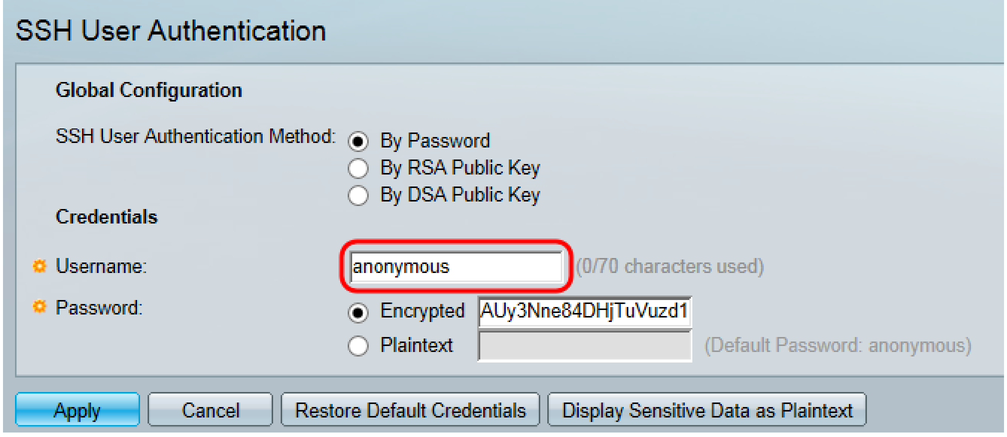
Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

The available options are as follows:

- By Password – This option lets you configure a password for user authentication. Enter a password or retain the default, “anonymous”.
- By RSA Public Key – This option lets you use an RSA public key for user authentication. RSA is used for encryption and signing. If this is selected, create an RSA public and Private key in the SSH User Key Table block.
- By DSA Public Key – This option lets you use a DSA public key for user authentication. DSA is used for signing only. If this is selected, create a DSA public/private key in the SSH User Key Table block.

Step 3. Locate the *Credentials* area. In the *Username* field, enter the username.



SSH User Authentication

Global Configuration

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

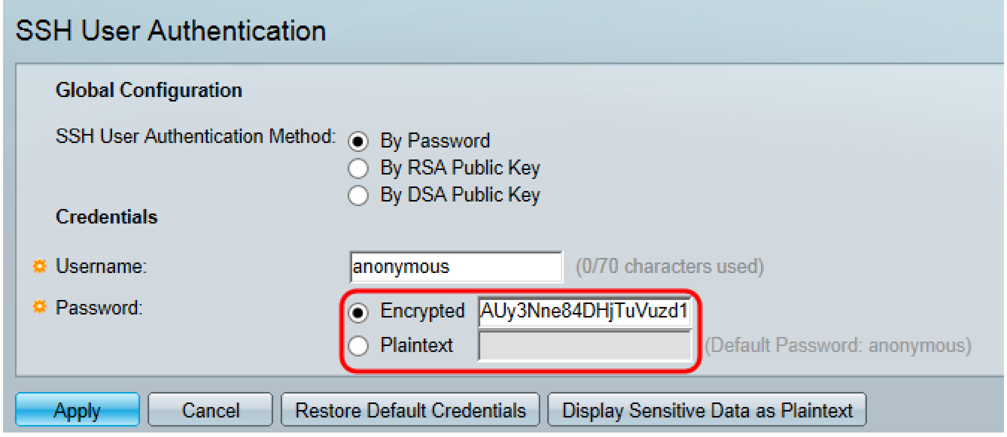
Credentials

Username: anonymous (0/70 characters used)

Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

Step 4. If **By Password** was selected in Step 2, click radio button for the desired password method in the *Password* field. The default password is “anonymous”.



