Configure Secure Shell (SSH) User Authentication Settings on a Cisco Business 350 Series Switch

Objective

This article provides instructions on how to configure client user authentication on Cisco Business 350 series switches.

Introduction

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.

Applicable Devices | Software Version

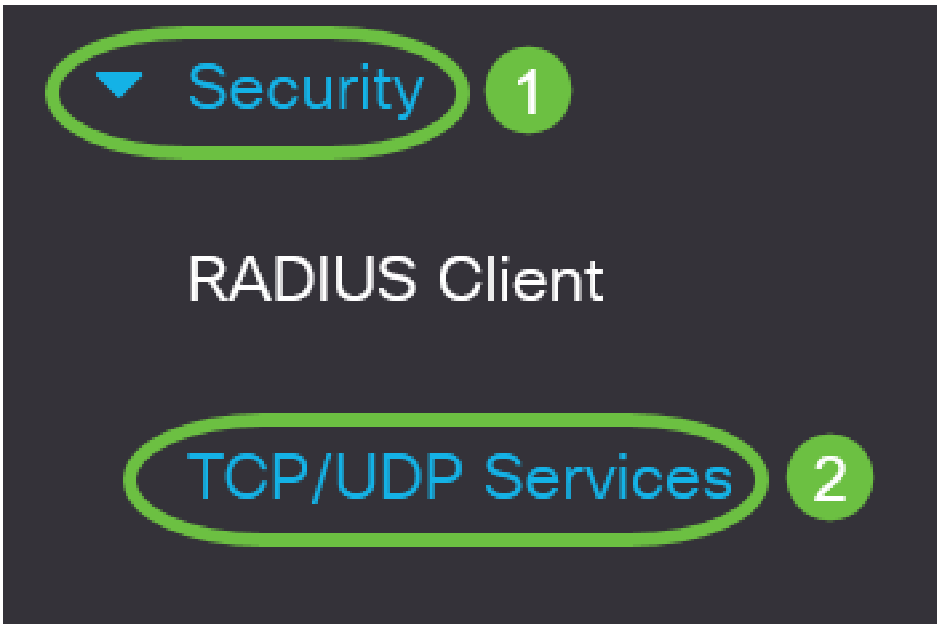
- CBS350 (Data Sheet) | 3.0.0.69 (Download latest)
- CBS350-2X (Data Sheet) | 3.0.0.69 (Download latest)
- CBS350-4X (Data Sheet) | 3.0.0.69 (Download latest)

Configure SSH Client User Authentication Settings

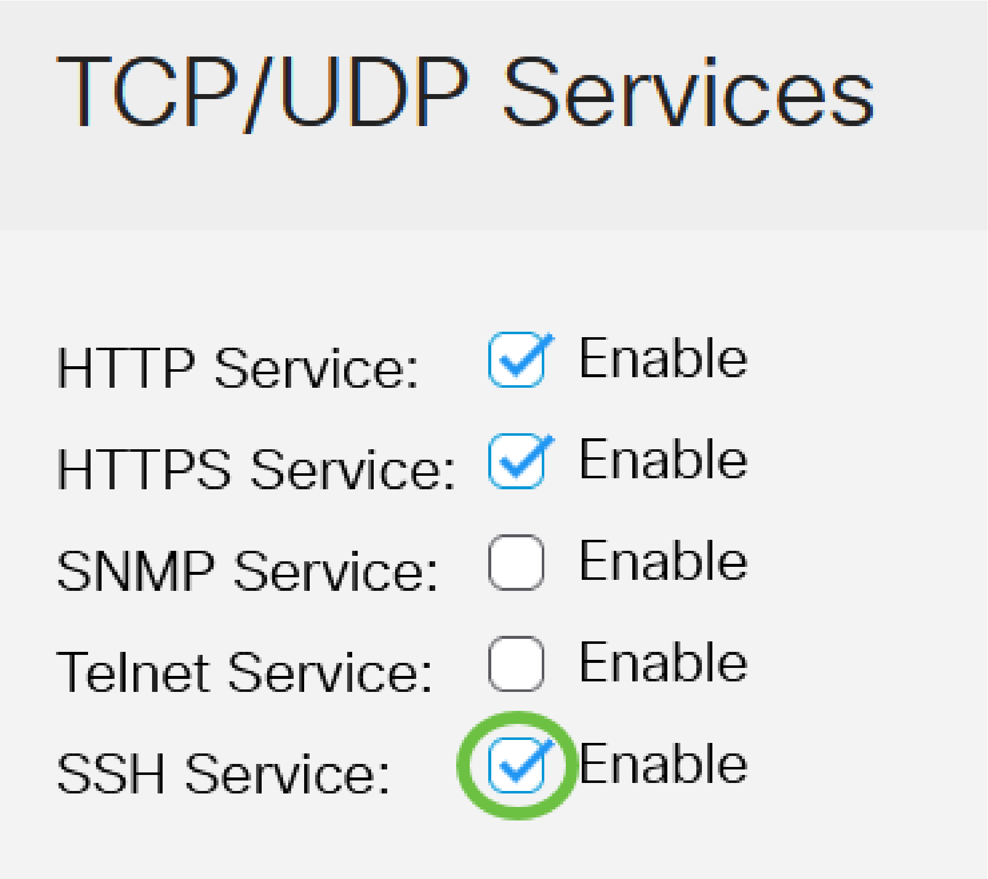
Enable SSH Service

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**



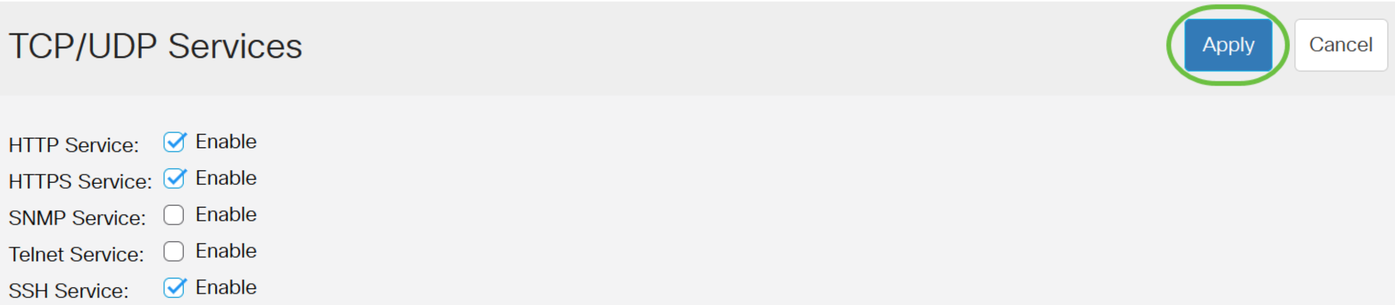
Step 2. Check the **SSH Service** check box to enable access of switches command prompt through SSH.



TCP/UDP Services

HTTP Service: ☑ Enable
HTTPS Service: ☑ Enable
SNMP Service: □ Enable
Telnet Service: □ Enable
SSH Service: ☑ Enable

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



TCP/UDP Services

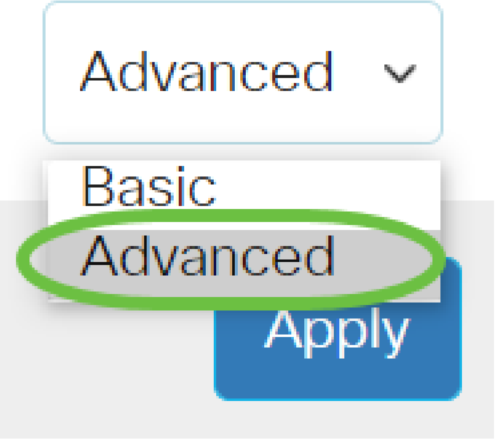
HTTP Service: ☑ Enable
HTTPS Service: ☑ Enable
SNMP Service: □ Enable
Telnet Service: □ Enable
SSH Service: ☑ Enable

