

# Konfigurieren der RADIUS-Servereinstellungen (Remote Authentication Dial-In User Service) auf einem Switch

## Ziel

Der Remote Authentication Dial-In User Service (RADIUS) ist ein Netzwerkprotokoll, das zentralisierte AAA- (Authentication, Authorization, and Accounting)-Verwaltung für Benutzer bereitstellt, die eine Verbindung mit einem Netzwerkdienst herstellen und diesen verwenden. Ein RADIUS-Server regelt den Zugriff auf das Netzwerk, indem er die Identität der Benutzer mithilfe der eingegebenen Anmeldeinformationen überprüft. So wird beispielsweise ein öffentliches Wi-Fi-Netzwerk auf einem Universitätsgelände installiert. Nur Schüler mit Passwort können auf diese Netzwerke zugreifen. Der RADIUS-Server überprüft die von den Benutzern eingegebenen Kennwörter und gewährt bzw. verweigert den Zugriff.

Die Einrichtung eines RADIUS-Servers ist nützlich, um die Sicherheit zu erhöhen, da er sich authentifiziert, bevor ein Client oder ein Benutzer den Zugriff auf das Netzwerk erhält. Der RADIUS-Server reagiert auf Client-Probleme im Zusammenhang mit Serververfügbarkeit, Neuübertragung und Timeouts. Der RADIUS-Server verarbeitet außerdem Verbindungsanforderungen von Benutzern, authentifiziert den Benutzer und sendet die erforderlichen Konfigurationsinformationen an den Client, um dem Benutzer Dienste bereitzustellen.

Der RADIUS-Server ist ein Server, der die Steuerung eines Netzwerks zentralisiert, das aus RADIUS-fähigen Geräten besteht. RADIUS-Server basierten ihre Weiterleitungsentscheidungen auf 802.1X- oder MAC-Adressen (Media Access Control).

In diesem Artikel wird erläutert, wie Sie die RADIUS-Einstellungen für die Switches der Serien Sx350, SG350X und Sx550X konfigurieren.

## Anwendbare Geräte

- Serie Sx350
- SG350X-Serie
- Serie Sx550X

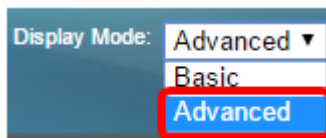
## Softwareversion

- 2,2 5,68

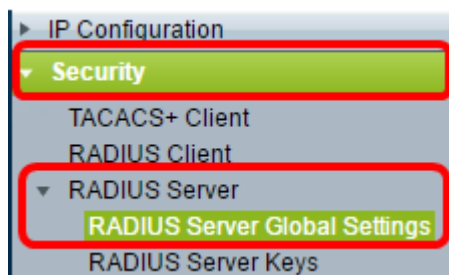
## Konfigurieren der RADIUS-Servereinstellungen

### Globale Einstellungen für den RADIUS-Server konfigurieren

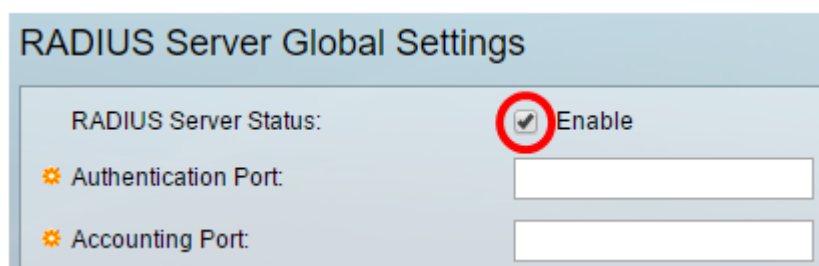
Schritt 1: Melden Sie sich beim webbasierten Switch-Dienstprogramm an, und wählen Sie in der Dropdown-Liste Anzeigemodus die Option **Erweitert** aus.