SSH User Authentication

Global Configuration

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

Credentials

Username: anonymous (0/70 characters used)

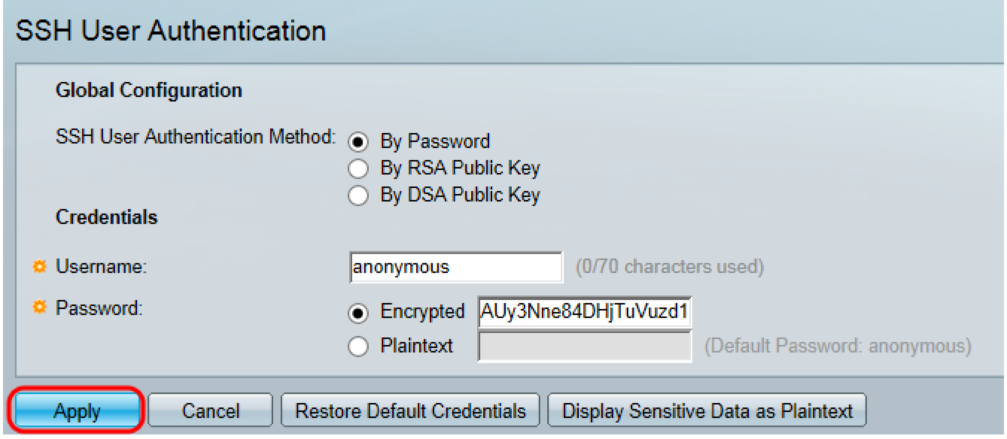
Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

The available options are described as follows:

- Encrypted – Enter an encrypted password.
- Plaintext – Enter a password as plain text.

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



SSH User Authentication

Global Configuration

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

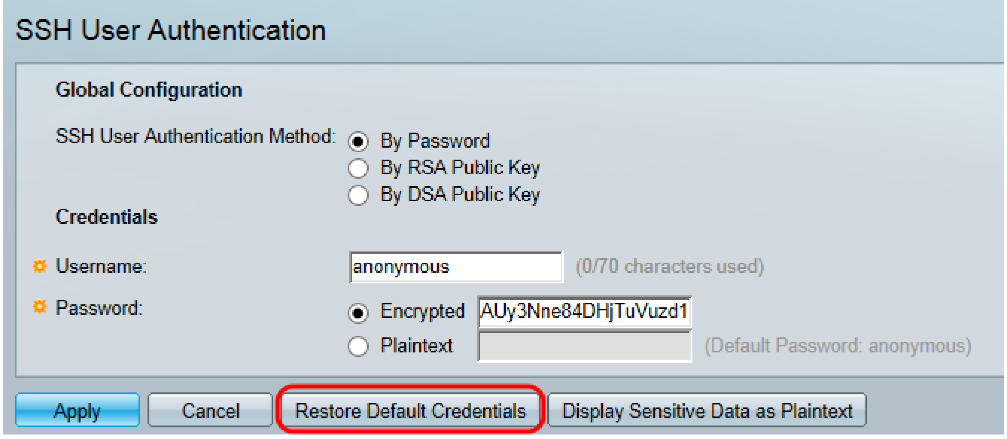
Credentials

Username: anonymous (0/70 characters used)

Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

Step 6. (Optional) To restore the default username and password, click **Restore Default Credentials**. The default the password is “anonymous”.



SSH User Authentication

Global Configuration

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

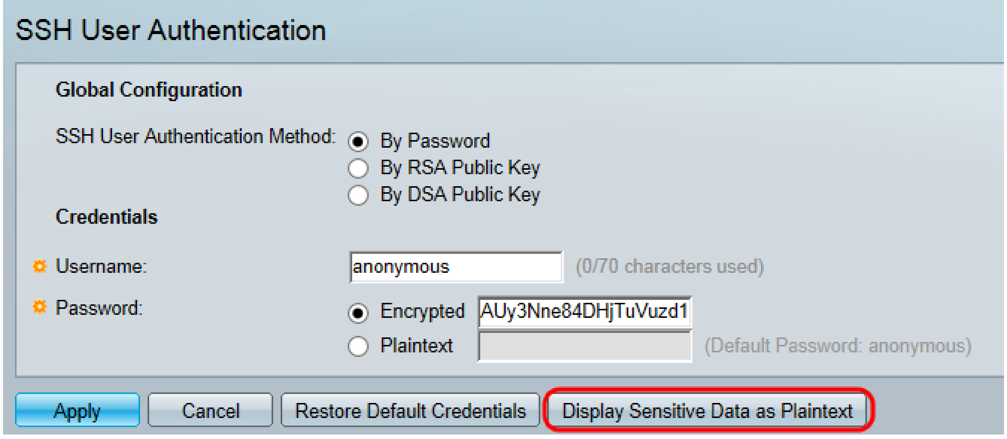
Credentials

Username: anonymous (0/70 characters used)

Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

Step 7. (Optional) To view the sensitive data as plaintext or as encrypted text, click **Display Sensitive Data as Plaintext/Encrypted.**



SSH User Authentication

Global Configuration

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

Credentials

Username: anonymous (0/70 characters used)

Password: ● Encrypted AUy3Nne84DHjTuVuzd1 ○ Plaintext (Default Password: anonymous)

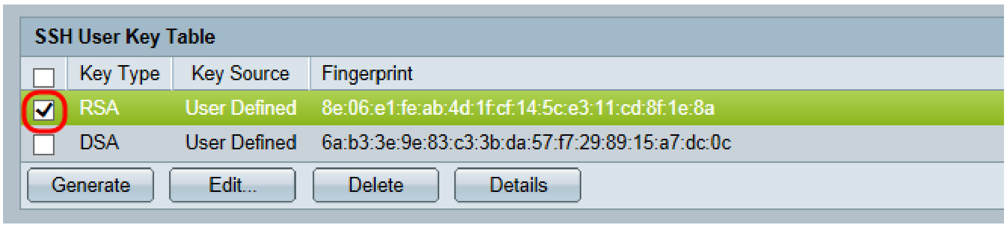
Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext

**Note:** The button’s name will alter depending on the current setting. The button will always toggle the display of the data.

## SSH User Key Table

This section explains how to manage the SSH User Table.

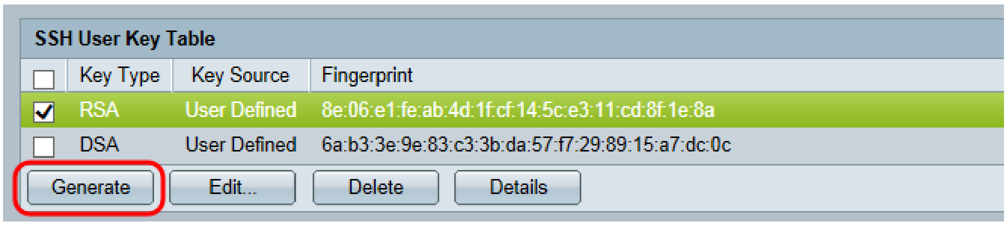
Step 1. Navigate to the *SSH User Key Table*. In the list displayed, select the checkbox(es) left to the key that you wish to manage .



SSH User Key Table

| ☐ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| ☑ | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| ☐ | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

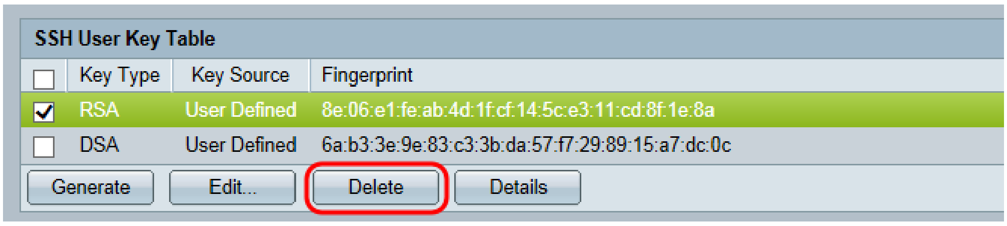
Step 2. (Optional) Click **Generate** to generate a new key. The new key overrides the selected key. A confirmation window will pop up. Click **OK** to continue.



