Konfigurieren der Secure Shell (SSH)-Benutzerauthentifizierungseinstellungen auf einem Cisco Business Switch der Serie 350

Ziel

Dieser Artikel enthält Anweisungen zum Konfigurieren der Client-Benutzerauthentifizierung auf Cisco Switches der Serie Business 350.

Einführung

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung mit bestimmten Netzwerkgeräten ermöglicht. Diese Verbindung stellt Funktionen bereit, die einer Telnet-Verbindung ähnlich sind, jedoch verschlüsselt sind. Mithilfe von SSH kann der Administrator den Switch über die Befehlszeilenschnittstelle (CLI) mit einem Drittanbieterprogramm konfigurieren.

Im CLI-Modus über SSH kann der Administrator erweiterte Konfigurationen in einer sicheren Verbindung ausführen. SSH-Verbindungen sind bei der Remote-Fehlerbehebung eines Netzwerks nützlich, wenn der Netzwerkadministrator nicht physisch am Netzwerkstandort anwesend ist. Mit dem Switch kann der Administrator Benutzer authentifizieren und verwalten, um über SSH eine Verbindung zum Netzwerk herzustellen. Die Authentifizierung erfolgt über einen öffentlichen Schlüssel, mit dem der Benutzer eine SSH-Verbindung zu einem bestimmten Netzwerk herstellen kann.

Die SSH-Clientfunktion ist eine Anwendung, die über das SSH-Protokoll ausgeführt wird, um Geräteauthentifizierung und -verschlüsselung bereitzustellen. Sie ermöglicht es einem Gerät, eine sichere und verschlüsselte Verbindung zu einem anderen Gerät herzustellen, das den SSH-Server ausführt. Mit Authentifizierung und Verschlüsselung ermöglicht der SSH-Client eine sichere Kommunikation über eine unsichere Telnet-Verbindung.

Unterstützte Geräte | Softwareversion

- CBS 350 (Datenblatt) | 3.0.0.69 (Laden Sie die aktuelle Version herunter)
- CBS350-2X (Datenblatt) | 3.0.0.69 (Laden Sie die aktuelle Version herunter)
- CBS350-4X (Datenblatt) | 3.0.0.69 (Laden Sie die aktuelle Version herunter)

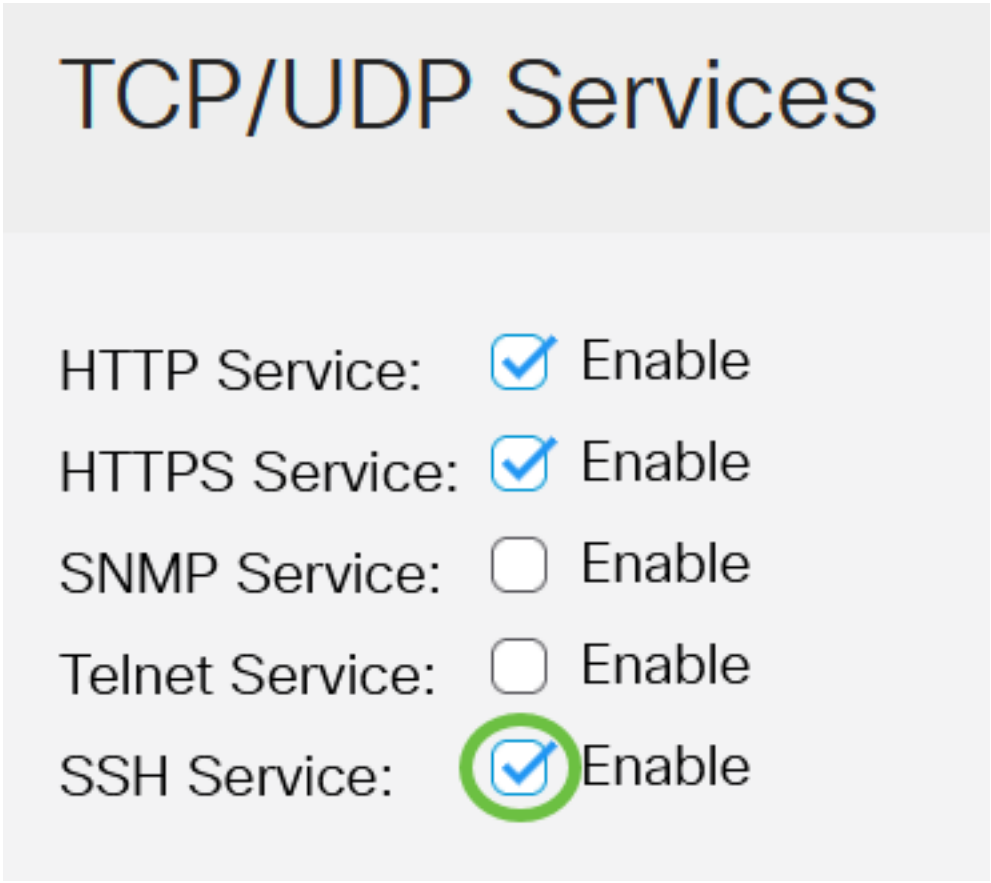
Konfigurieren der Authentifizierungseinstellungen für den SSH-Client

SSH-Dienst aktivieren

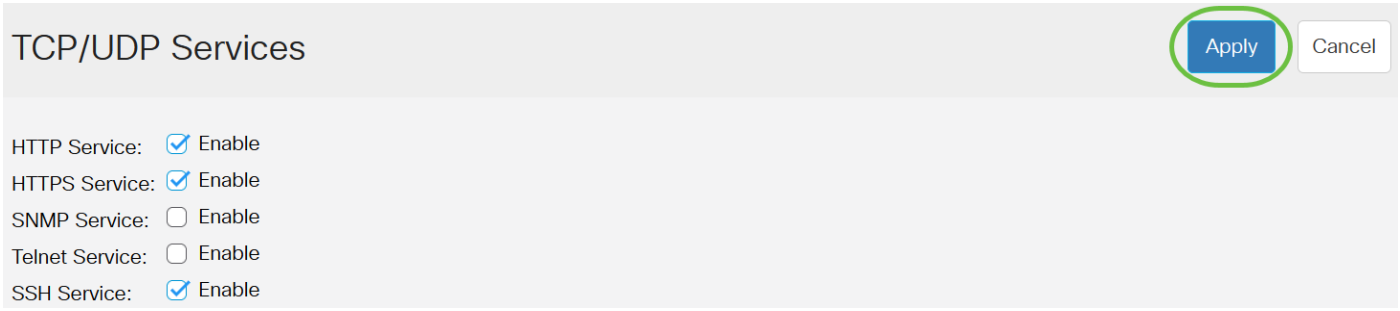
Zur Unterstützung der automatischen Konfiguration eines Out-of-Box-Geräts (Gerät mit werksseitiger Standardkonfiguration) ist die SSH-Serverauthentifizierung standardmäßig deaktiviert.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > TCP/UDP Services aus.**

Schritt 2: Aktivieren Sie das Kontrollkästchen **SSH-Service**, um den Zugriff auf die Switch-Eingabeaufforderung über SSH zu aktivieren.



Schritt 3: Klicken Sie auf **Apply**, um den SSH-Dienst zu aktivieren.