Configure SSH User Authentication Settings

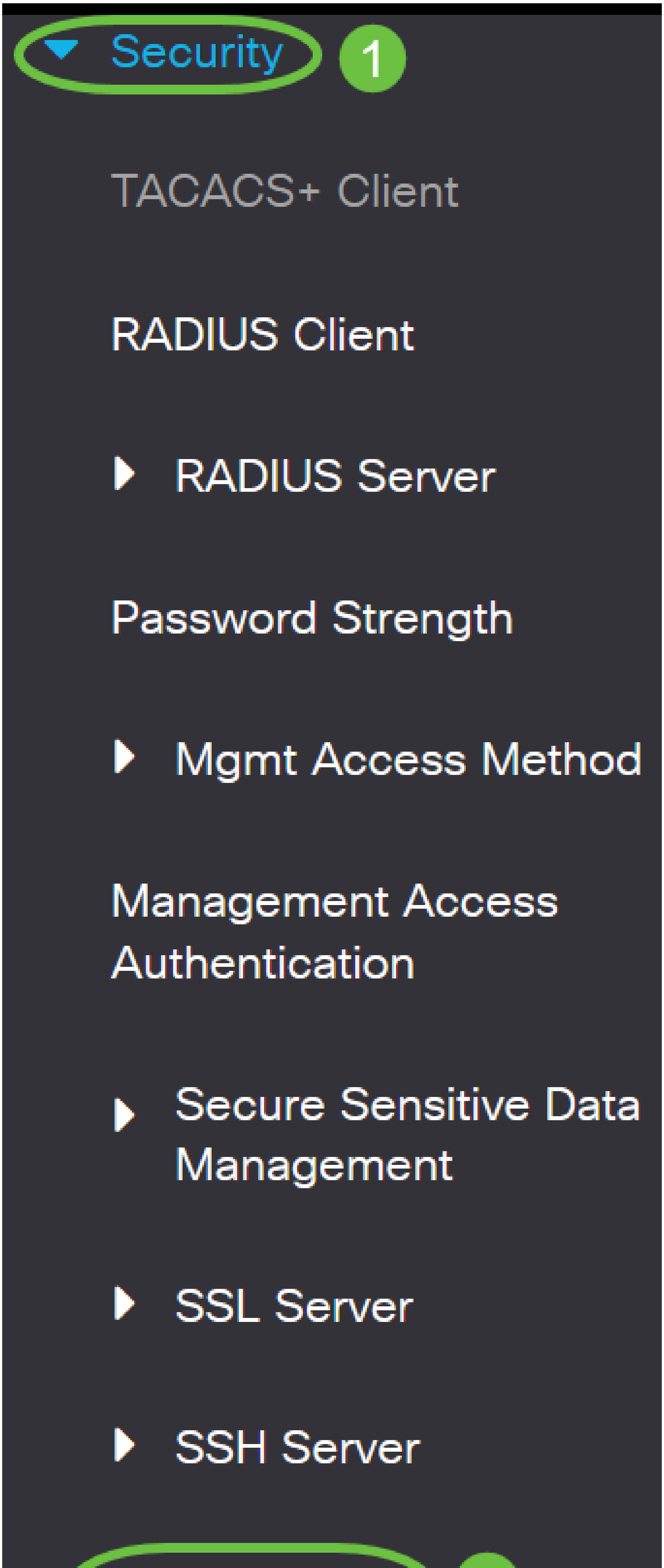
Use this page to choose an SSH user authentication method. You can set a username and password on the device if the password method is chosen. You can also generate a Ron Rivest, Adi Shamir and Leonard Adleman (RSA) or Digital Signature Algorithm (DSA) key if the public or private key method is selected.

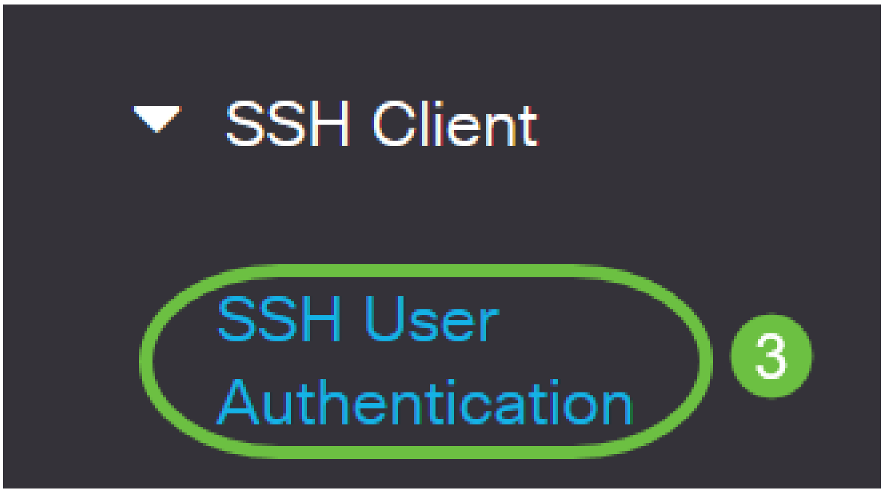
RSA and DSA default key pairs are generated for the device when it is booted. One of these keys is used to encrypt the data being downloaded from the SSH server. The RSA key is used by default. If the user deletes one or both of these keys, they are regenerated.

Step 1. Log in to the web-based utility of your switch then choose Advanced in the Display Mode drop-down list.

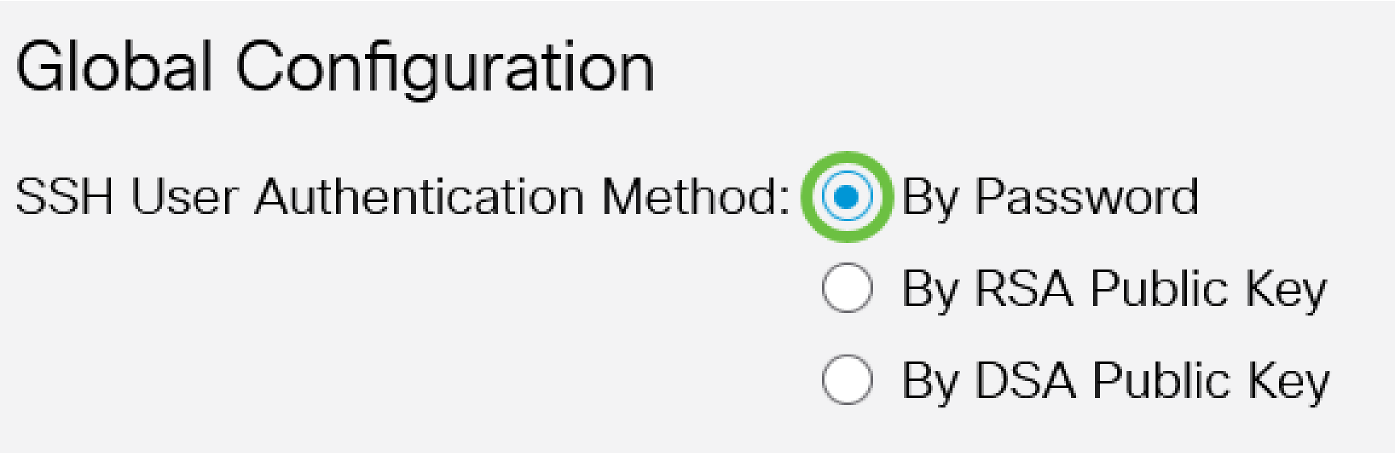


Step 2. Choose **Security > SSH Client > SSH User Authentication** from the menu.


Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Step 3. Under Global Configuration, click the desired SSH User Authentication Method.



Global Configuration

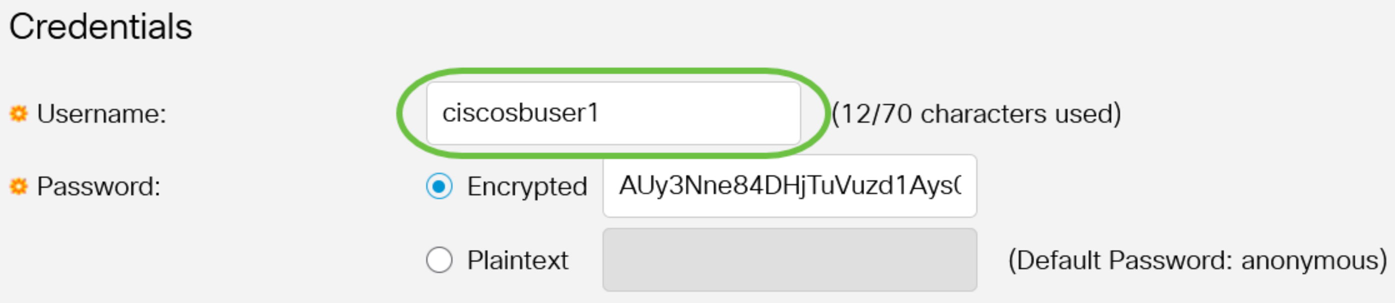
SSH User Authentication Method: ● By Password
○ By RSA Public Key
○ By DSA Public Key

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.