SSH User Key Table

| ☐ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| ☑ | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| ☐ | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

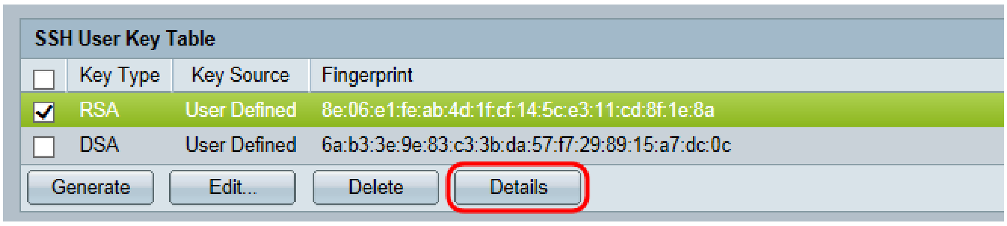
Step 3. (Optional) Click **Delete** to delete the selected key. A confirmation window will pop up. Click **OK** to continue.



SSH User Key Table

| ☐ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| ☑ | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| ☐ | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

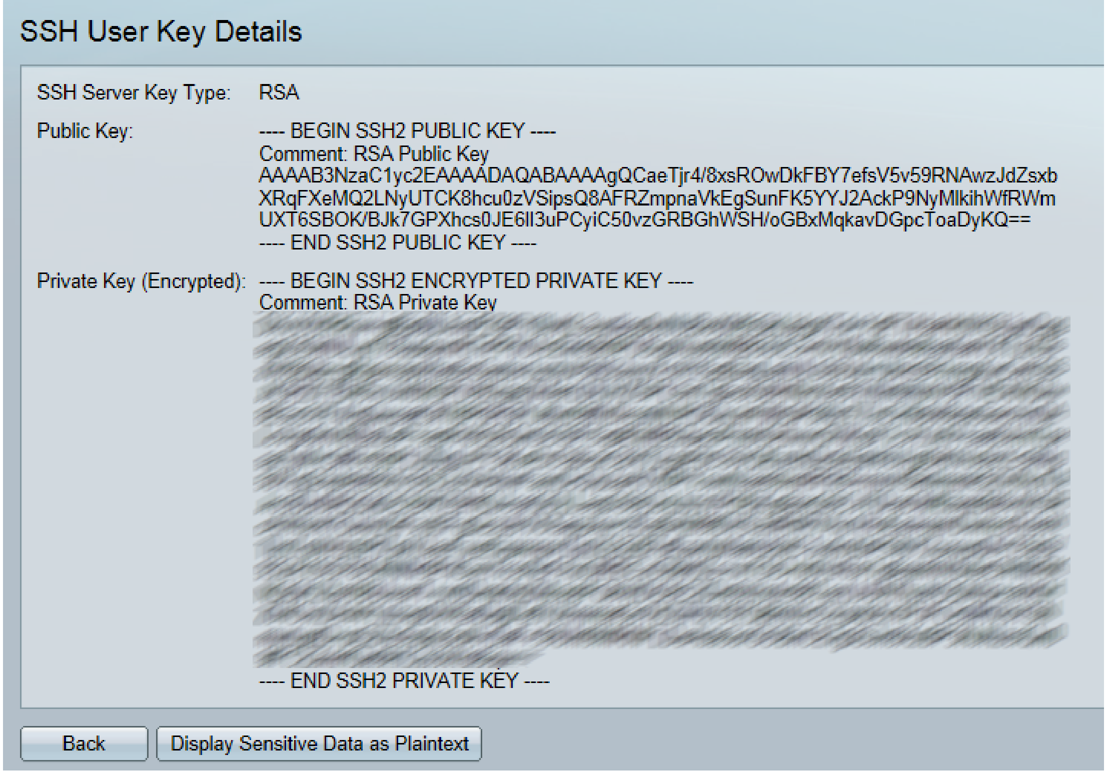
Step 4. (Optional) Click **Details** to view the details of the selected key.



SSH User Key Table

| ☐ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| ☑ | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| ☐ | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

The SSH User Key Details page appears. Click **Back** to return to the SSH User Key Table.