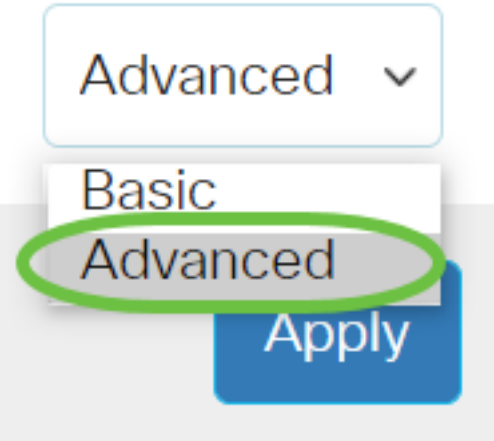


Konfigurieren der Authentifizierungseinstellungen für SSH-Benutzer

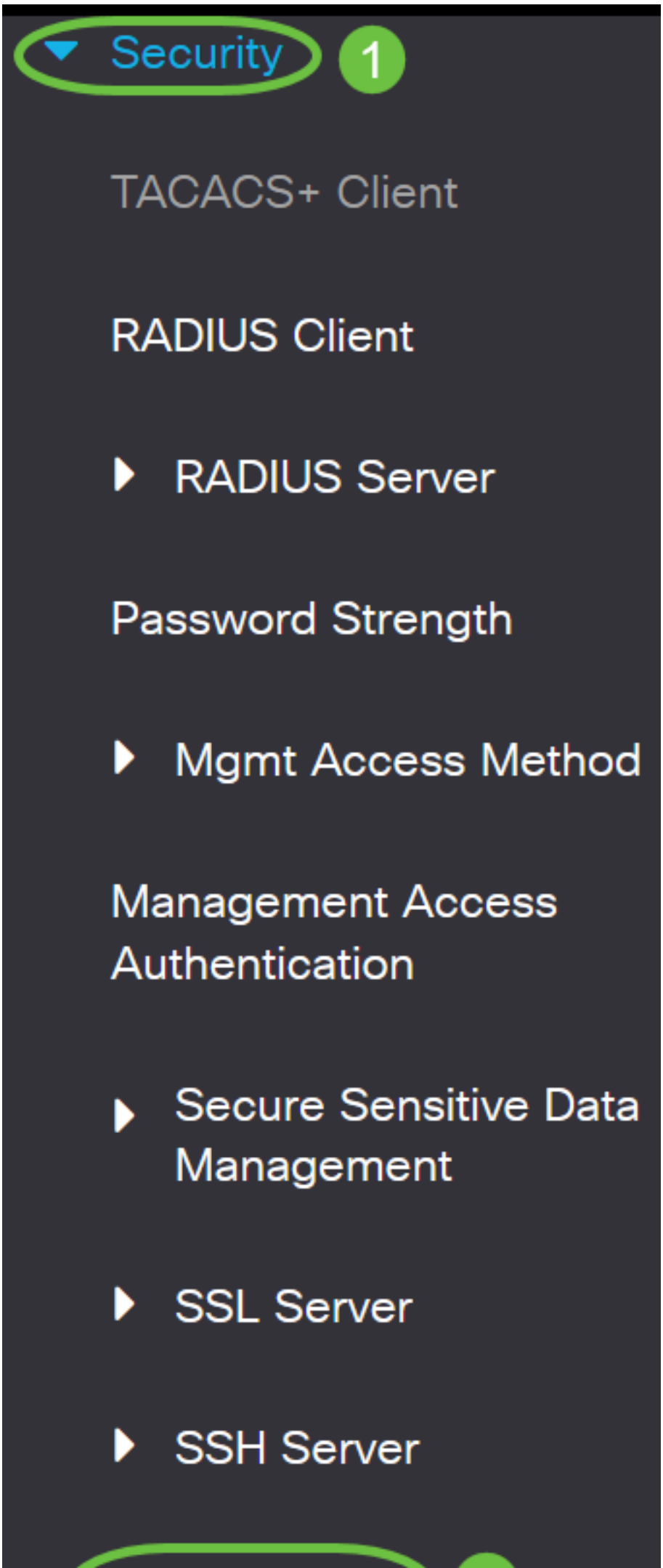
Wählen Sie auf dieser Seite eine SSH-Benutzerauthentifizierungsmethode aus. Sie können einen Benutzernamen und ein Kennwort auf dem Gerät festlegen, wenn Sie die Kennwortmethode auswählen. Sie können auch einen Ron Rivest-, Adi Shamir- und Leonard Adleman-Schlüssel (RSA) oder einen DSA-Schlüssel (Digital Signature Algorithm) generieren, wenn die Methode des öffentlichen oder privaten Schlüssels ausgewählt ist.

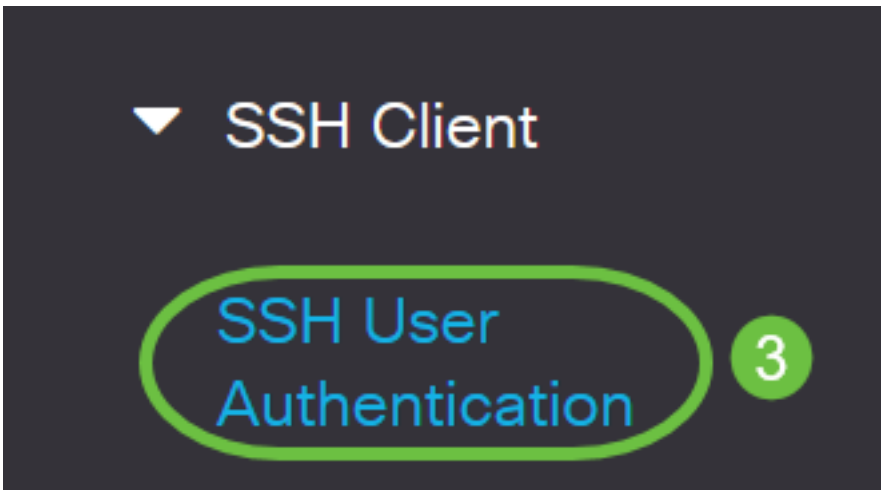
Beim Booten werden für das Gerät RSA- und DSA-Standardschlüsselpaare generiert. Einer dieser Schlüssel wird zur Verschlüsselung der Daten verwendet, die vom SSH-Server heruntergeladen werden. Der RSA-Schlüssel wird standardmäßig verwendet. Wenn der Benutzer eine oder beide Schlüssel löscht, werden diese neu generiert.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an, und wählen Sie dann in der Dropdown-Liste Anzeigemodus die Option Erweitert aus.

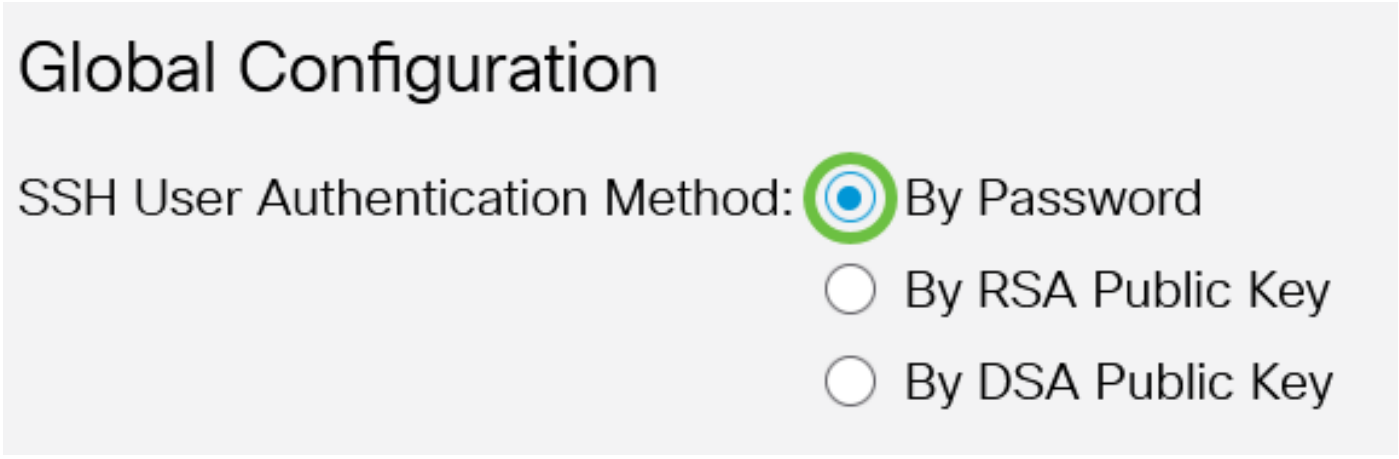


Schritt 2: Wählen Sie **Security > SSH Client > SSH User Authentication** (Sicherheit > SSH-Client > SSH-Benutzerauthentifizierung) aus dem Menü aus.


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



Schritt 3: Klicken Sie unter "Globale Konfiguration" auf die gewünschte SSH-Benutzerauthentifizierungsmethode.