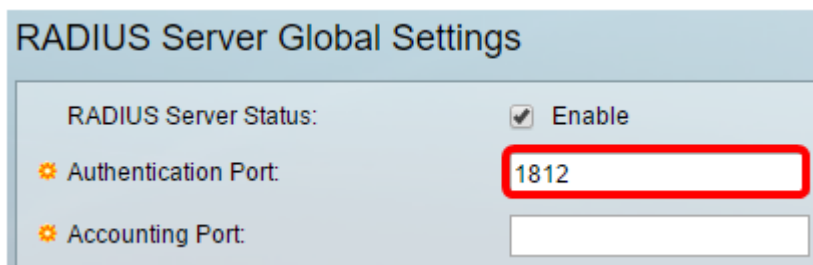
Schritt 2: Wählen Sie **Security > RADIUS Server > RADIUS Server Global Settings** aus.



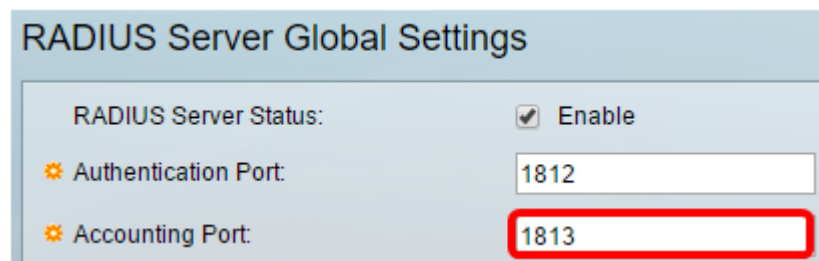
Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren** für RADIUS-Serverstatus.



Schritt 4: Geben Sie die UDP-Portnummer (User Datagram Protocol) des RADIUS-Serverports für Authentifizierungsanforderungen ein. Der Bereich liegt zwischen 1 und 65535, der Standardwert ist 1812.



Schritt 5: Geben Sie die UDP-Portnummer des RADIUS-Server-Ports für Buchhaltungsanfragen ein. Der Bereich liegt zwischen 1 und 65.535, der Standardwert ist 1813.



Schritt 6: (Optional) Um Traps für RADIUS-Accounting-Ereignisse zu generieren, aktivieren Sie das Kontrollkästchen **Aktivieren** für RADIUS Accounting Traps unter Trap Settings (Trap-Einstellungen).

**Trap Settings**

RADIUS Accounting Traps:  Enable

RADIUS Authentication Failure Traps:  Enable

RADIUS Authentication Success Traps:  Enable

Apply Cancel

Schritt 7: (Optional) Um Traps für fehlgeschlagene Anmeldungen zu generieren, aktivieren Sie das Kontrollkästchen **Aktivieren** für Traps für RADIUS Authentication Failure (RADIUS-Authentifizierungsfehler).

**Trap Settings**

RADIUS Accounting Traps:  Enable

RADIUS Authentication Failure Traps:  Enable

RADIUS Authentication Success Traps:  Enable

Apply Cancel

Schritt 8: (Optional) Um Traps für erfolgreich ausgeführte Anmeldungen zu generieren, aktivieren Sie das Kontrollkästchen **Aktivieren** für Erfolgsfallen bei der RADIUS-Authentifizierung.

**Trap Settings**



RADIUS Accounting Traps:  Enable

RADIUS Authentication Failure Traps:  Enable

RADIUS Authentication Success Traps:  Enable

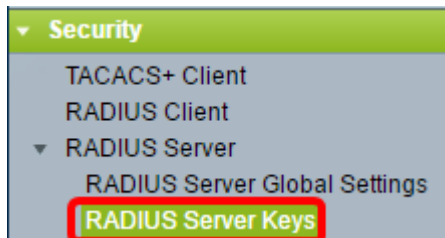
Apply Cancel

Schritt 9: Klicken Sie auf **Übernehmen**.

Schritt 10: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  Symbol am oberen Seitenrand. Andernfalls klicken Sie auf **Schließen**.

## Konfigurieren von RADIUS-Serverschlüsseln

Schritt 1: Wählen Sie **RADIUS Server Keys (RADIUS-Serverschlüssel)** unter RADIUS Server (RADIUS-Server) aus.