SSH User Key Details

SSH Server Key Type: RSA

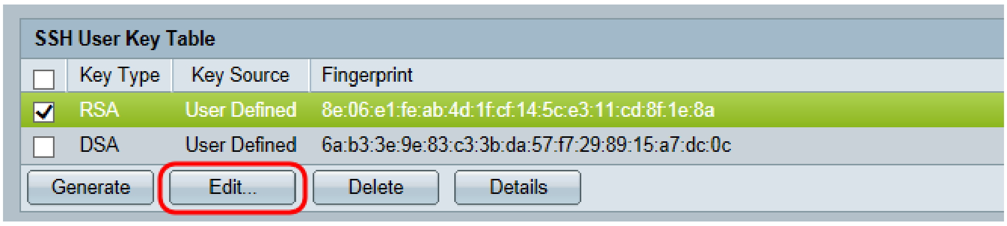
Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb
XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMlkihWfRWm
UXT6SBOK/BJk7GPXhcs0JE6lI3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ==
---- END SSH2 PUBLIC KEY ----
```

Private Key (Encrypted):

```
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
[redacted]
---- END SSH2 PRIVATE KEY ----
```

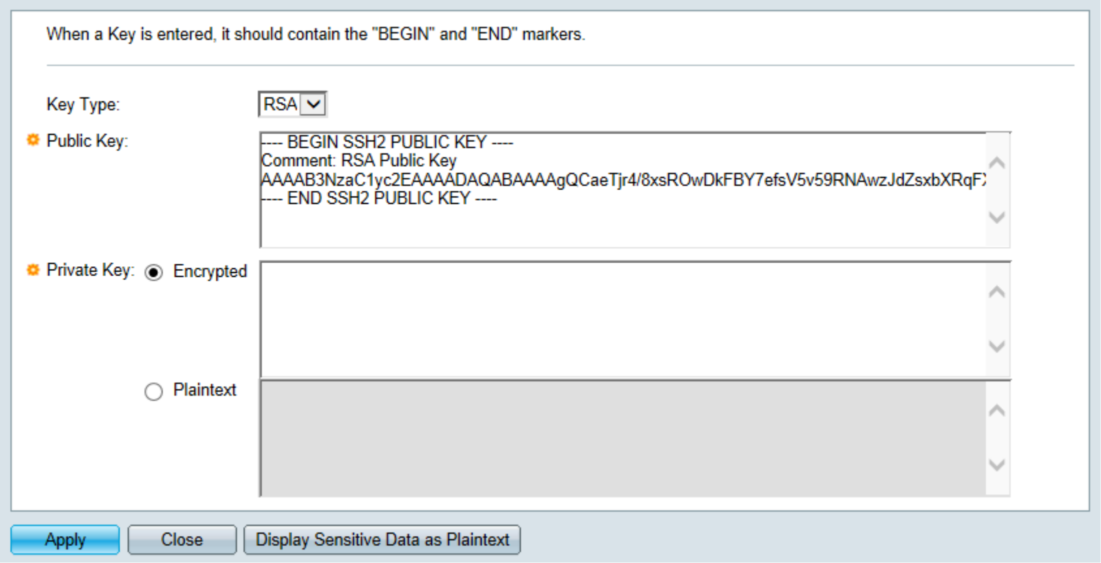
Step 5. Click **Edit** to edit the chosen key.



SSH User Key Table

| □ | Key Type | Key Source | Fingerprint |
|---|---|---|---|
| ☑ | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| □ | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

The *Edit SSH Client Authentication Settings* window opens:



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

Key Type: RSA

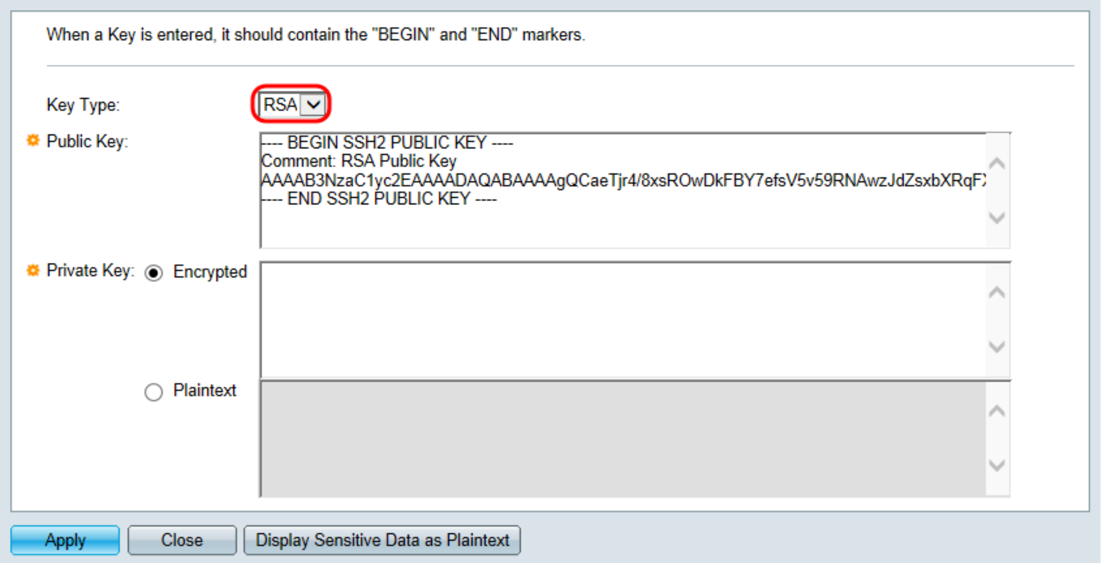
Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF>
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted

○ Plaintext

Step 6. Select the desired key type from the *Key Type* drop-down list.



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

Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF
---- END SSH2 PUBLIC KEY ----
```