Wenn ein Gerät (SSH-Client) versucht, eine SSH-Sitzung zum SSH-Server einzurichten, verwendet der SSH-Server eine der folgenden Methoden für die Client-Authentifizierung:

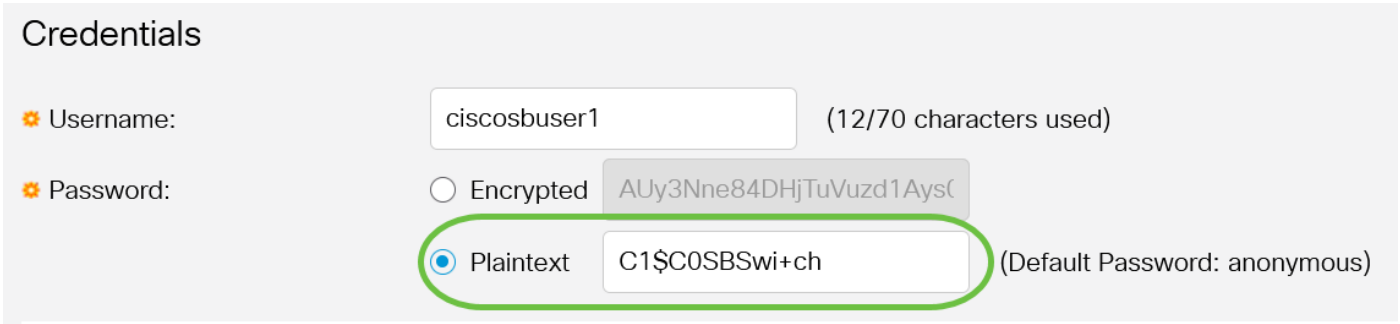
- By Password (Kennwort) - Mit dieser Option können Sie ein Kennwort für die Benutzerauthentifizierung konfigurieren. Dies ist die Standardeinstellung, und das Standardkennwort ist anonym. Wenn diese Option ausgewählt ist, stellen Sie sicher, dass der Benutzername und die Anmeldeinformationen für das Kennwort auf dem SSH-Server festgelegt wurden.
- By RSA Public Key (Öffentlicher RSA-Schlüssel) - Mit dieser Option können Sie den öffentlichen RSA-Schlüssel für die Benutzerauthentifizierung verwenden. Ein RSA-Schlüssel ist ein verschlüsselter Schlüssel, der auf der Faktorisierung großer Ganzzahlen basiert. Dieser Schlüssel ist der gängigste Schlüssel für die SSH-Benutzerauthentifizierung.
- By DSA Public Key (Öffentlicher DSA-Schlüssel) - Mit dieser Option können Sie einen öffentlichen DSA-Schlüssel für die Benutzerauthentifizierung verwenden. Ein DSA-Schlüssel ist ein verschlüsselter Schlüssel, der auf dem diskreten ElGamal-Algorithmus basiert. Dieser Schlüssel wird normalerweise nicht für die SSH-Benutzerauthentifizierung verwendet, da der Authentifizierungsprozess mehr Zeit in Anspruch nimmt.

In diesem Beispiel wird By Password (Kennwort) ausgewählt.

Schritt 4: Geben Sie im Bereich Anmeldeinformationen im Feld *Benutzername* den Benutzernamen ein.

In diesem Beispiel wird ciscosbuser1 verwendet.

Schritt 5: (Optional) Wenn Sie in Schritt 2 die Option By Password (Kennwort) ausgewählt haben, klicken Sie auf die Methode, und geben Sie das Kennwort in das Feld *Encrypted (Verschlüsselt)* oder *Plaintext* ein.

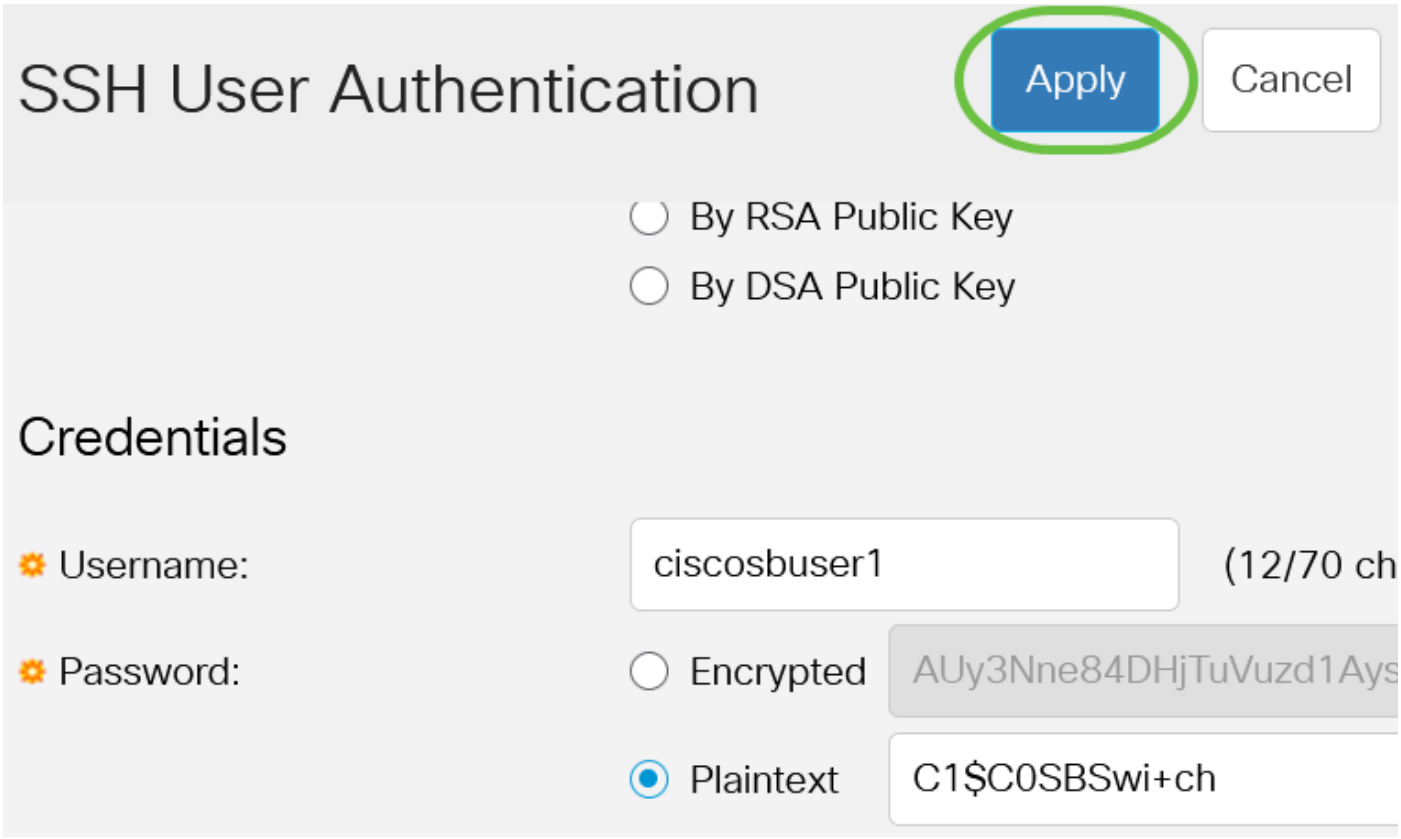


Folgende Optionen sind verfügbar:

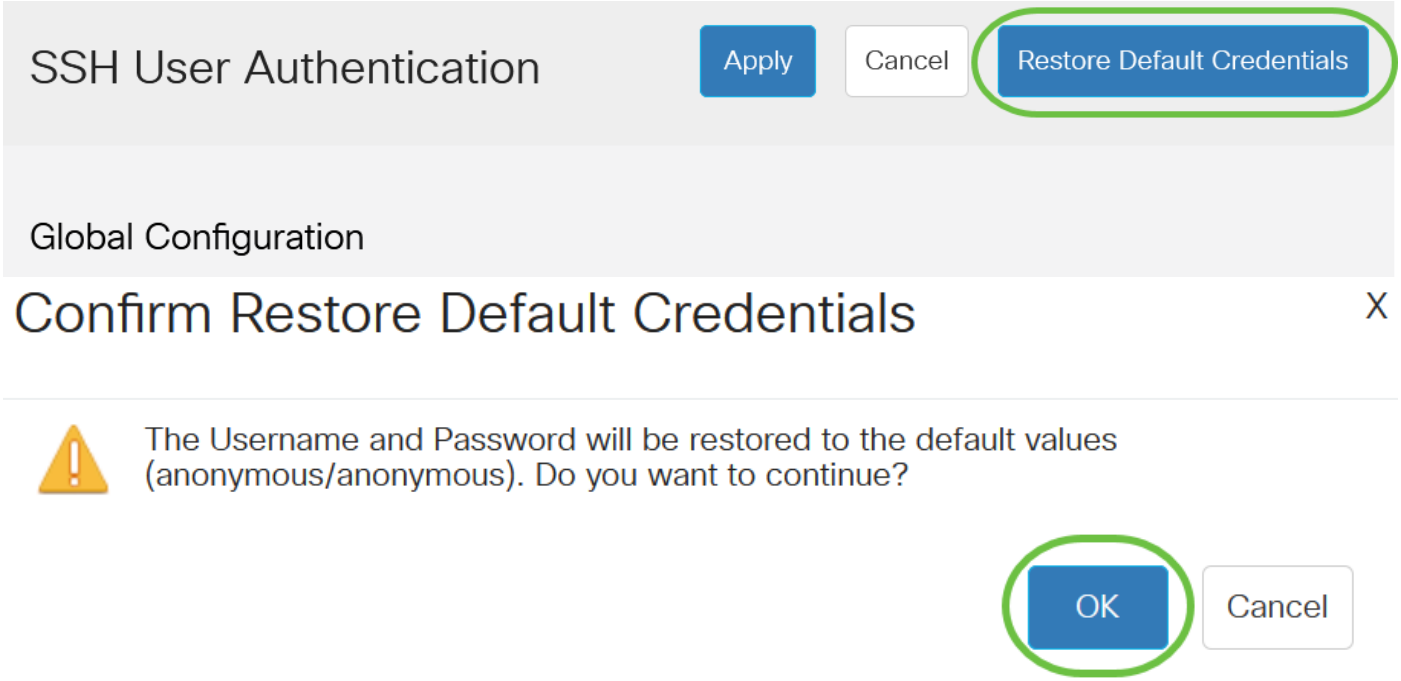
- Verschlüsselt - Mit dieser Option können Sie eine verschlüsselte Version des Kennworts eingeben.
- Plaintext: Mit dieser Option können Sie ein Passwort im Klartext eingeben.

In diesem Beispiel wird Plaintext gewählt und ein Passwort für einfachen Text eingegeben.

Schritt 6: Klicken Sie auf **Apply**, um die Authentifizierungskonfiguration zu speichern.

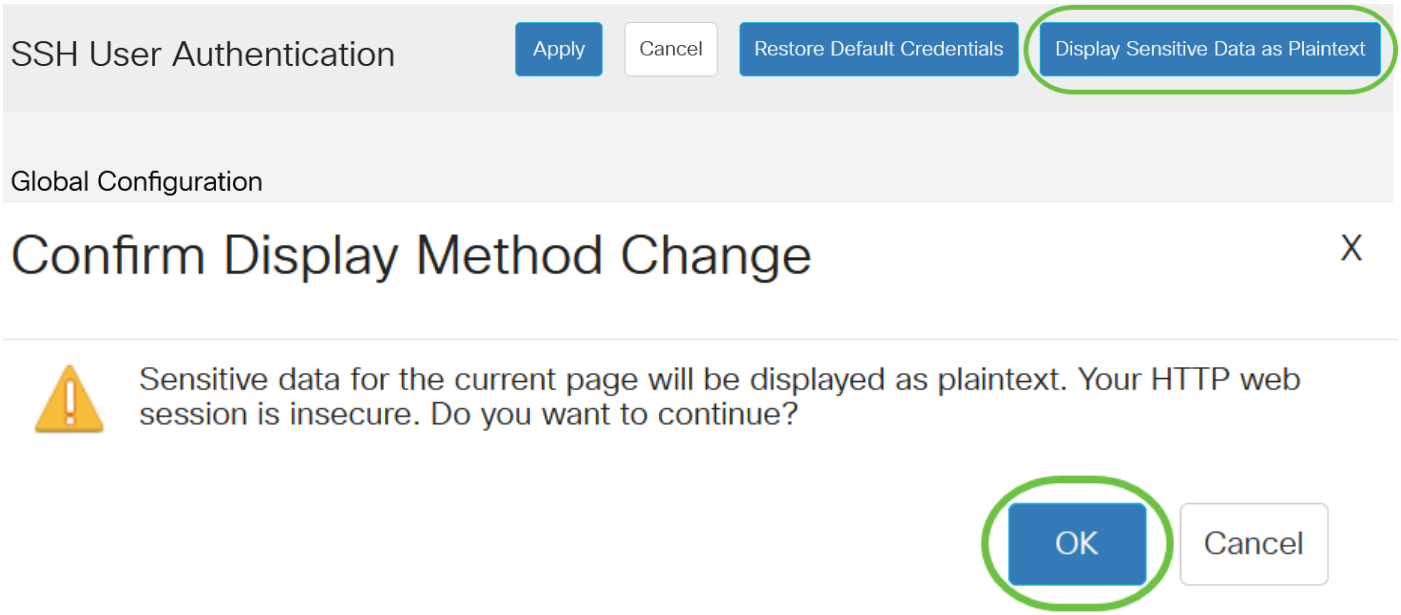


Schritt 7: (Optional) Klicken Sie auf **Standardanmeldeinformationen wiederherstellen**, um den Standardbenutzernamen und das Standardkennwort wiederherzustellen. Klicken Sie anschließend auf **OK**, um fortzufahren.



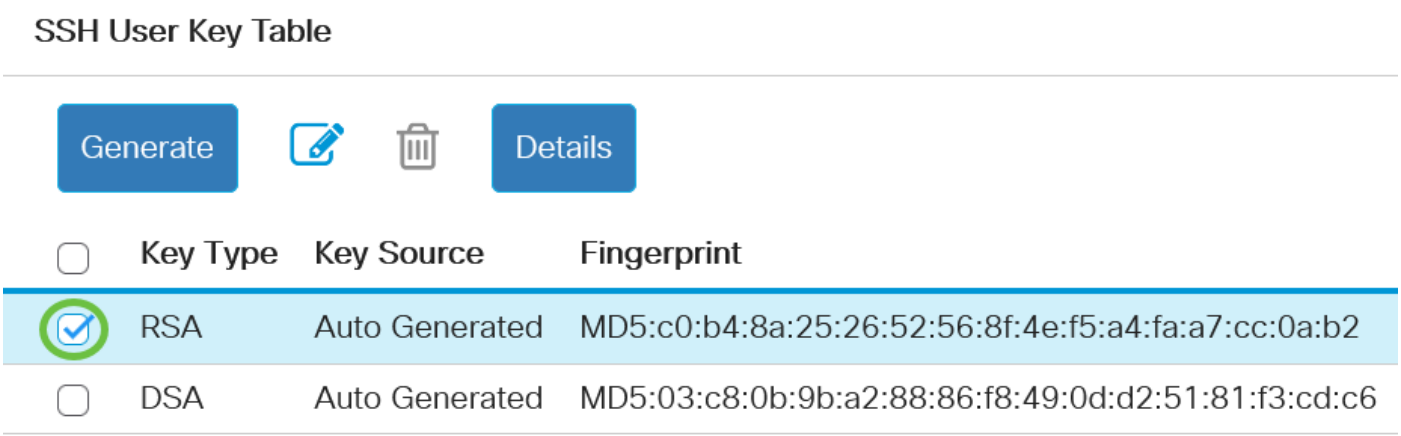
Der Benutzername und das Kennwort werden auf die Standardwerte zurückgesetzt: anonym/anonym.

Schritt 8: (Optional) Klicken Sie auf **Sensitive Daten als Nur-Text anzeigen**, um die sensiblen Daten der Seite im Textformat anzuzeigen, und klicken Sie dann auf **OK**, um fortzufahren.