Schritt 2: (Optional) Geben Sie bei Bedarf den RADIUS-Standardschlüssel ein. Die im Standardschlüssel eingegebenen Werte werden auf alle Server angewendet, die (auf der Seite RADIUS-Server hinzufügen) für die Verwendung des Standardschlüssels konfiguriert wurden.



**Default Key (Standardschlüssel):** Wählen Sie die Standardschlüsselzeichenfolge aus, die zur Authentifizierung und Verschlüsselung zwischen dem Gerät und dem RADIUS-Client verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- Behalten Sie den vorhandenen Standardschlüssel bei - Bei angegebenen Servern versucht das Gerät, den RADIUS-Client mithilfe der vorhandenen Standardschlüsselzeichenfolge zu authentifizieren.
- Verschlüsselt - Um die Kommunikation mit dem MD5-Algorithmus (Message Digest 5) zu verschlüsseln, geben Sie den Schlüssel in verschlüsselter Form ein.
- Plaintext - Geben Sie die Schlüsselzeichenfolge im Klartextmodus ein.

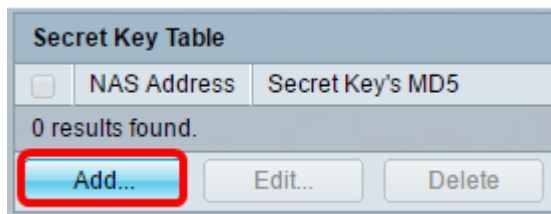
**MD5 Digest:** Zeigt den MD5-Digest des vom Benutzer eingegebenen Kennworts an.

**Hinweis:** In diesem Beispiel wird der vorhandene Standardschlüssel unter Standardschlüssel beibehalten gewählt.

Schritt 3: Klicken Sie auf **Übernehmen**.

Schritt 4: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  Symbol am oberen Seitenrand.

Schritt 5: (Optional) Klicken Sie im Bereich "Secret Key Table" (geheime Schlüsseltabelle) auf die Schaltfläche **Add** (Hinzufügen), um einen geheimen Schlüssel hinzuzufügen.



Schritt 6: Geben Sie die IP-Adresse des NAS-Geräts oder des Switches ein, der den RADIUS-Client im Feld *NAS-Adresse* enthält.

**Hinweis:** In der Abbildung unten wird 192.168.1.118 als Beispiel für die IP-Adresse verwendet.



Schritt 7: Wählen Sie Ihren bevorzugten Geheimschlüssel aus.

**Hinweis:** Im Bild unten wird als Beispiel Plaintext ausgewählt.

Folgende Optionen stehen zur Verfügung:

- Standardschlüssel verwenden: Bei angegebenen Servern versucht das Gerät, den RADIUS-Client mithilfe der vorhandenen Standardschlüsselzeichenfolge zu authentifizieren.
- Verschlüsselt - Um Kommunikation mit MD5 zu verschlüsseln, geben Sie den Schlüssel in verschlüsselter Form ein.
- Plaintext - Geben Sie die Schlüsselzeichenfolge im Klartextmodus ein. Sie können bis zu 128 Zeichen eingeben.

Schritt 8: Klicken Sie auf **Übernehmen**.

Schritt 9: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  Symbol am oberen Seitenrand. Andernfalls klicken Sie auf **Schließen**.

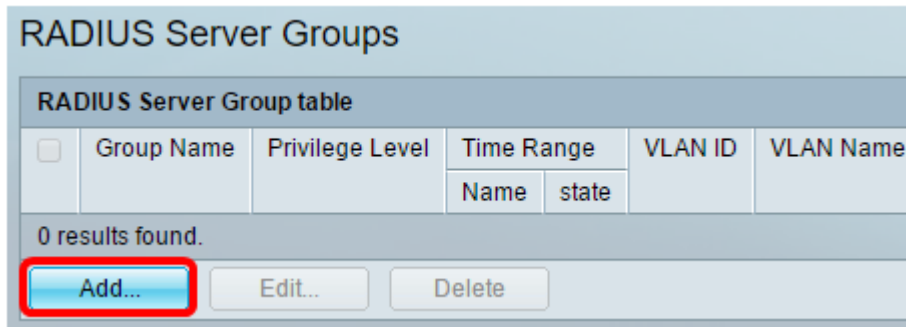
## Konfigurieren von RADIUS-Servergruppen