In this example, By Password is chosen.

Step 4. In the Credentials area, enter the user name in the *Username* field.



Credentials

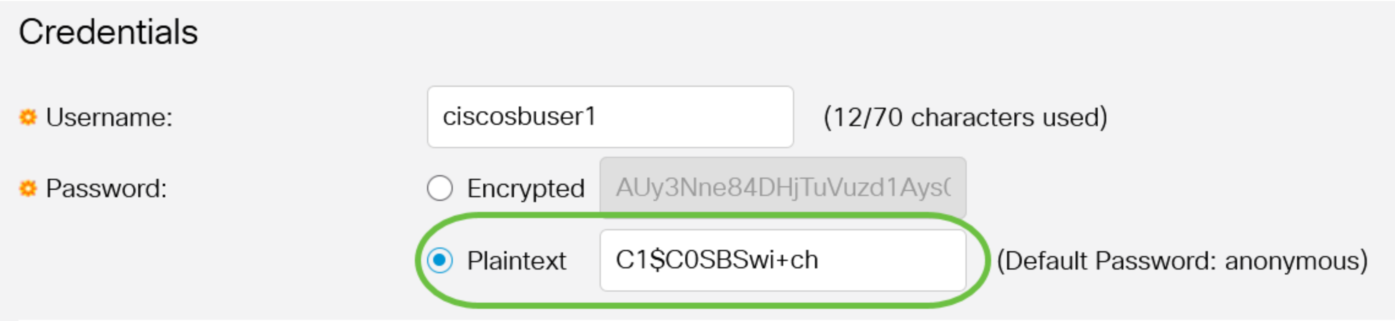
Username: ciscosbuser1 (12/70 characters used)

Password: ● Encrypted AUy3Nne84DHjTuVuzd1Ays(

○ Plaintext (Default Password: anonymous)

In this example, ciscosbuser1 is used.

Step 5. (Optional) If you chose By Password in Step 2, click the method then enter the password in the *Encrypted* or *Plaintext* field.



Credentials

Username: ciscosbuser1 (12/70 characters used)

Password: ○ Encrypted AUy3Nne84DHjTuVuzd1Ays(

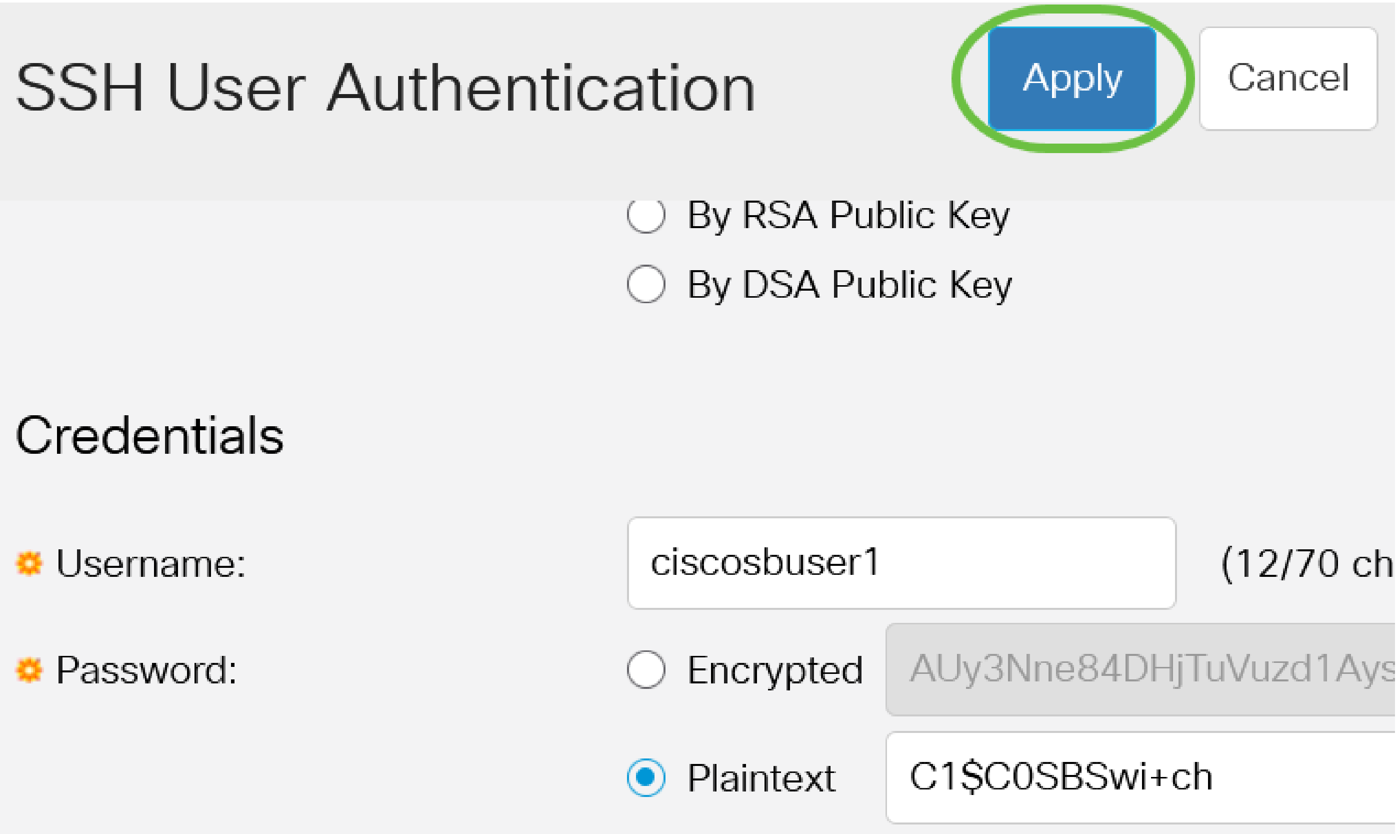
● Plaintext C1$C0SBSwi+ch (Default Password: anonymous)

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.

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

Step 6. Click **Apply** to save your authentication configuration.



SSH User Authentication

○ By RSA Public Key

○ By DSA Public Key

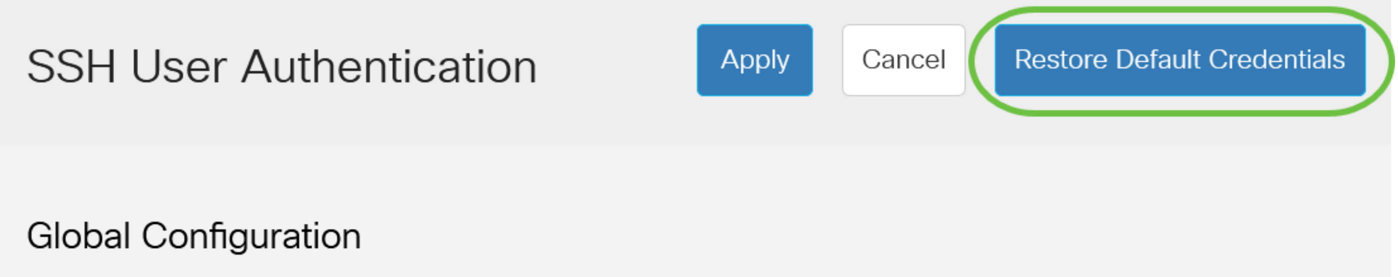
Credentials

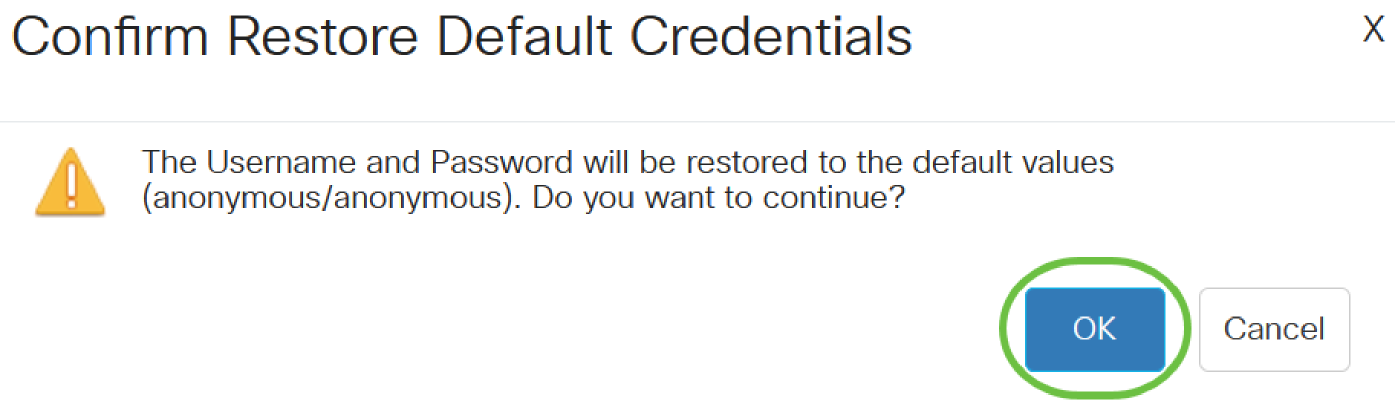
Username: ciscosbuser1 (12/70 ch

Password: ○ Encrypted AUy3Nne84DHjTuVuzd1Ays

● Plaintext C1$C0SBSwi+ch

Step 7. (Optional) Click **Restore Default Credentials** to restore the default user name and password then click **OK** to proceed.

