

# Client Secure Shell (SSH)- Benutzerauthentifizierung für die SG350XG- und SG550XG-Switches

## Ziel

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung mit einem bestimmten Gerät bereitstellt. Mit den Managed Switches der Serien 350XG und 550XG können Benutzer authentifiziert und verwaltet werden, um eine Verbindung zum Gerät über SSH herzustellen. Die Authentifizierung erfolgt über einen öffentlichen Schlüssel, sodass der Benutzer mit diesem Schlüssel eine SSH-Verbindung zu einem bestimmten Gerät herstellen kann. SSH-Verbindungen sind nützlich, um Fehler in einem Netzwerk remote zu beheben, falls sich der Netzwerkadministrator nicht am Netzwerkstandort befindet.

In diesem Artikel wird die Konfiguration der Client-Benutzerauthentifizierung für die Managed Switches der Serien SG350XG und SG550XG erläutert.

## Anwendbare Geräte

- SG350XG
- SG550XG

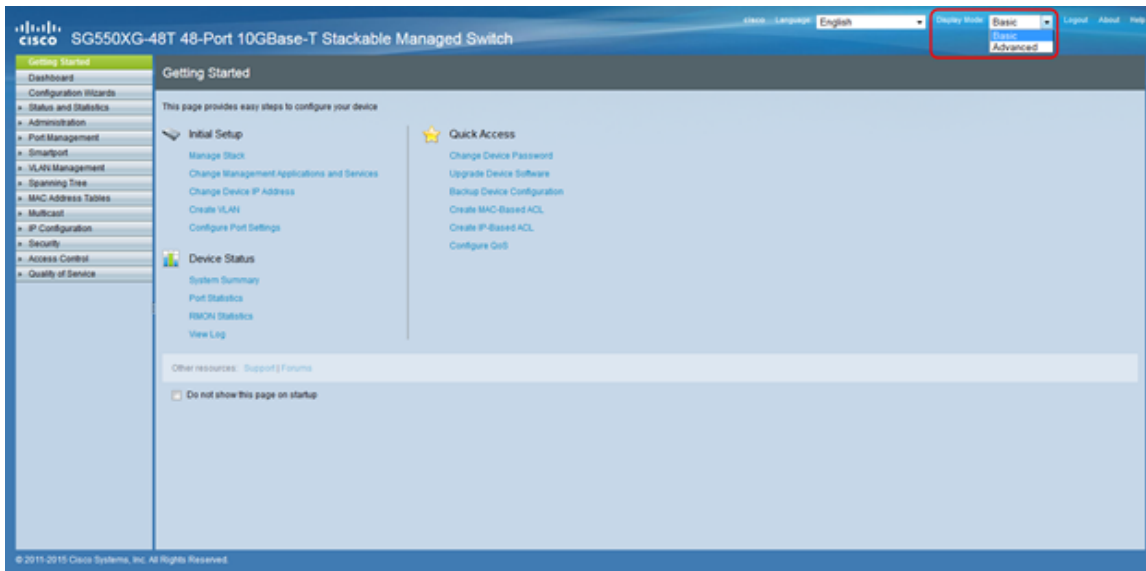
## Softwareversion

- V2.0.0.73

## SSH konfigurieren Client Authentifizierung

### Globale Konfiguration

**Hinweis:** Die folgenden Screenshots stammen aus dem Advanced Display. Sie können dies umschalten, indem Sie auf die Dropdown-Liste *Anzeigemodus* oben rechts im Bildschirm klicken.



Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > SSH Client > SSH User Authentication** aus. Die Seite *SSH-Benutzerauthentifizierung* wird geöffnet:

### SSH User Authentication

**Global Configuration**

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

**Credentials**

✦ Username:  (0/70 characters used)

✦ Password:  Encrypted   
 Plaintext  (Default Password: anonymous)

**SSH User Key Table**

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	Auto Generated	6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1
<input type="checkbox"/>	DSA	Auto Generated	24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48

Schritt 2: Klicken Sie im Feld *SSH User Authentication Method* (SSH-Benutzerauthentifizierungsmethode) auf das Optionsfeld für die gewünschte globale Authentifizierungsmethode.

