

# 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

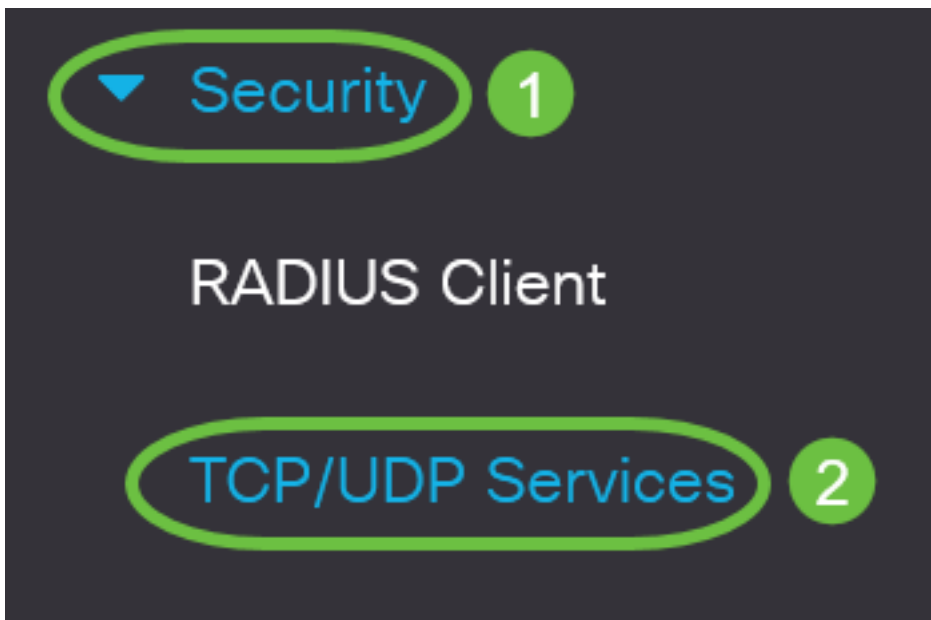
- CBS 350 ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-2X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))
- CBS350-4X ([Datenblatt](#)) | 3.0.0.69 ([Laden Sie die aktuelle Version herunter](#))