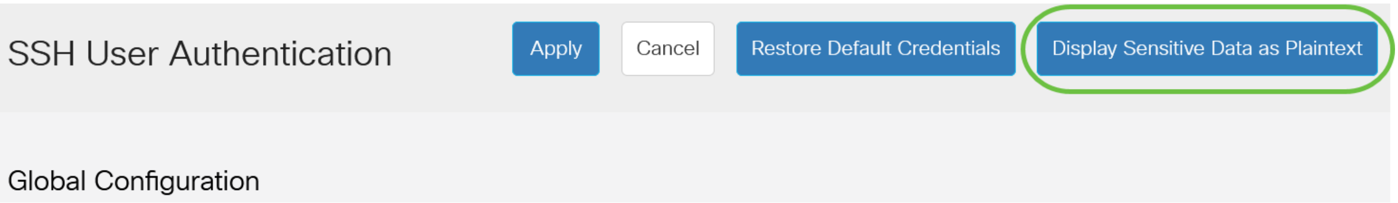


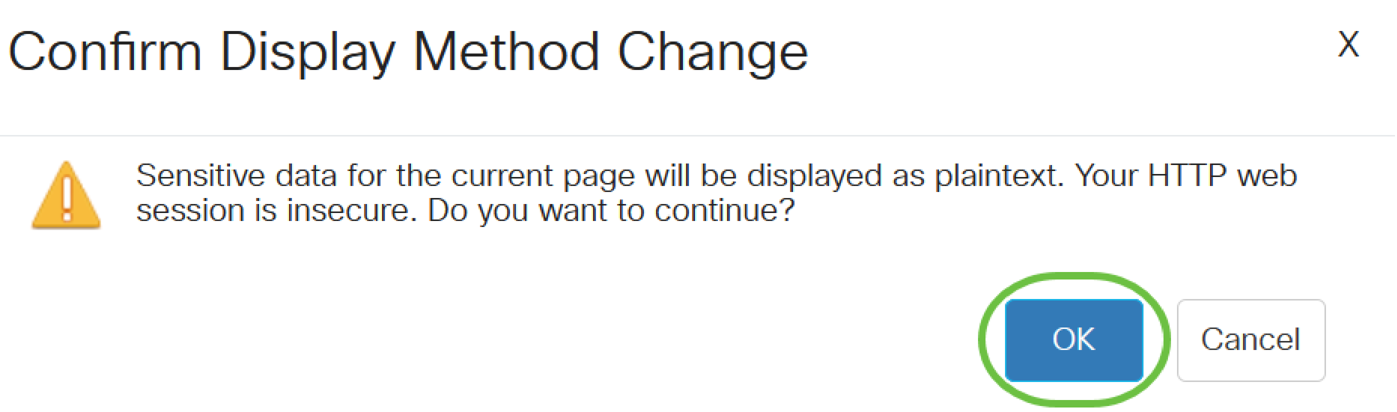


The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?

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

Step 8. (Optional) Click **Display Sensitive Data as Plaintext** to show the sensitive data of the page in plain text format then click **OK** to proceed.

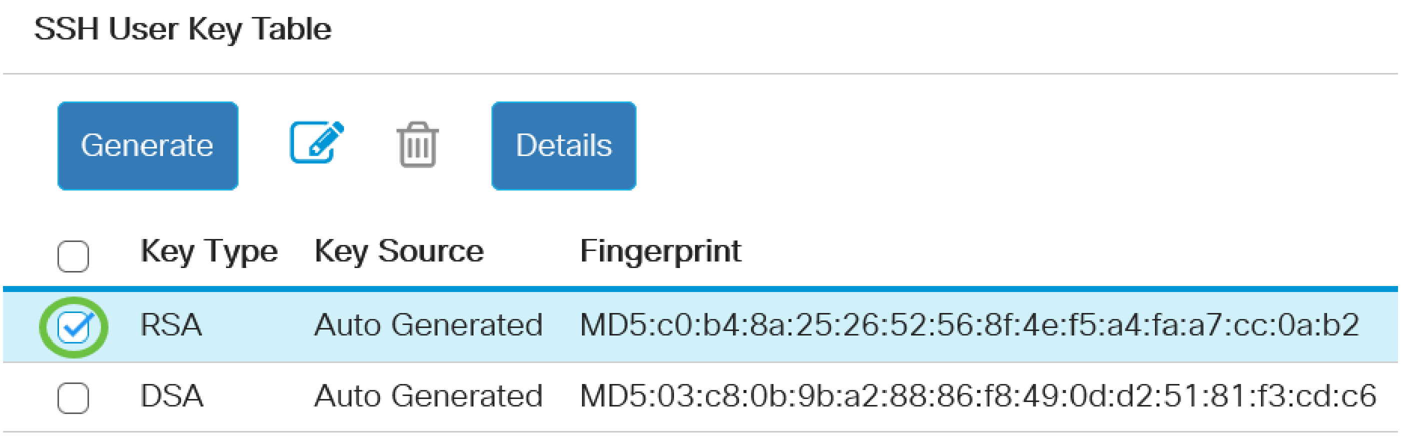

SSH User Authentication
Apply
Cancel
Restore Default Credentials
Display Sensitive Data as Plaintext
Global Configuration



Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Configure SSH User Key Table

Step 9. Check the check box of the key you wish to manage.