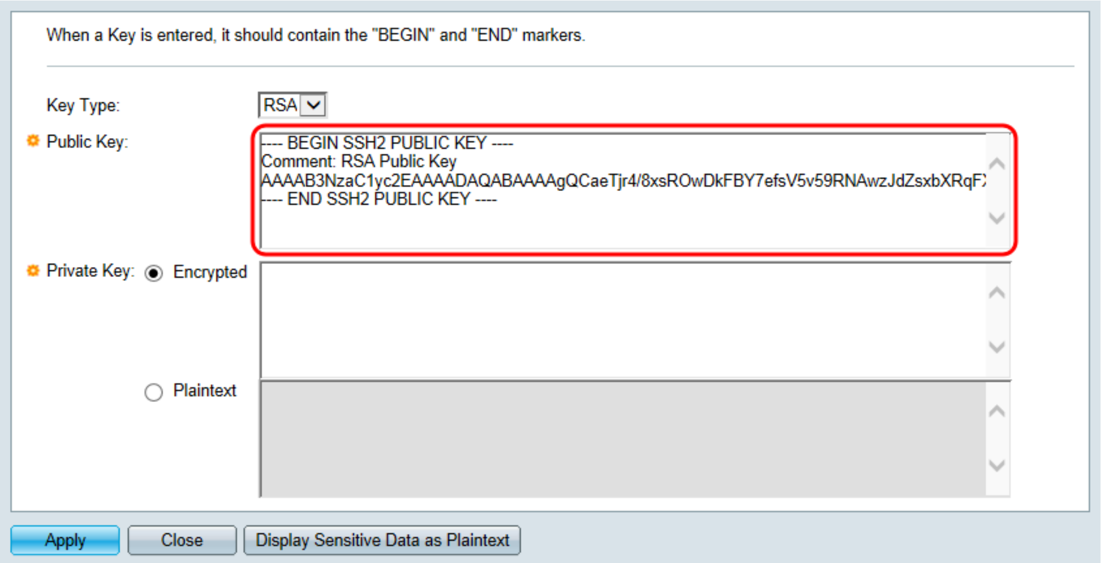
Private Key: ● Encrypted

○ Plaintext

The available options are as follows:

- RSA – RSA is used for encryption and signing.
- DSA – DSA is used for signing only.

Step 7. In the *Public Key* field, you can edit the current public key.