RADIUS-Servergruppen sind eine Benutzergruppe, die das Gerät als RADIUS-Server verwendet. Um eine Gruppe einzurichten, befolgen Sie die folgenden Anweisungen:

Schritt 1: Wählen Sie **RADIUS Server Groups** unter RADIUS Server (RADIUS-Server) aus.

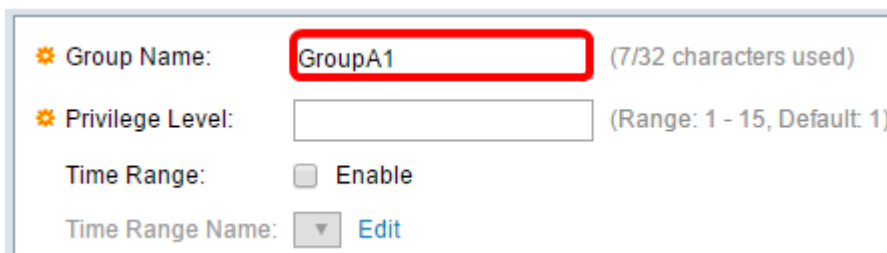


Schritt 2: Klicken Sie unter Tabelle "RADIUS Server Group" auf die Schaltfläche **Hinzufügen**.



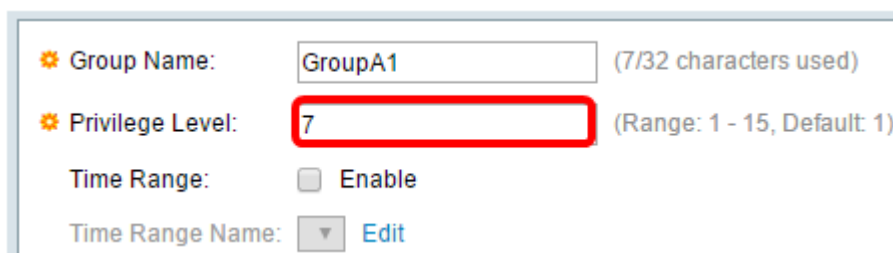
Schritt 3: Geben Sie im Popup-Fenster im Feld *Gruppenname* einen Namen für die Gruppe ein. Sie können bis zu 32 Zeichen eingeben.

**Hinweis:** In der Abbildung unten wird GroupA1 als Beispiel verwendet.



Schritt 4: Geben Sie die Berechtigungsebene ein, die Sie der Gruppe zuweisen möchten. Die Berechtigungsebene legt die Zugriffsebene fest, die Sie jeder von Ihnen erstellten Gruppe zuweisen. Sie können die Stufen zwischen 1 und 15 einstellen. Der Standardwert ist 2.

**Hinweis:** In diesem Beispiel wird 7 verwendet.



- 1 (Read-Only CLI Access) - Benutzer in der Gruppe können nicht auf die GUI zugreifen und nur auf CLI-Befehle zugreifen, die die Gerätekonfiguration nicht ändern.
- 7 (Lese-/Beschränkter Lese-/Schreibzugriff) - Benutzer in der Gruppe können nicht auf die GUI zugreifen und nur auf einige CLI-Befehle zugreifen, die die Gerätekonfiguration ändern. Weitere Informationen finden Sie im [CLI-Referenzhandbuch](#) .

- 15 (Read/Write Management Access) - Benutzer in der Gruppe können auf die GUI zugreifen und das Gerät konfigurieren.