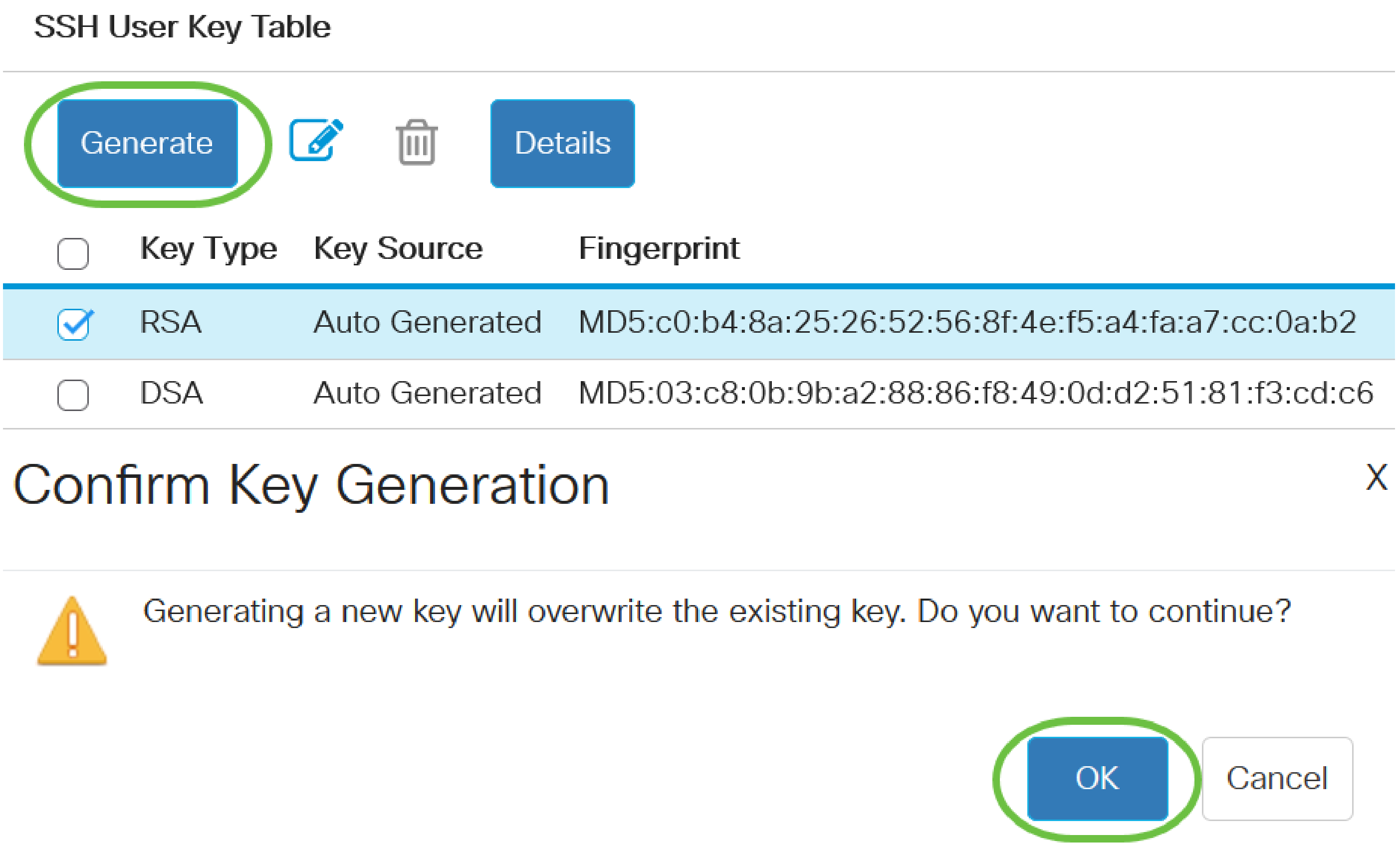


SSH User Key Table

□	Key Type	Key Source	Fingerprint
☑	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
□	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

In this example, RSA is chosen.

Step 10. (Optional) Click **Generate** to generate a new key. The new key will override the checked key then click **OK** to proceed.



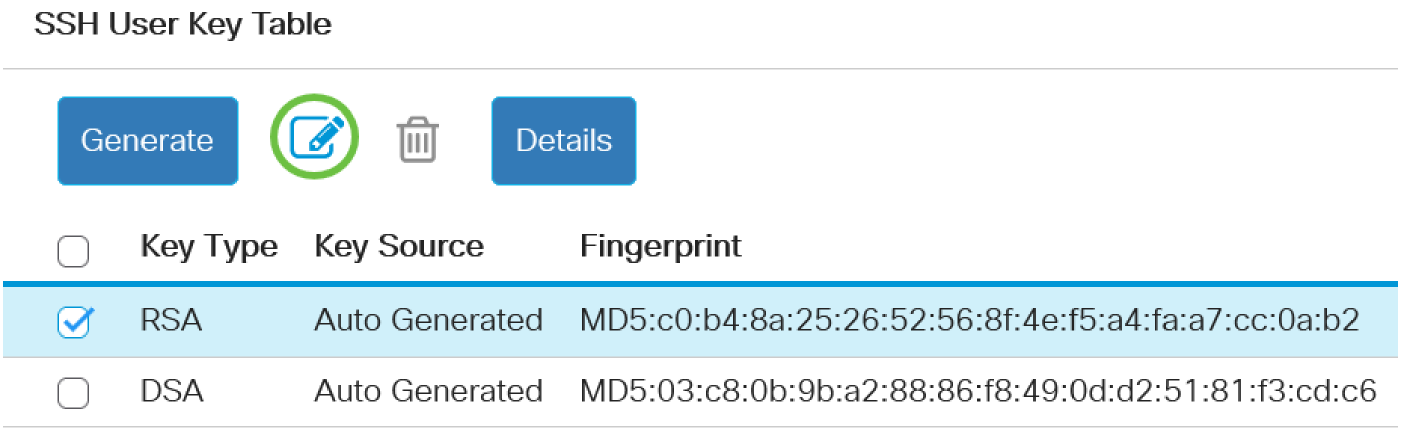
SSH User Key Table

□	Key Type	Key Source	Fingerprint
☑	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
□	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Confirm Key Generation

Generating a new key will overwrite the existing key. Do you want to continue?

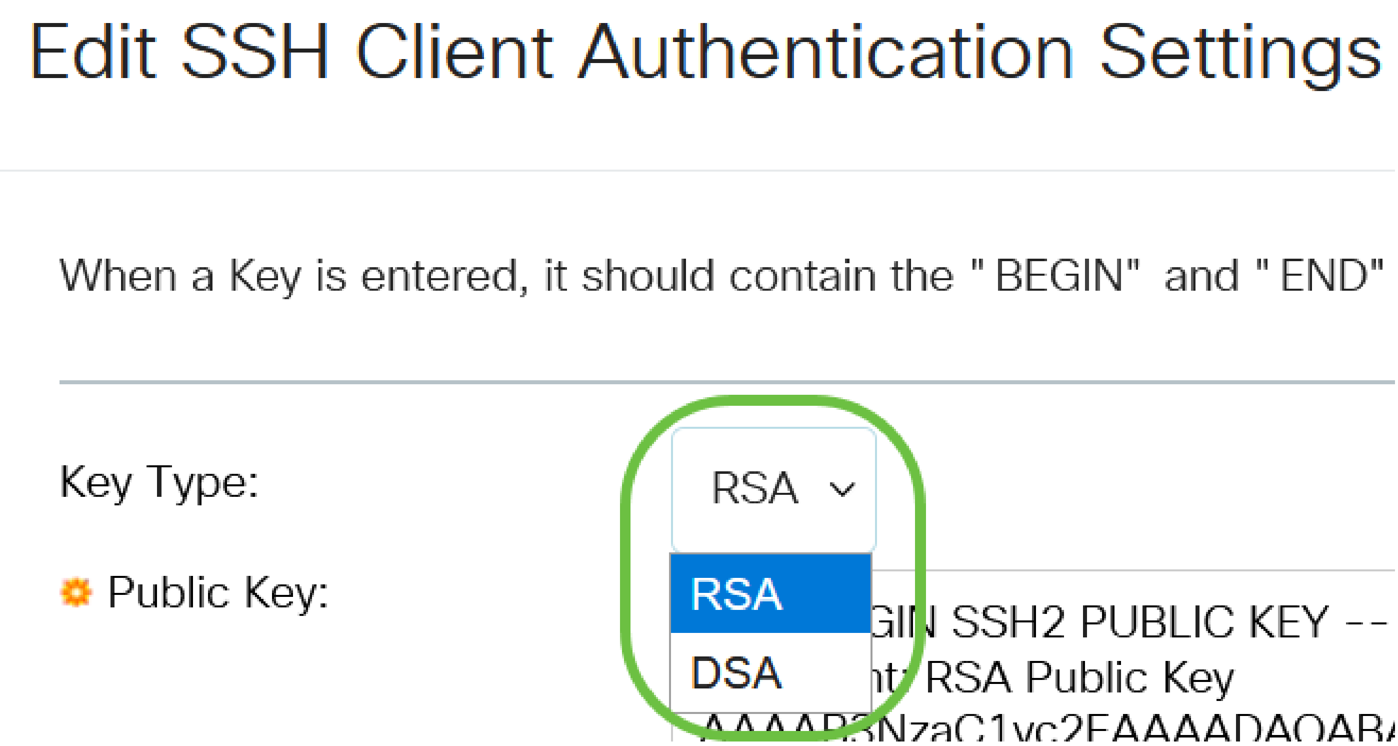
Step 11. (Optional) Click **Edit** to edit a current key.



SSH User Key Table

☐	Key Type	Key Source	Fingerprint
☑	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
☐	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Step 12. (Optional) Choose a key type from the Key Type drop-down list.