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

Key Type: RSA

Public Key:

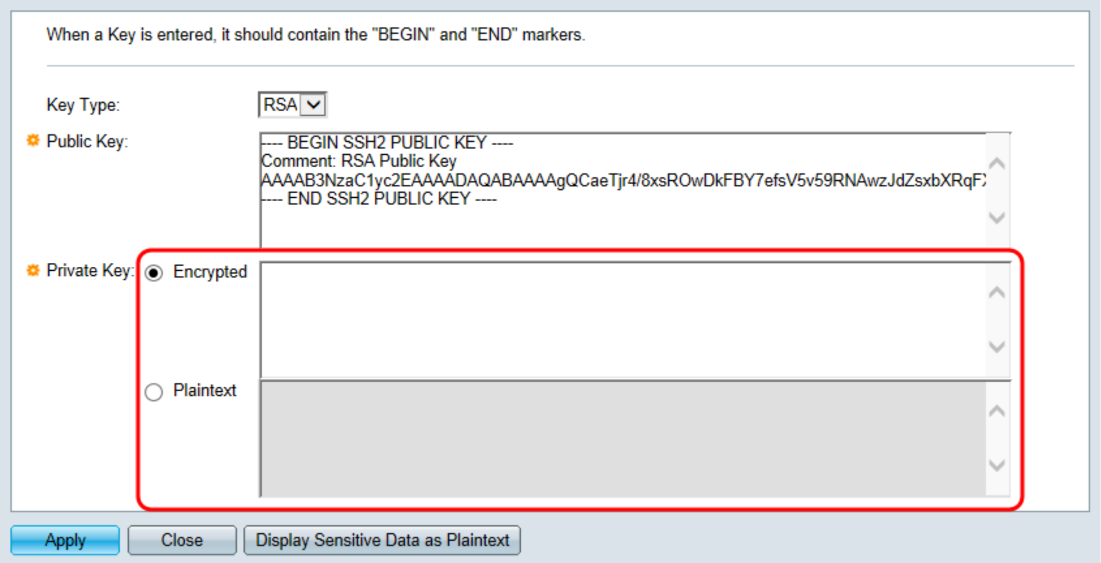
```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted

○ Plaintext

Step 8. In the *Private Key* field, you can edit the current private key. Click the

**Encrypted** radio button to see the current private key as encrypted. Otherwise, click the **Plaintext** radio button to see the current private key as plain text.



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

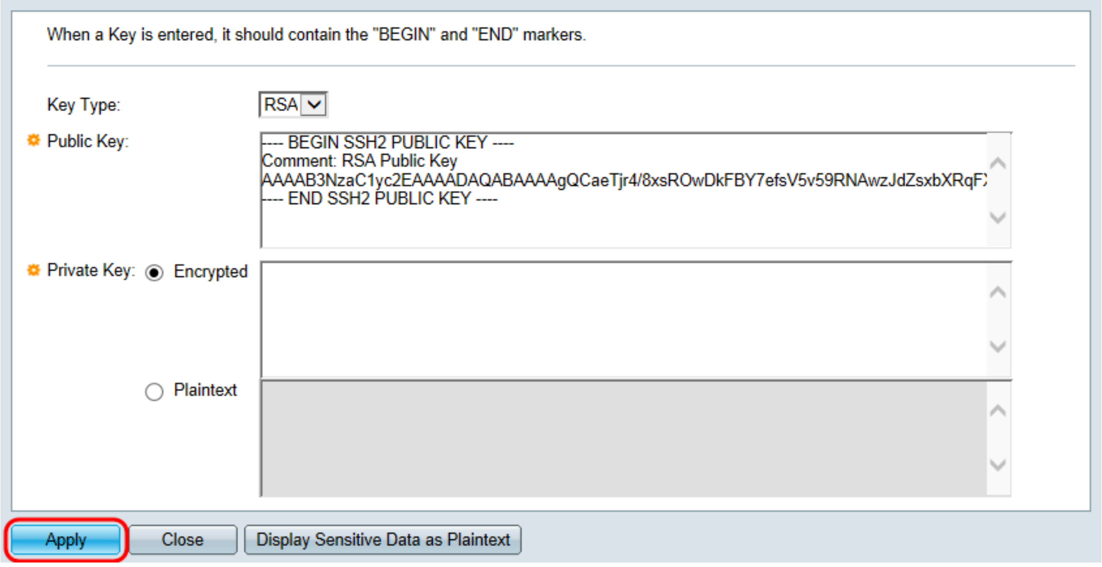
Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF)
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted ○ Plaintext

Step 9. Click **Apply** to save your changes.



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

Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCaeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF)
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted ○ Plaintext