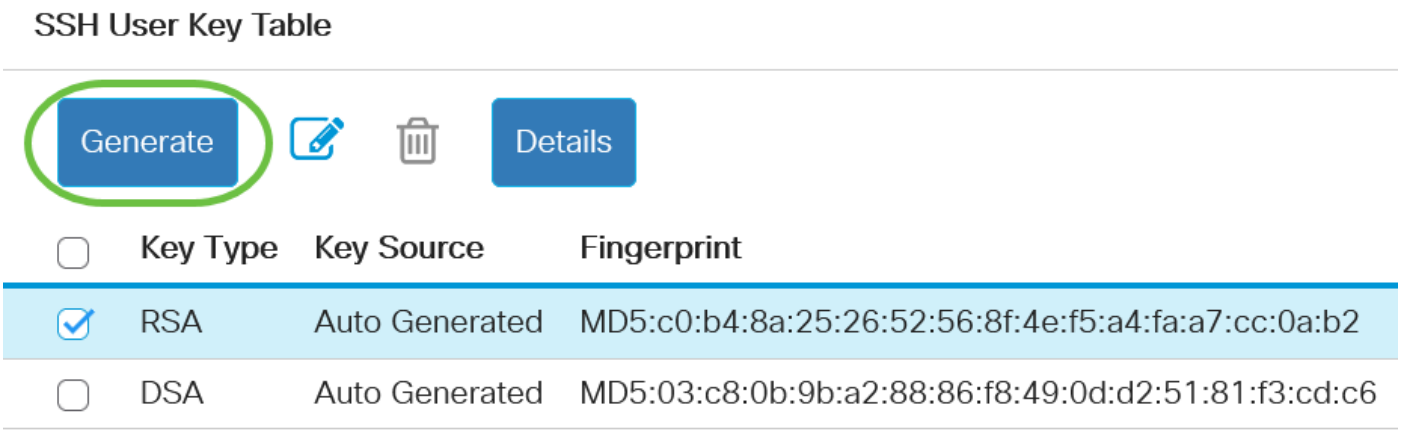
Konfigurieren der SSH-Benutzerschlüsseltabelle

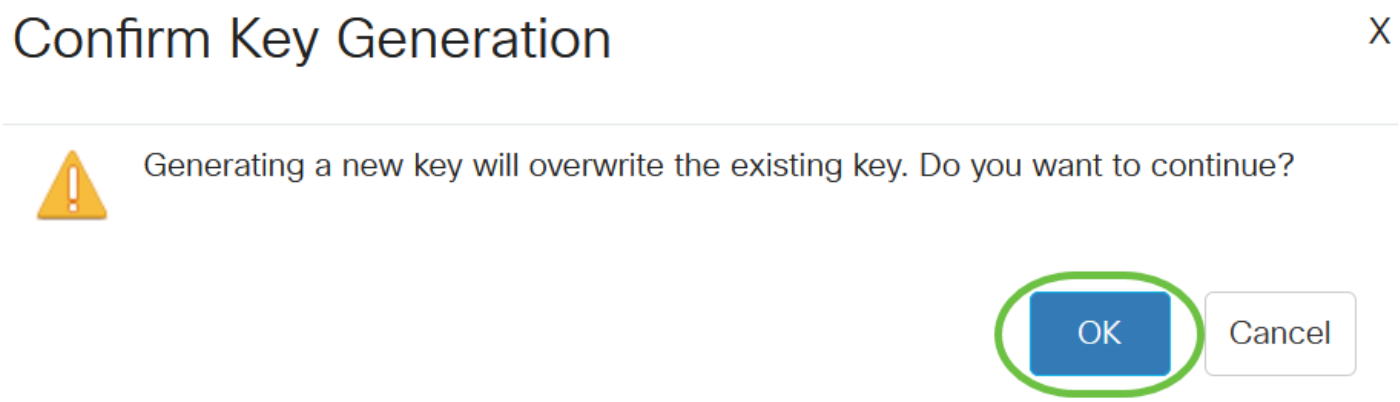
Schritt 9: Aktivieren Sie das Kontrollkästchen des Schlüssels, den Sie verwalten möchten.



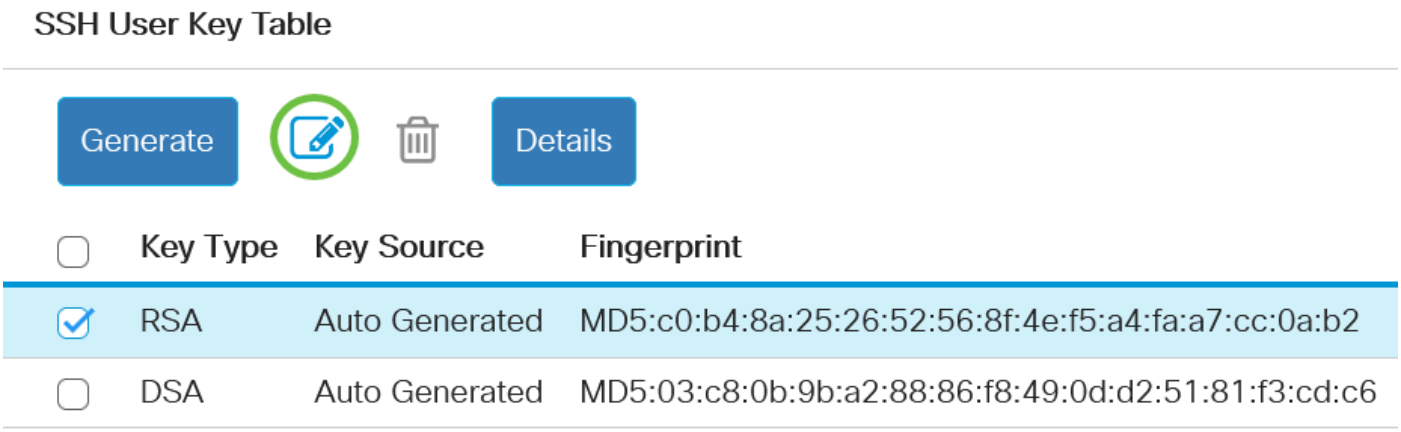
In diesem Beispiel wird RSA ausgewählt.

Schritt 10: (Optional) Klicken Sie auf **Generate (Generieren)**, um einen neuen Schlüssel zu generieren. Der neue Schlüssel überschreibt die aktivierte Taste und klickt dann auf **OK**, um fortzufahren.

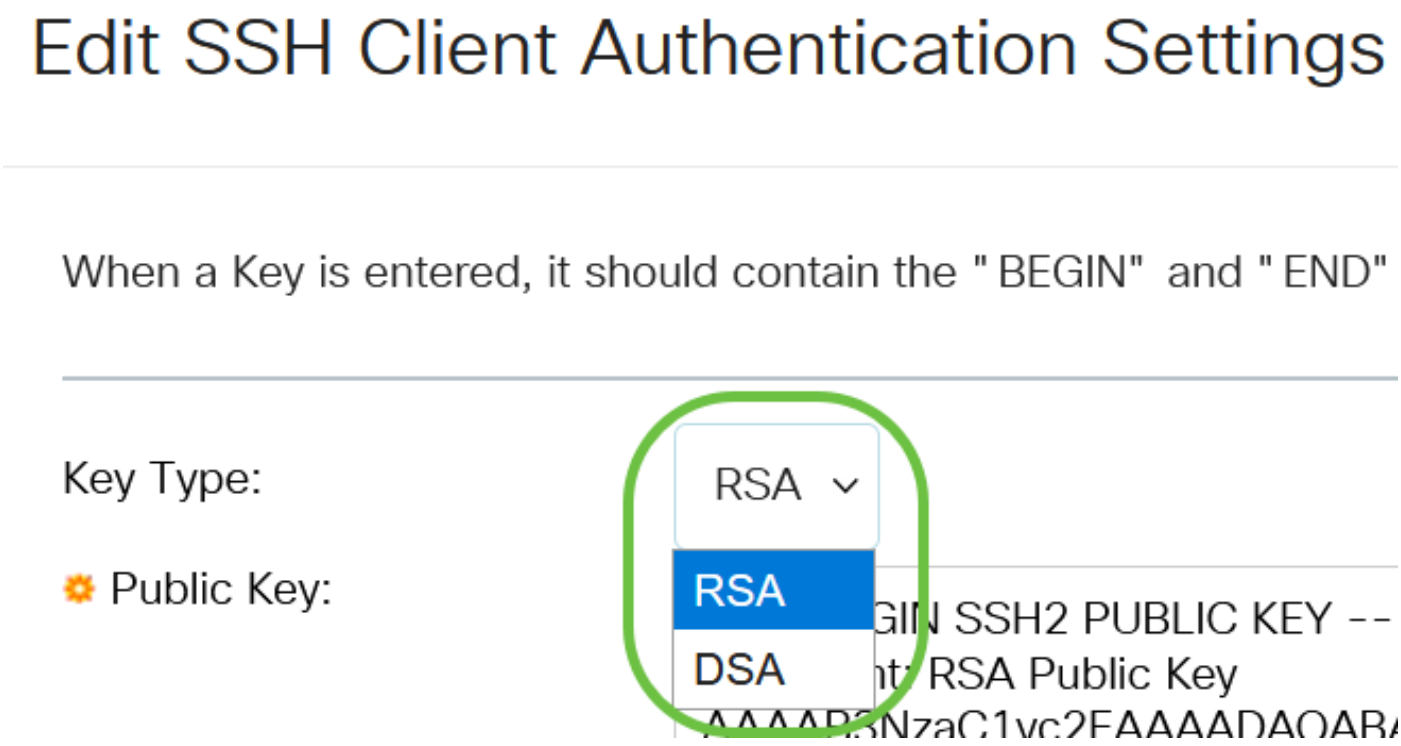




Schritt 11: (Optional) Klicken Sie auf **Bearbeiten**, um einen aktuellen Schlüssel zu bearbeiten.