Edit SSH Client Authentication Settings

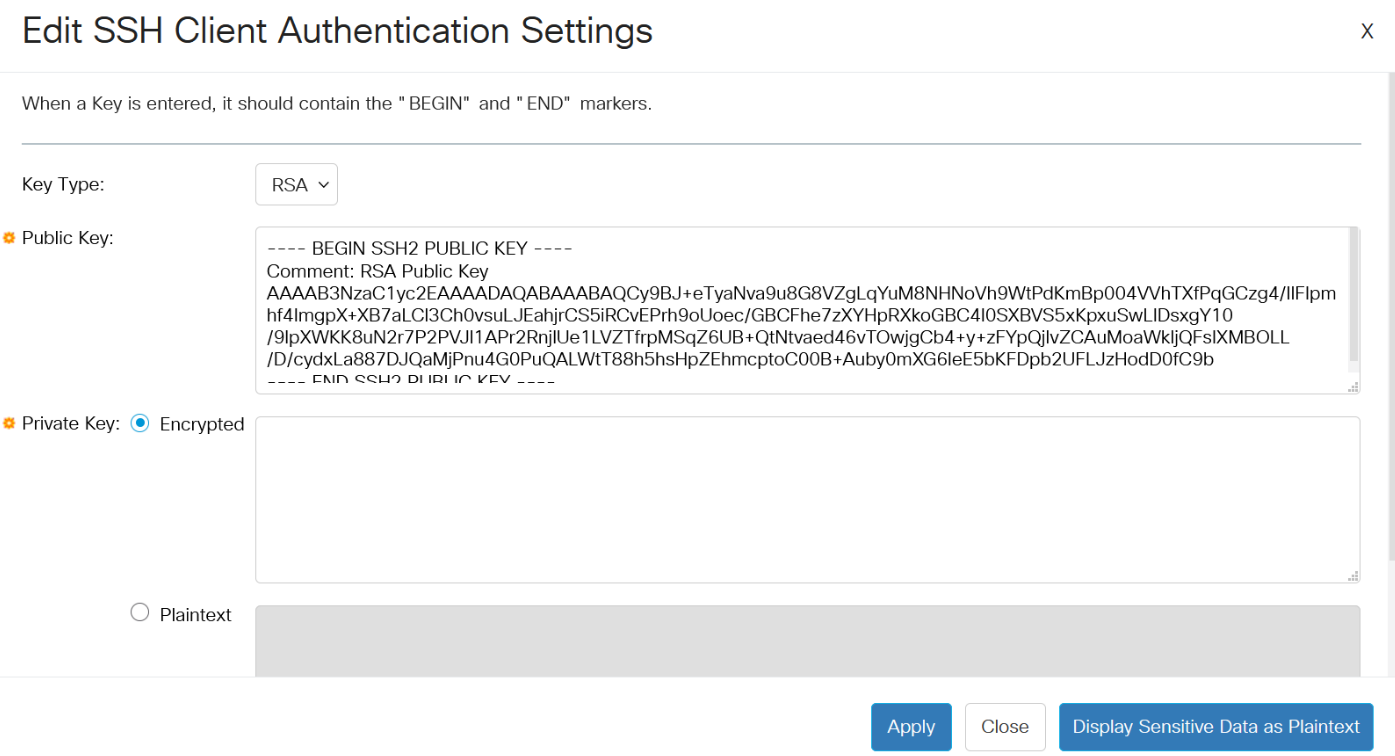
When a Key is entered, it should contain the " BEGIN" and " END"

Key Type: RSA

Public Key: GIN SSH2 PUBLIC KEY --
nt: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQAB

In this example, RSA is chosen.

Step 13. (Optional) Enter the new public key in the *Public Key* field.