## Konfigurieren der Authentifizierungseinstellungen für den SSH-Client

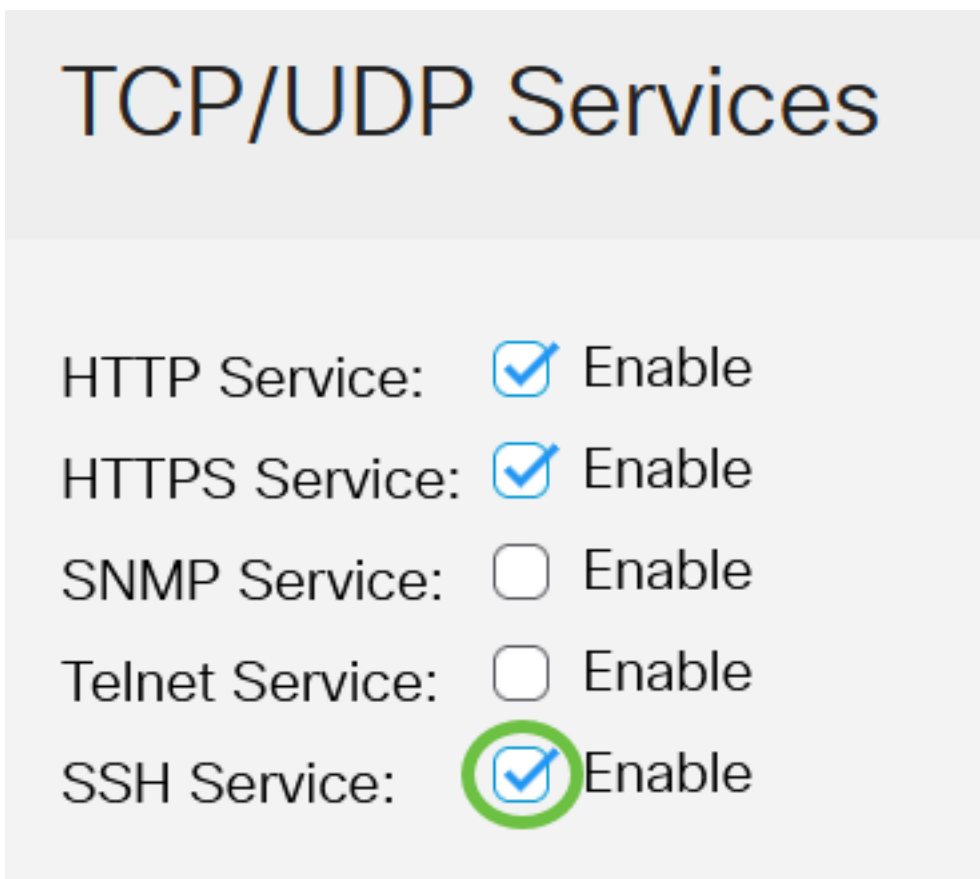
### SSH-Dienst aktivieren

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

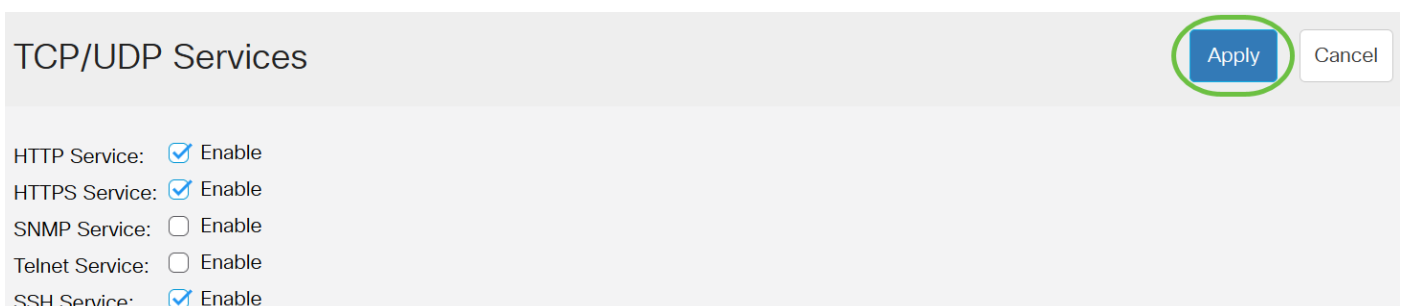
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > TCP/UDP Services aus**.



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.

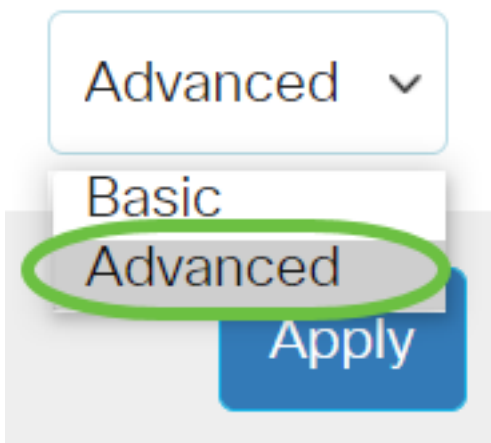


**Konfigurieren der Authentifizierungseinstellungen für SSH-Benutzer**

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

## ▼ SSH Client

SSH User  
Authentication

3

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

## Global Configuration

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

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.

## Credentials

✦ Username:  (12/70 characters used)

✦ Password:  Encrypted

Plaintext  (Default Password: anonymous)

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.

## Credentials

✦ Username:  (12/70 characters used)

✦ Password:  Encrypted

Plaintext  (Default Password: anonymous)

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.

# SSH User Authentication

Apply

Cancel

By RSA Public Key

By DSA Public Key

## Credentials

Username:

ciscosbuser1

(12/70 ch

Password:

Encrypted

AUy3Nne84DHjTuVuzd1Ays

Plaintext

C1\$C0SBSwi+ch

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

# SSH User Authentication

Apply

Cancel

Restore Default Credentials

Global Configuration

## Confirm Restore Default Credentials

X



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

OK

Cancel

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.