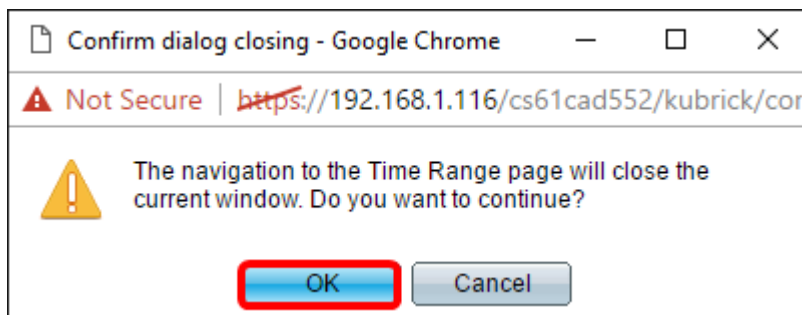
Schritt 5: (Optional) Wenn Sie einen Zeitbereich für diese Gruppe anwenden möchten, aktivieren Sie das Kontrollkästchen **Aktivieren** für den Zeitbereich. Fahren Sie andernfalls mit [Schritt 15 fort](#).

Group Name:  (7/32 characters used)  
Privilege Level:  (Range: 1 - 15, Default: 1)  
Time Range:  Enable

Schritt 6: Klicken Sie auf den Link **Bearbeiten** neben Name des Zeitbereichs, um die Zeiteinstellungen zu konfigurieren.

Group Name:  (7/32 characters used)  
Privilege Level:  (Range: 1 - 15, Default: 1)  
Time Range:  Enable  
Time Range Name:  [Edit](#)

Schritt 7: Es wird ein Popup-Fenster mit der Meldung angezeigt, dass das aktuelle Fenster geschlossen wird, damit Sie mit den Zeitbereichseinstellungen fortfahren können. Klicken Sie auf **OK**.



Sie werden dann zur Seite "Time Range" (Zeitbereich) weitergeleitet.

Schritt 8: Klicken Sie unter der Zeitbereichstabelle auf **Hinzufügen**.

Time Range  
Time Range Table  

<input type="checkbox"/>	Time Range Name	Absolute Starting Time	Absolute Ending Time
0 results found.			

  
[Add...](#) [Edit...](#) [Delete](#)

Schritt 9: Geben Sie im Feld *Zeitbereichsname* einen Namen für den Zeitbereich ein.



**Hinweis:** In der Abbildung unten wird Reconnect als Beispiel verwendet.

Schritt 10: Wählen Sie durch Klicken auf das Optionsfeld Ihre bevorzugte Absolute Start- und Endzeit aus.

- Absolute Startzeit - Sie können die Startzeit wie folgt definieren:
- Sofortige - Wählen Sie diese Option aus, wenn der Zeitraum sofort beginnen soll.
- Date, Time (Datum, Uhrzeit): Wählen Sie diese Option aus, wenn Sie das Datum und die Uhrzeit angeben möchten, zu dem der Zeitbereich beginnt.
- Absolute Endzeit - Wählen Sie zum Definieren der Startzeit eine der folgenden Optionen aus:
- Infinite (Unbegrenzt) - Wählen Sie diese Option, wenn der Zeitbereich niemals enden soll.
- Date, Time (Datum, Uhrzeit): Wählen Sie diese Option aus, wenn Sie das Datum und die Uhrzeit angeben möchten, an dem der Zeitbereich endet.

**Hinweis:** In diesem Beispiel werden Datum und Uhrzeit ausgewählt.

Schritt 11: Klicken Sie auf **Übernehmen**.

Schritt 12: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  **Save** Symbol am oberen Seitenrand. Andernfalls klicken Sie auf **Schließen**.