### SSH User Authentication

**Global Configuration**

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

**Credentials**

✦ Username:  (0/70 characters used)

✦ Password:  Encrypted   
 Plaintext  (Default Password: anonymous)

Folgende Optionen sind verfügbar:

- By Password (Kennwort) - Mit dieser Option können Sie ein Kennwort für die Benutzerauthentifizierung konfigurieren. Geben Sie ein Kennwort ein, oder übernehmen Sie die Standardeinstellung "anonymous" (Anonym).
- Durch RSA Public Key (Öffentlicher RSA-Schlüssel): Mit dieser Option können Sie einen öffentlichen RSA-Schlüssel für die Benutzerauthentifizierung verwenden. RSA wird für Verschlüsselung und Signierung verwendet. Wenn diese Option ausgewählt ist, erstellen Sie im Block SSH-Benutzerschlüsseltabelle einen öffentlichen und privaten RSA-Schlüssel.
- By DSA Public Key (Öffentlicher DSA-Schlüssel) - Mit dieser Option können Sie einen öffentlichen DSA-Schlüssel für die Benutzerauthentifizierung verwenden. DSA wird nur für die Signierung verwendet. Wenn diese Option ausgewählt ist, erstellen Sie im Block SSH-Benutzerschlüsseltabelle einen öffentlichen/privaten DSA-Schlüssel.

Schritt 3: Suchen Sie den Bereich *Anmeldeinformationen*. Geben Sie im Feld *Benutzername* den Benutzernamen ein.

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

Schritt 4: Wenn **By Password (Kennwort)** in [Schritt 2](#) ausgewählt wurde, klicken Sie im Feld *Password (Kennwort)* auf das Optionsfeld für die gewünschte Kennwortmethode. Das Standardkennwort lautet "anonymous" (Anonym).

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

Die verfügbaren Optionen werden wie folgt beschrieben:

- Verschlüsselt - Geben Sie ein verschlüsseltes Kennwort ein.
- Klartext: Geben Sie ein Kennwort als Nur-Text ein.

Schritt 5: Klicken Sie auf **Apply**, um die Authentifizierungskonfiguration zu speichern.

**SSH User Authentication**

**Global Configuration**

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

**Credentials**

Username:  (0/70 characters used)

Password:  Encrypted   
 Plaintext  (Default Password: anonymous)

**Apply** Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Schritt 6: (Optional) Um den Standardbenutzernamen und das Standardkennwort wiederherzustellen, klicken Sie auf **Standardanmeldeinformationen wiederherstellen**. Der Standardwert ist "anonymous" (Anonym).

**SSH User Authentication**

**Global Configuration**

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

**Credentials**

Username:  (0/70 characters used)

Password:  Encrypted   
 Plaintext  (Default Password: anonymous)

**Apply** Cancel **Restore Default Credentials** Display Sensitive Data as Plaintext

Schritt 7: (Optional) Um die vertraulichen Daten als unverschlüsselt oder als verschlüsselten Text anzuzeigen, klicken Sie auf **Sensitive Daten als unverschlüsselt/verschlüsselt anzeigen**.

**SSH User Authentication**

**Global Configuration**

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

**Credentials**

Username:  (0/70 characters used)

Password:  Encrypted   
 Plaintext  (Default Password: anonymous)

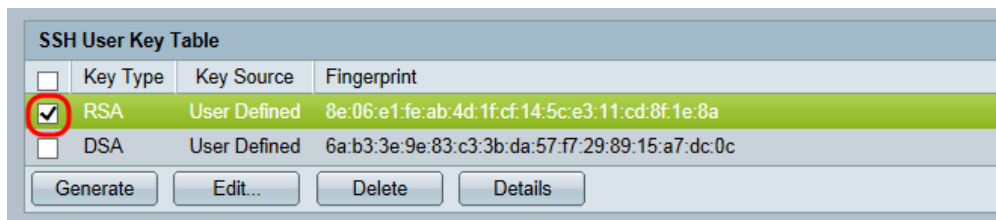
**Apply** Cancel Restore Default Credentials **Display Sensitive Data as Plaintext**

**Hinweis:** Der Name der Schaltfläche ändert sich je nach aktueller Einstellung. Über die Schaltfläche wird die Anzeige der Daten immer umgeschaltet.

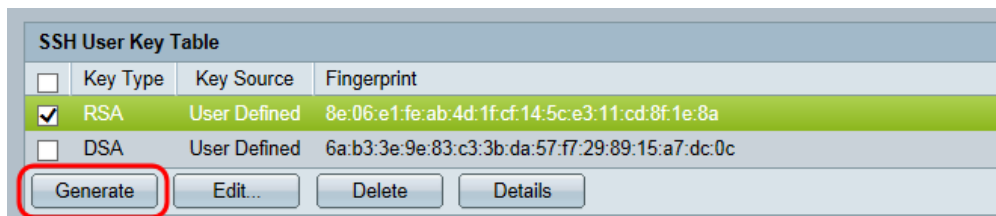
## SSH-Benutzerschlüsseltabelle

In diesem Abschnitt wird erläutert, wie die SSH-Benutzertabelle verwaltet wird.