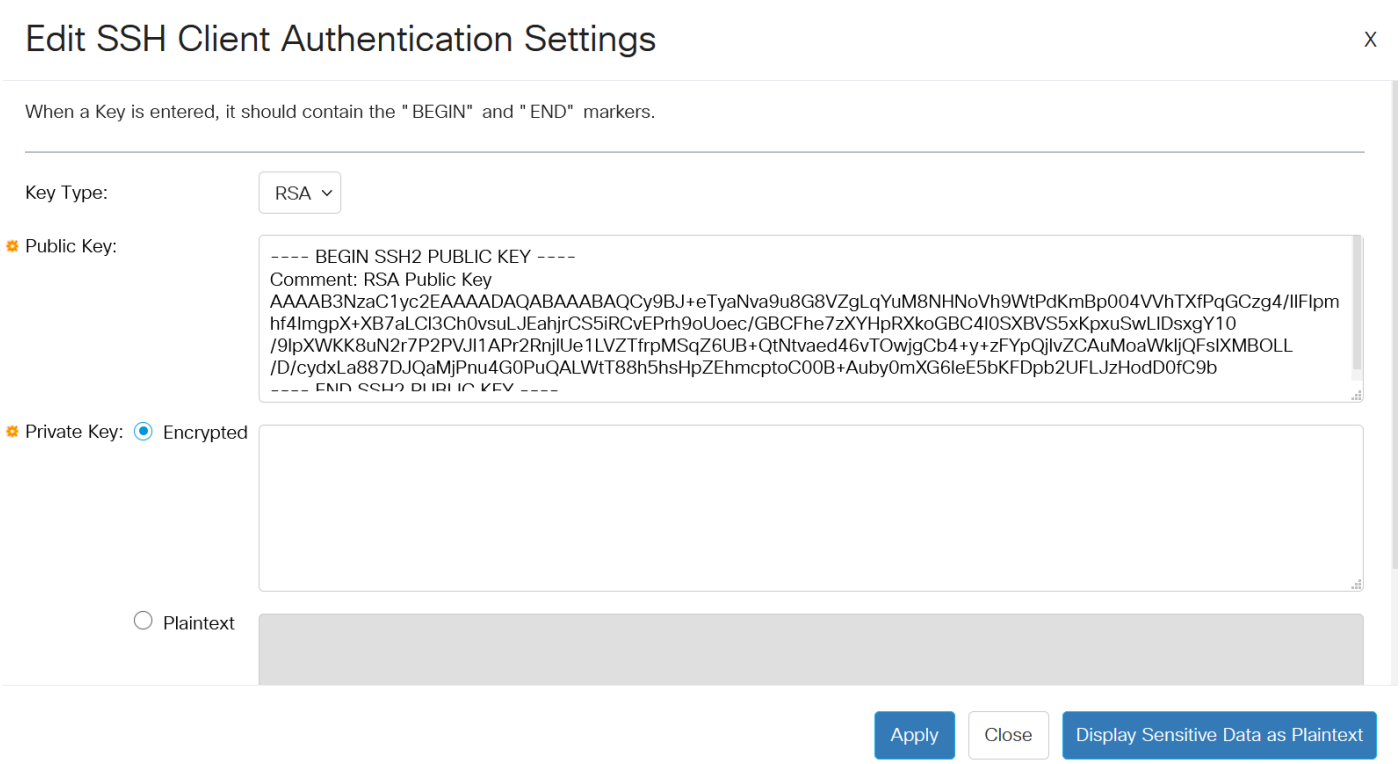


Schritt 12: (Optional) Wählen Sie in der Dropdown-Liste Key Type (Schlüsseltyp) einen Schlüsseltyp aus.



In diesem Beispiel wird RSA ausgewählt.

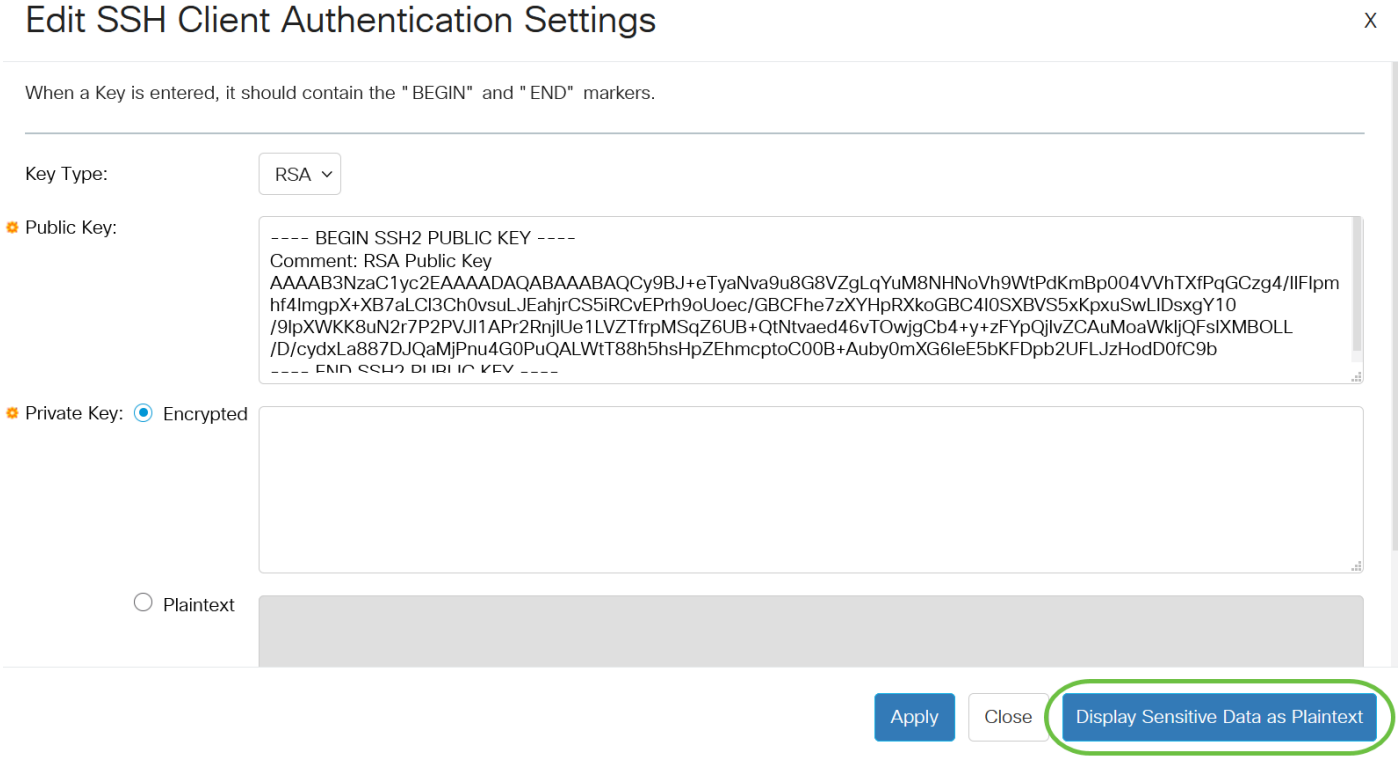
Schritt 13: (Optional) Geben Sie den neuen öffentlichen Schlüssel in das Feld *Öffentlicher Schlüssel ein*.