## Confirm Display Method Change



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

OK

Cancel

### Konfigurieren der SSH-Benutzerschlüsseltabelle

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

#### SSH User Key Table

Generate



Details

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 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.

#### SSH User Key Table

Generate



Details

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

X



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



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

## SSH User Key Table



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

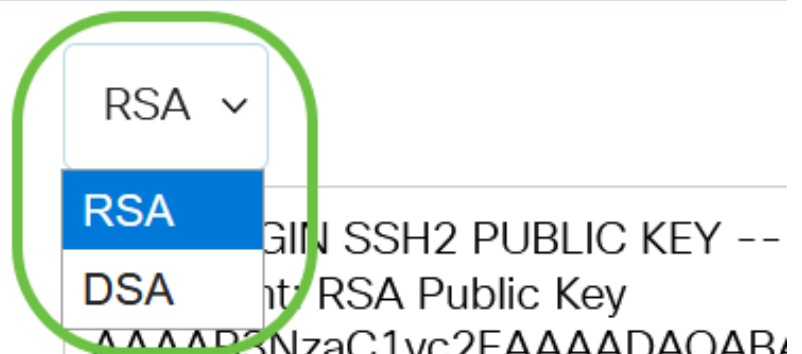
Schritt 12: (Optional) Wählen Sie in der Dropdown-Liste Key Type (Schlüsseltyp) einen Schlüsseltyp aus.

# Edit SSH Client Authentication Settings

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

Key Type:

Public Key:



In diesem Beispiel wird RSA ausgewählt.

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

## Edit SSH Client Authentication Settings

X

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

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.

## Edit SSH Client Authentication Settings

X

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

# Confirm Display Method Change

X



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

Don't show me this again



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

## Edit SSH Client Authentication Settings

X

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

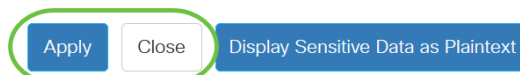
Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHPrXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJl1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWt88h5hsHpZEHmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext



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

## SSH User Key Table



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

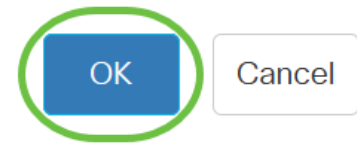
Schritt 18: (Optional) Klicken Sie nach Aufforderung durch eine Bestätigungsmeldung, wie unten gezeigt, auf **OK**, um den Schlüssel zu löschen.

# Delete User Generated Key

X

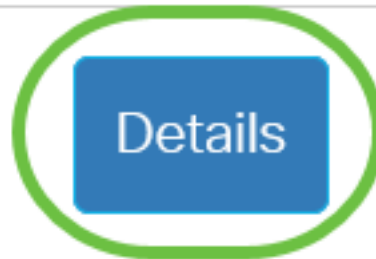


The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



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

## SSH User Key Table



Key Type

Key Source

Fingerprint

### SSH User Key Details

Back

SSH Server Key Type: RSA  
Public Key: ----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQ=CxBoUggILUWLBwkarVUG9jbM4OQUdsPdr  
VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhbcSNdlaUrw;  
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP  
/RvGDNCNOphqMM.JyCQ3D+WG2136I+li+U3Kn9BOBosSn+gz7c1OvNoXQ9t+NvtJDF-  
3MfMhmvwX0XIEKgMZgV+ennjipMPja0FP8HGblh  
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E-  
K9qsLJZlqeMm2gWjziB  
----- END SSH2 PUBLIC KEY -----  
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----  
Comment: RSA Private Key  
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDIj/79rYDLBnYKdSHk3A7Hqg0  
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLliHAj2gWaXerYB-  
D5suZx+BOqL R0A0zL I05G663mEMVcOT

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



CBS350-8P-E-2G - swi...



## SSH User Authentication

Apply

Cancel

Res

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