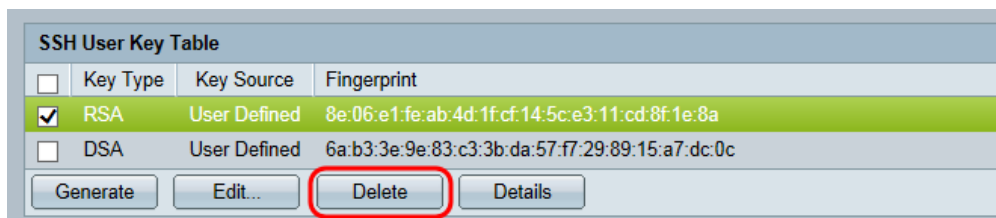
Schritt 1: Navigieren Sie zur *Tabelle mit den SSH-Benutzerschlüsseln*. Aktivieren Sie in der angezeigten Liste das bzw. die Kontrollkästchen neben dem Schlüssel, den Sie verwalten möchten.



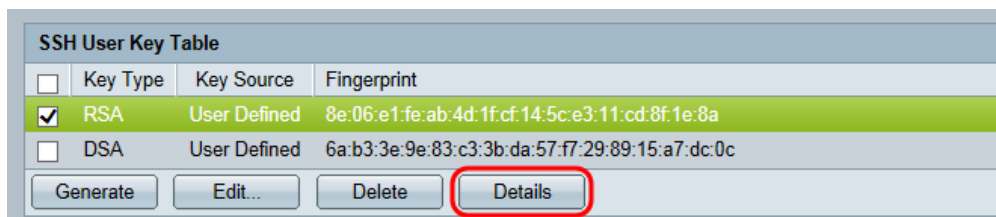
Schritt 2: (Optional) Klicken Sie auf **Generieren**, um einen neuen Schlüssel zu generieren. Der neue Schlüssel überschreibt den ausgewählten Schlüssel. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **OK**, um fortzufahren.



Schritt 3: (Optional) Klicken Sie auf **Löschen**, um den ausgewählten Schlüssel zu löschen. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **OK**, um fortzufahren.



Schritt 4: (Optional) Klicken Sie auf **Details**, um die Details des ausgewählten Schlüssels anzuzeigen.




Die Seite Details zum SSH-Benutzerschlüssel wird angezeigt. Klicken Sie auf **Zurück**, um zur Tabelle mit den SSH-Benutzerschlüsseln zurückzukehren.

### SSH User Key Details

SSH Server Key Type: RSA

Public Key: ---- BEGIN SSH2 PUBLIC KEY ----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb  
XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMikihWfRWm  
UXT6SBOK/BJk7GPXhcs0JE6II3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ==  
---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted): ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----  
Comment: RSA Private Key  
  
---- END SSH2 PRIVATE KEY ----

Back    Display Sensitive Data as Plaintext

Schritt 5: Klicken Sie auf **Bearbeiten**, um den ausgewählten Schlüssel zu bearbeiten.

### SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate    **Edit...**    Delete    Details

Das Fenster *Einstellungen für die SSH-Client-Authentifizierung bearbeiten* wird geöffnet:

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'  
---- END SSH2 PUBLIC KEY ----
```

Private Key:  Encrypted

Plaintext

Apply    Close    Display Sensitive Data as Plaintext

Schritt 6: Wählen Sie den gewünschten Schlüsseltyp aus der Dropdown-Liste *Key Type* (Typ) aus.

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
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;
---- END SSH2 PUBLIC KEY ----

```

Private Key:  Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Folgende Optionen sind verfügbar:

- RSA - RSA wird für die Verschlüsselung und Signierung verwendet.
- DSA - DSA wird nur für die Signierung verwendet.

Schritt 7: Im Feld *Öffentlicher Schlüssel* können Sie den aktuellen öffentlichen Schlüssel bearbeiten.

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
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;
---- END SSH2 PUBLIC KEY ----

```

Private Key:  Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Schritt 8: Im Feld *Privater Schlüssel* können Sie den aktuellen privaten Schlüssel bearbeiten. Klicken Sie auf

**Verschlüsselte** Optionsschaltfläche, um den aktuellen privaten Schlüssel als verschlüsselt anzuzeigen. Andernfalls klicken Sie auf das Optionsfeld **Nur Text**, um den aktuellen privaten Schlüssel als Nur-Text anzuzeigen.

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted  Plaintext

Schritt 9: Klicken Sie auf **Apply**, um die Änderungen zu speichern.

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted  Plaintext