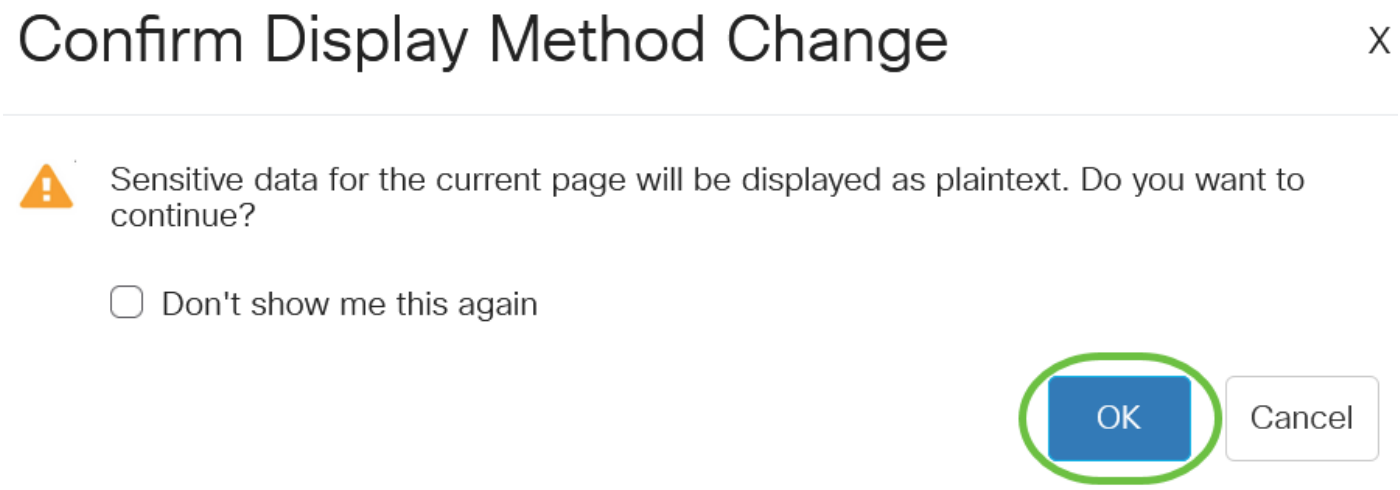


Schritt 14: (Optional) Geben Sie den neuen privaten Schlüssel in das Feld *Privater Schlüssel ein*.

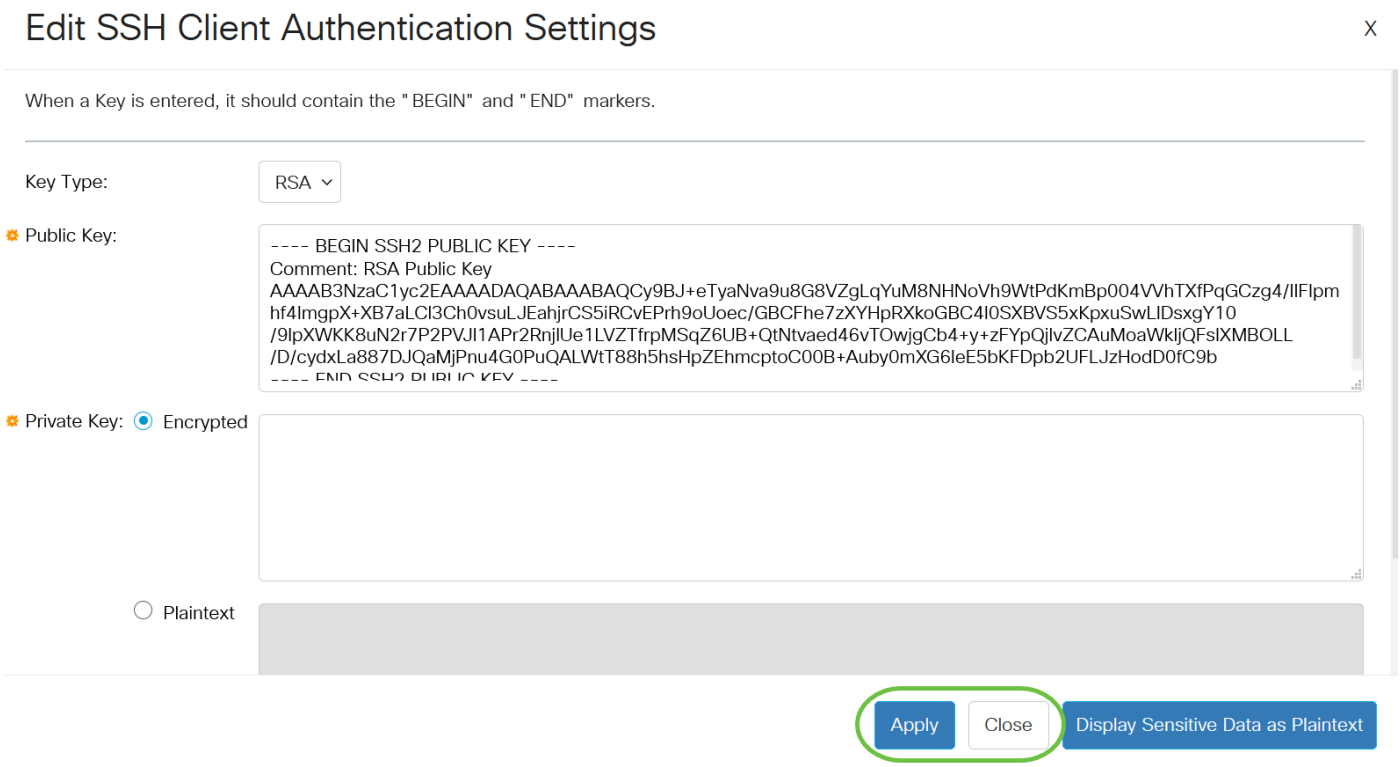
Sie können den privaten Schlüssel bearbeiten und auf Verschlüsselt klicken, um den aktuellen privaten Schlüssel als verschlüsselten Text anzuzeigen, oder auf Nur-Text, um den aktuellen privaten Schlüssel im Klartext anzuzeigen.

Schritt 15: (Optional) Klicken Sie auf **Sensitive Daten als Nur-Text anzeigen**, um die verschlüsselten Daten der Seite im Textformat anzuzeigen, und klicken Sie dann auf **OK**, um fortzufahren.