Edit SSH Client Authentication Settings

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
AAAAB3NzaC1yc2EAAAADAQABAAABAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VVhTXfPqGCzg4/IIFIpm
hf4ImgpX+XB7aLCl3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6IeE5bKFDpb2UFLJzHodD0fC9b
---- END SSH2 PUBLIC KEY ----
```

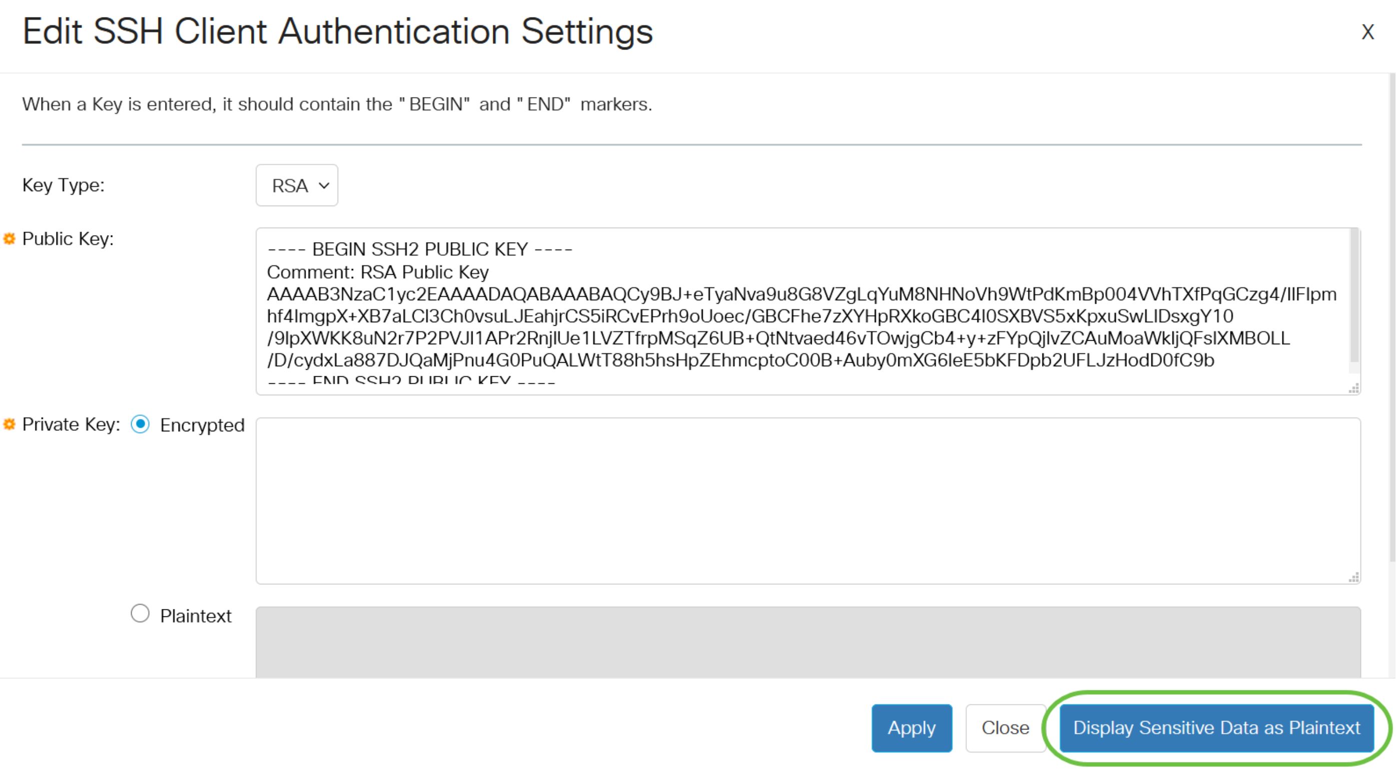
Private Key: ● Encrypted

○ Plaintext

Step 14. (Optional) Enter the new private key in the *Private Key* 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 15. (Optional) Click **Display Sensitive Data as Plaintext** to show the encrypted data of the page in plain text format then click **OK** to proceed.



Edit SSH Client Authentication Settings

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

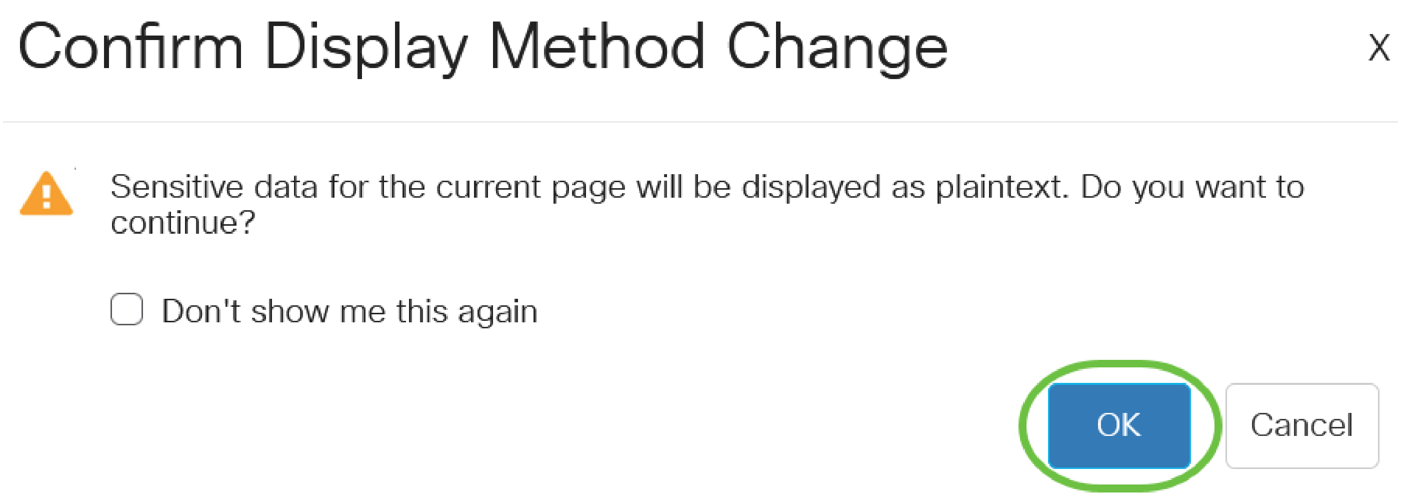
Key Type: RSA

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAABAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VVhTXfPqGCzg4/IIFIpm
hf4ImgpX+XB7aLCl3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6IeE5bKFDpb2UFLJzHodD0fC9b
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted

○ Plaintext

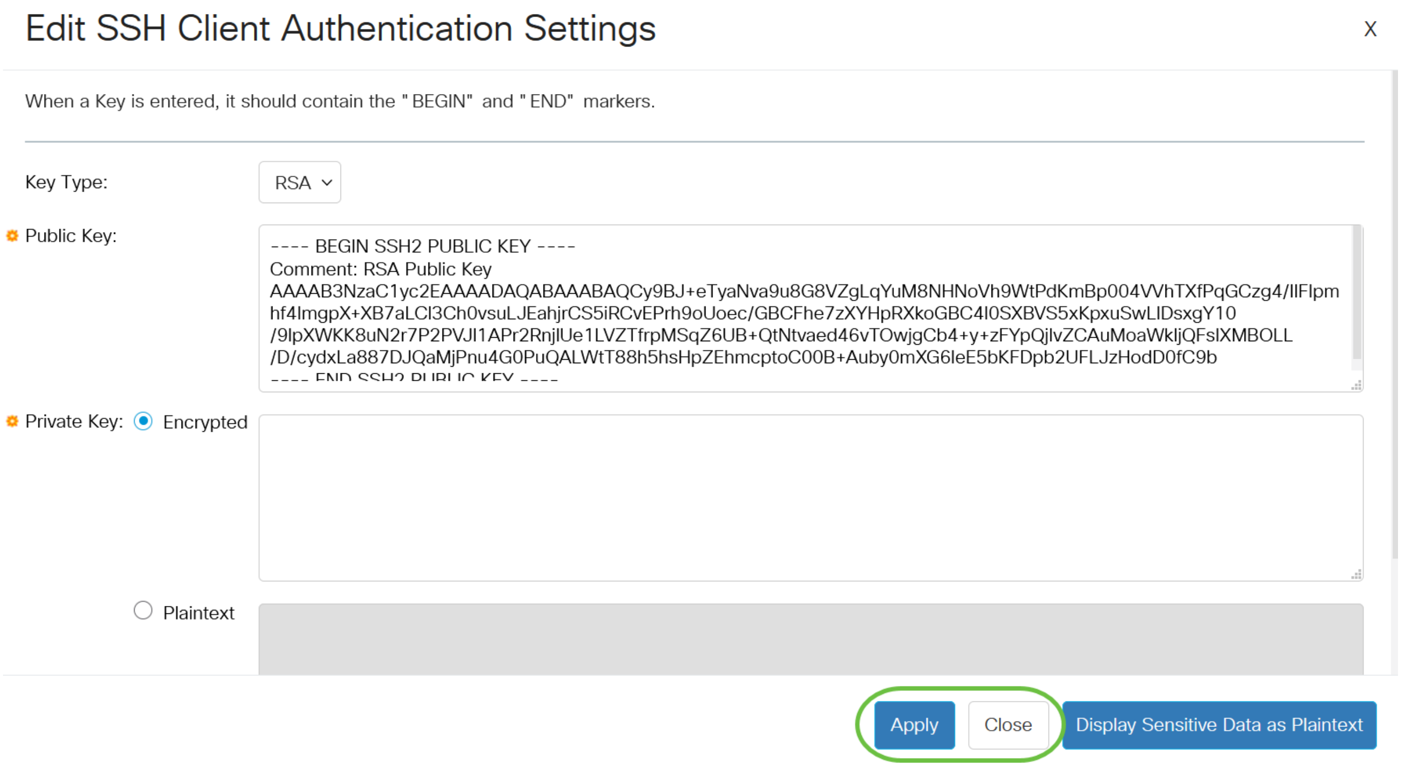


Confirm Display Method Change

Sensitive data for the current page will be displayed as plaintext. Do you want to continue?

□ Don't show me this again

Step 16. Click **Apply** to save your changes then click **Close**.



Edit SSH Client Authentication Settings

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

Key Type: RSA

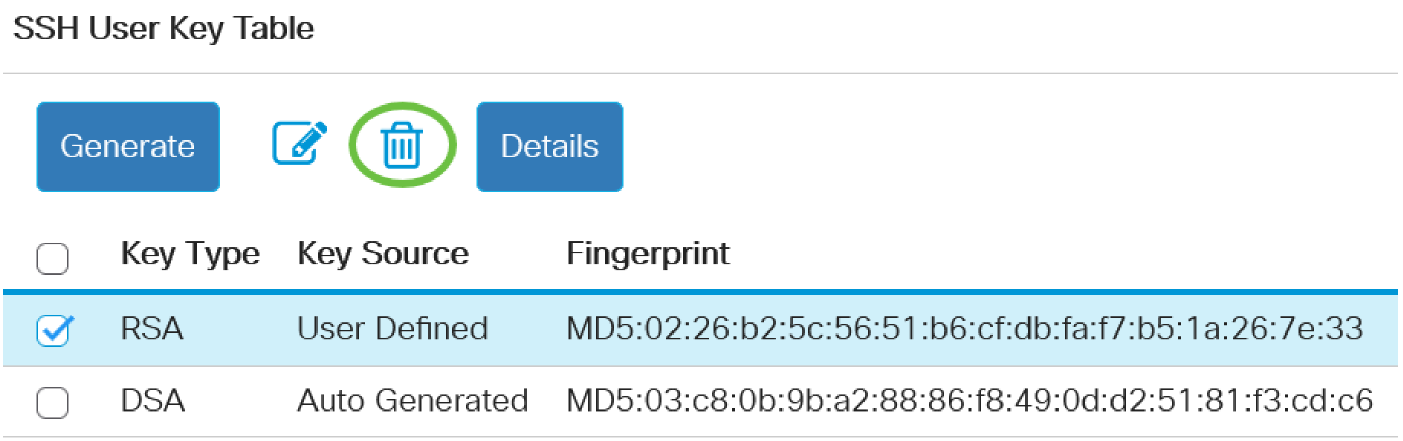
Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAABAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VVhTXfPqGCzg4/IlFlpm
hf4ImgpX+XB7aLCl3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10
/9lpXWKK8uN2r7P2PVJl1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFsIXMBOLL
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6IeE5bKFDpb2UFLJzHodD0fC9b
---- END SSH2 PUBLIC KEY ----
```

Private Key: ● Encrypted

○ Plaintext

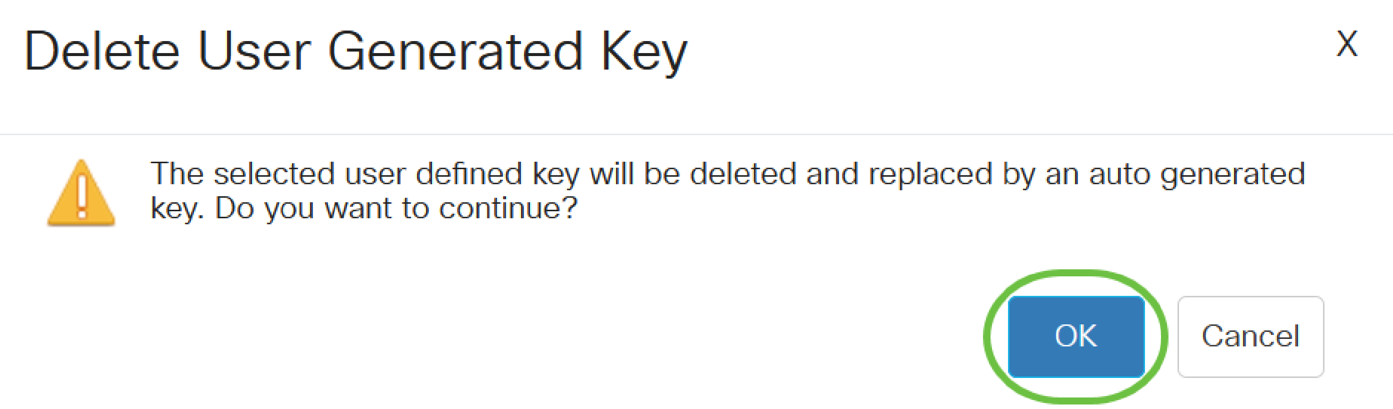
Step 17. (Optional) Click **Delete** to delete the checked key.



SSH User Key Table

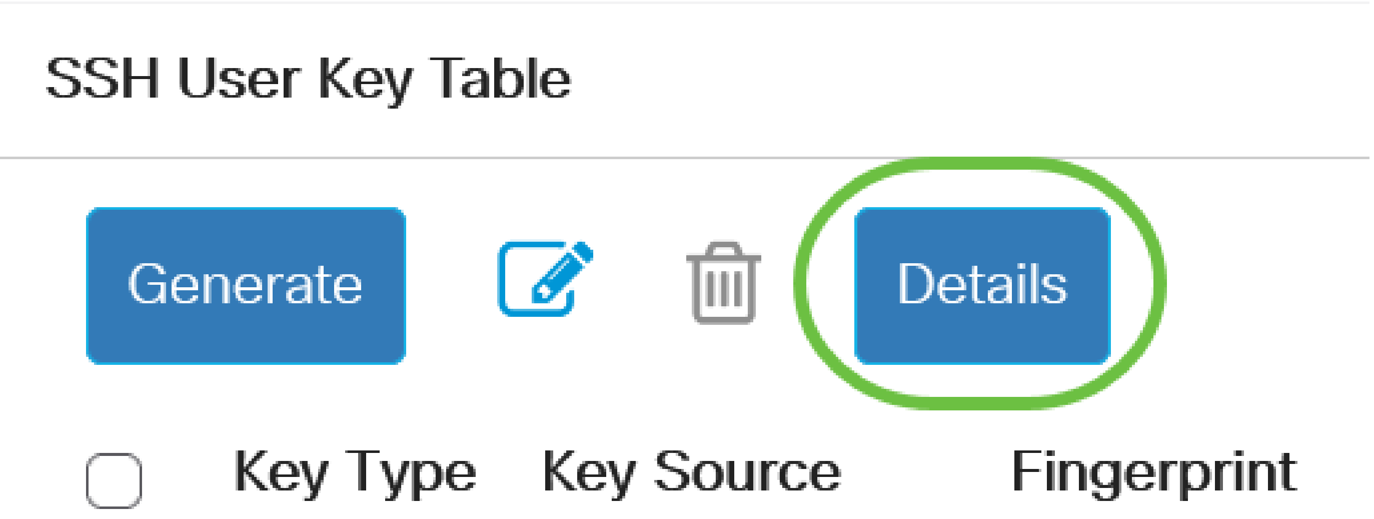
□	Key Type	Key Source	Fingerprint
☑	RSA	User Defined	MD5:02:26:b2:5c:56:51:b6:cf:db:fa:f7:b5:1a:26:7e:33
□	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

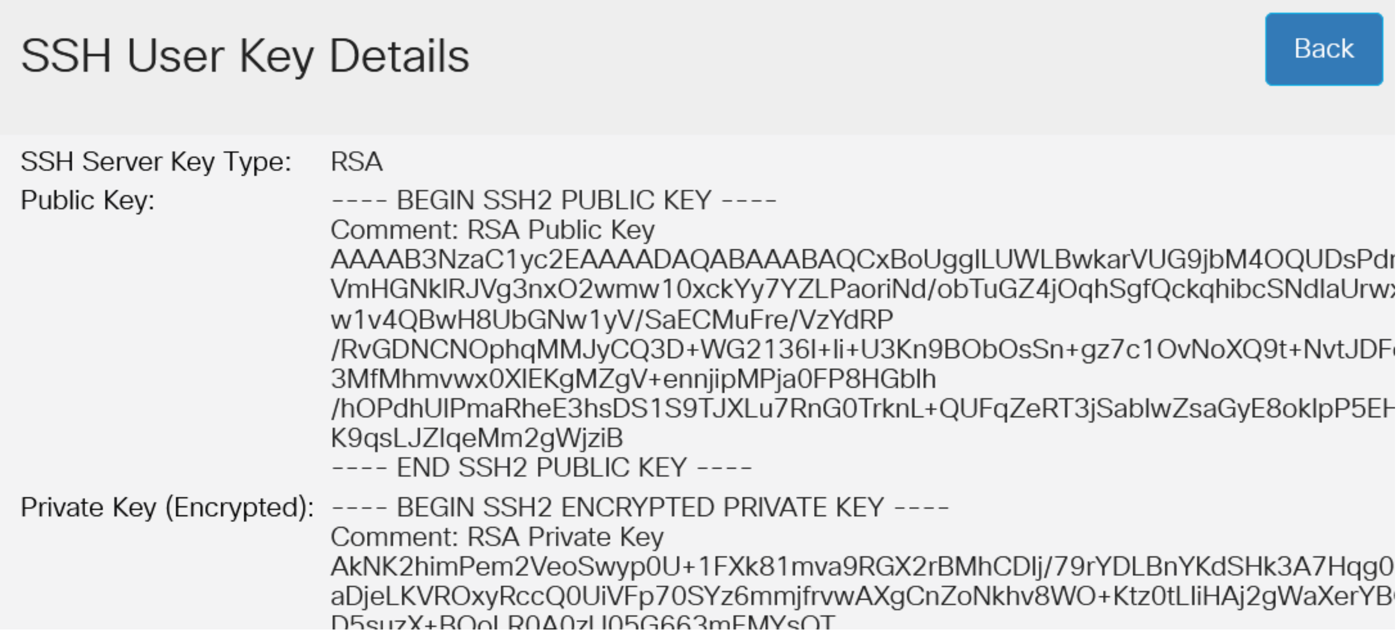
Step 18. (Optional) Once prompted by a confirmation message as shown below, click **OK** to delete the key.


Delete User Generated Key

The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?

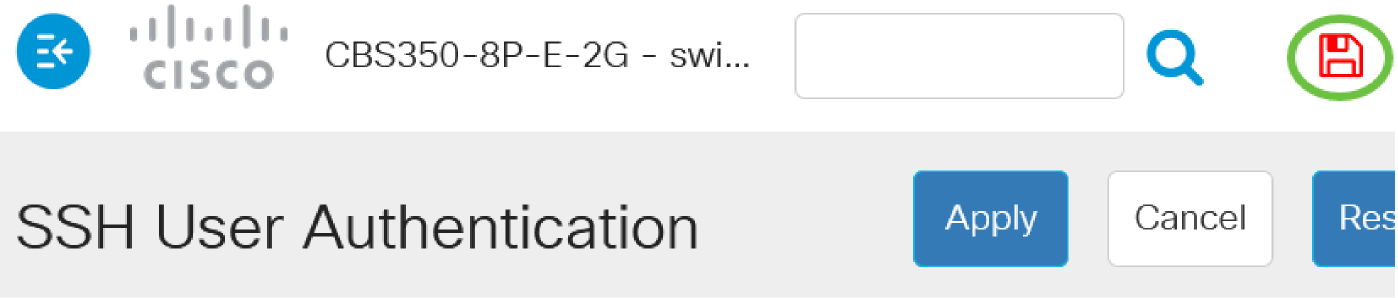
Step 19. (Optional) Click **Details** to see the details of the checked key.




SSH User Key Details

```
SSH Server Key Type:        RSA
Public Key:                 ---- BEGIN SSH2 PUBLIC KEY ----
                            Comment: RSA Public Key
                            AAAAB3NzaC1yc2EAAAADAQABAAABAQCxBoUggILUWLBwkarVUG9jbM4OQUDsPd
                            VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw
                            w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP
                            /RvGDNCNOphqMMJyCQ3D+WG2136I+li+U3Kn9BObOsSn+gz7c1OvNoXQ9t+NvtJDF
                            3MfMhmvwx0XIEKgMZgV+ennjipMPja0FP8HGblh
                            /hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8okIpP5E
                            K9qsLJZIqeMm2gWjziB
                            ---- END SSH2 PUBLIC KEY ----
Private Key (Encrypted):    ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
                            Comment: RSA Private Key
                            AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDIj/79rYDLBnYKdSHk3A7Hqg0
                            aDjeLKVROxyRccQ0UiVFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLIiHAj2gWaXerYB
                            D5suzX+BOoLR0A0zU05G663mEMYsOT
```

Step 20. (Optional) Click the **Save** button at the top portion of the page to save the changes to the startup configuration file.



You have now configured the client user authentication settings on your Cisco Business 350 series switch.