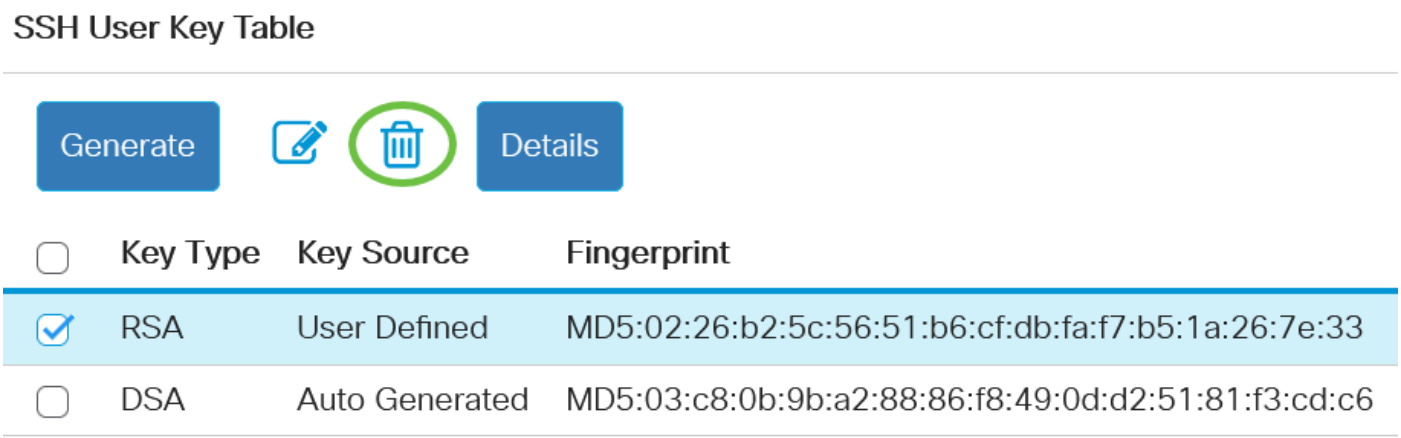




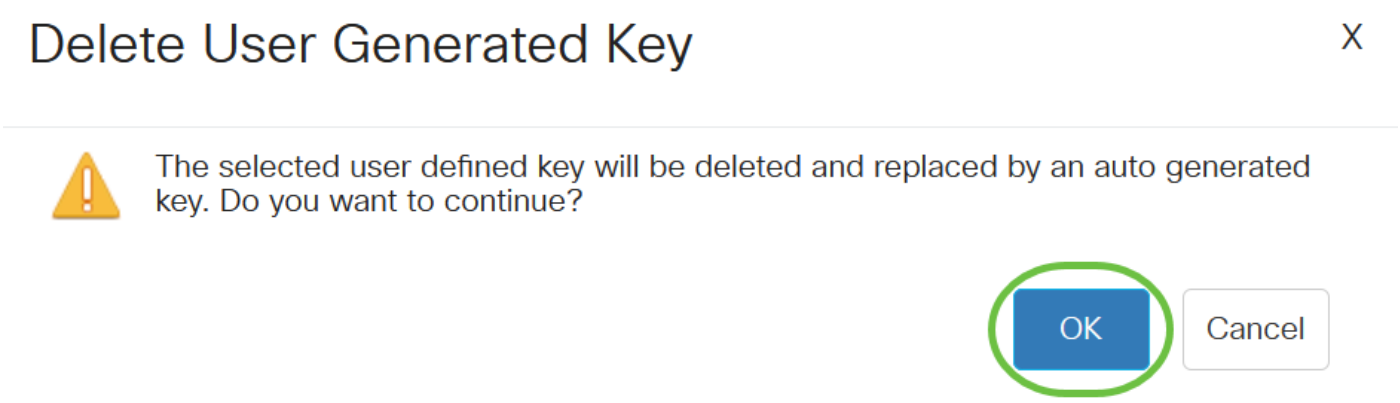
Schritt 16: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, und klicken Sie dann auf **Schließen**.



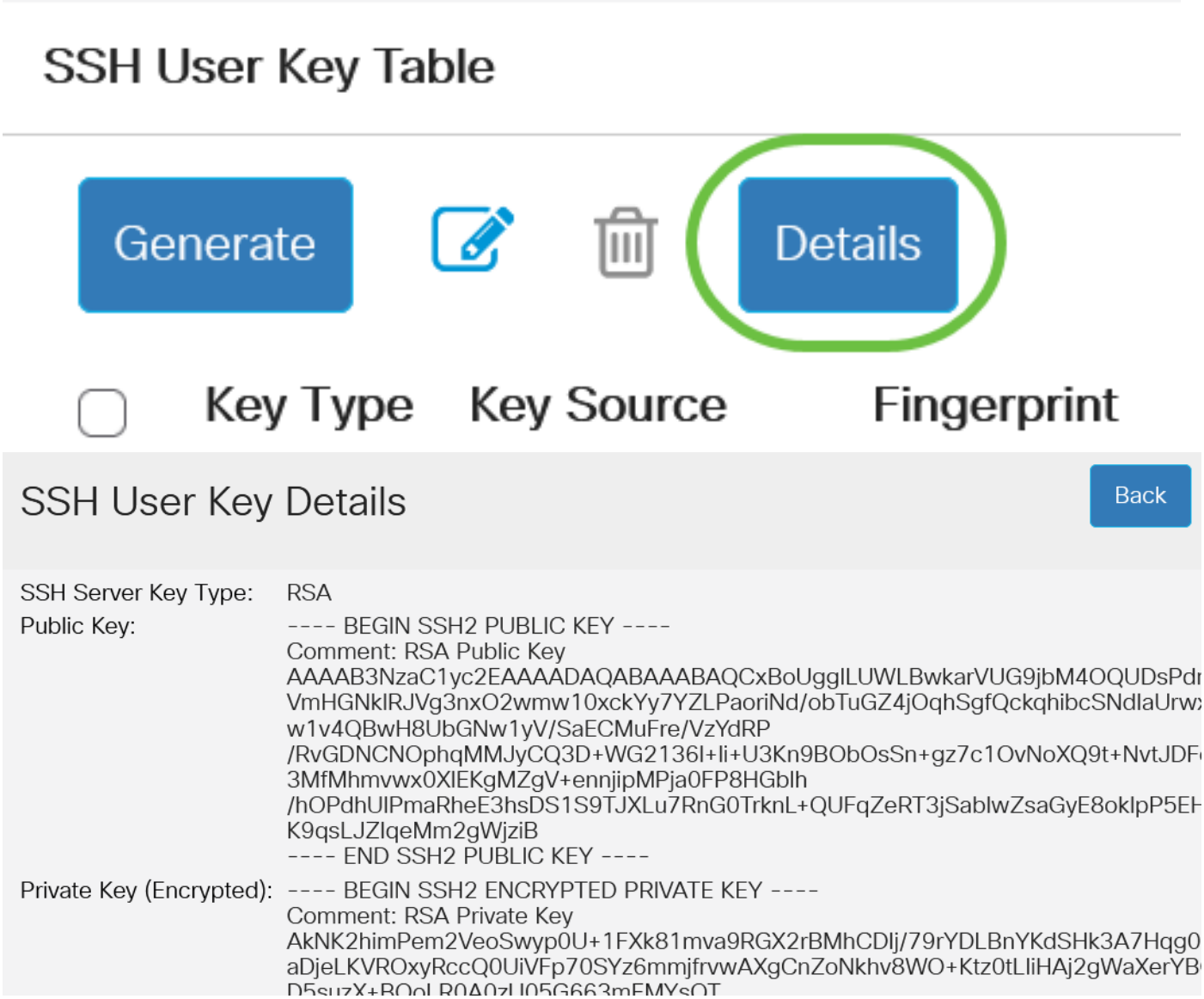
Schritt 17: (Optional) Klicken Sie auf **Löschen**, um den aktivierten Schlüssel zu löschen.



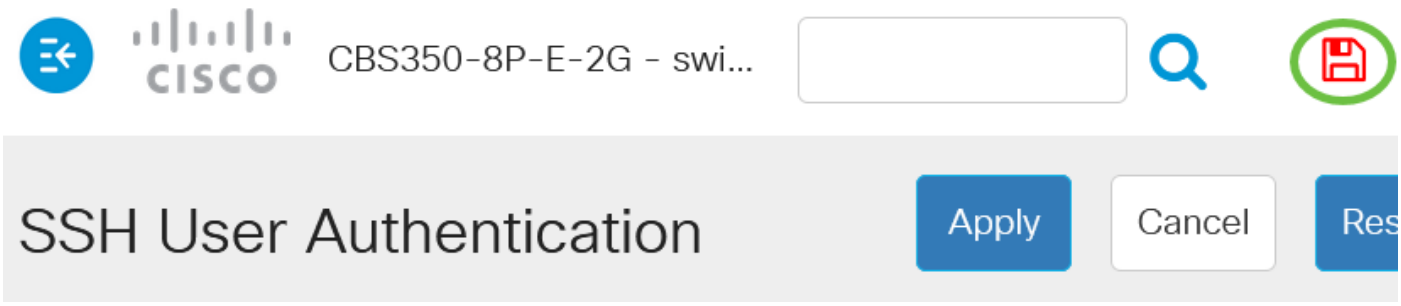
Schritt 18: (Optional) Klicken Sie nach Aufforderung durch eine Bestätigungsmeldung, wie unten gezeigt, auf **OK**, um den Schlüssel zu löschen.



Schritt 19: (Optional) Klicken Sie auf **Details**, um die Details des aktivierten Schlüssels anzuzeigen.



Schritt 20: (Optional) Klicken Sie auf die Schaltfläche **Speichern** am oberen Seitenrand, um die Änderungen in der Startkonfigurationsdatei zu speichern.



Sie haben jetzt die Einstellungen für die Client-Benutzerauthentifizierung auf Ihrem Cisco Switch der Serie Business 350 konfiguriert.