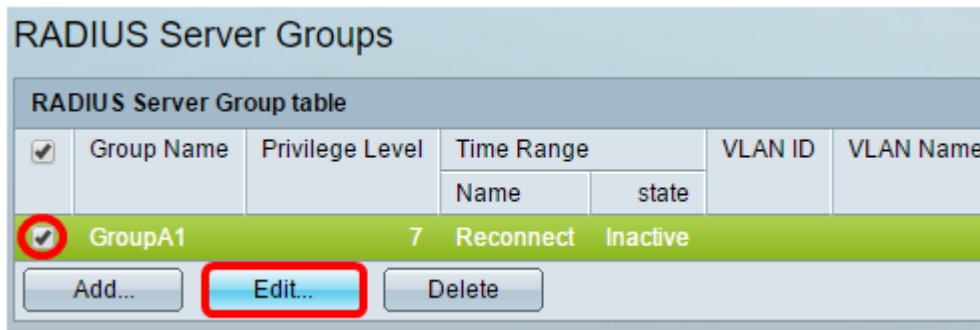
Sie werden dann zur Hauptseite weitergeleitet.

Schritt 13: Klicken Sie unter RADIUS Server erneut auf **RADIUS Server Groups**.





Schritt 14: Die neu erstellte Gruppe wird nun unter der Tabelle RADIUS Server Group (RADIUS-Servergruppe) angezeigt. Aktivieren Sie das Kontrollkästchen neben dem Namen der Gruppe, und klicken Sie dann auf **Bearbeiten**.





Schritt 15: (Optional) Wählen Sie das VLAN für die Gruppe aus. Folgende Optionen stehen zur Verfügung:

- None (Keine): Kein VLAN angegeben.
- VLAN-ID: Geben Sie eine VLAN-ID an.
- VLAN Name (VLAN-Name): Geben Sie einen VLAN-Namen an.

The screenshot shows the configuration form for a RADIUS Server Group. The fields are: Group Name (dropdown menu with 'GroupA1' selected), Privilege Level (input field with '7' and '(Range: 1 - 15, Default: 1)'), Time Range (checkbox 'Enable' checked), Time Range Name (dropdown menu with 'Reconnect' selected and an 'Edit' link), and VLAN (radio buttons for 'None', 'VLAN ID' (selected), and 'VLAN Name' (input field with '8' and '(Range: 1 - 4094)')). At the bottom are 'Apply' and 'Close' buttons.

**Hinweis:** In diesem Beispiel wird die VLAN-ID 8 verwendet.

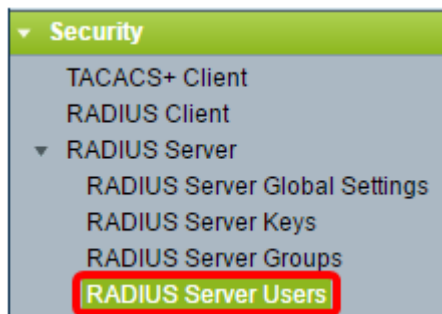
Schritt 16: Klicken Sie auf **Übernehmen**.

Schritt 17: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  Symbol am oberen Seitenrand. Andernfalls klicken Sie auf **Schließen**.

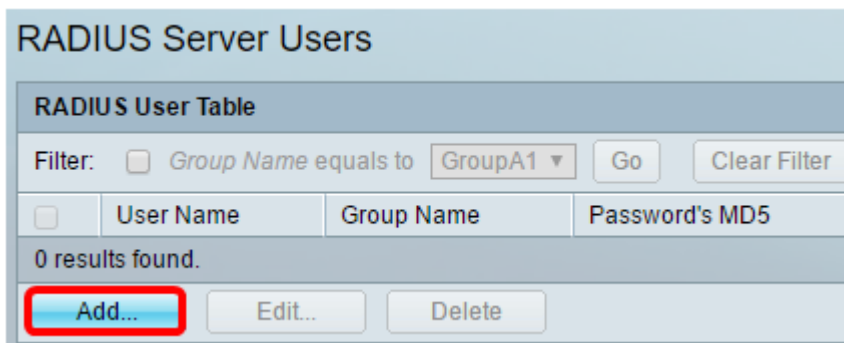
## Konfigurieren von RADIUS-Serverbenutzern

So fügen Sie Benutzer zur zuvor erstellten Gruppe hinzu:

Schritt 1: Klicken Sie unter RADIUS-Server auf **RADIUS Server Users**.

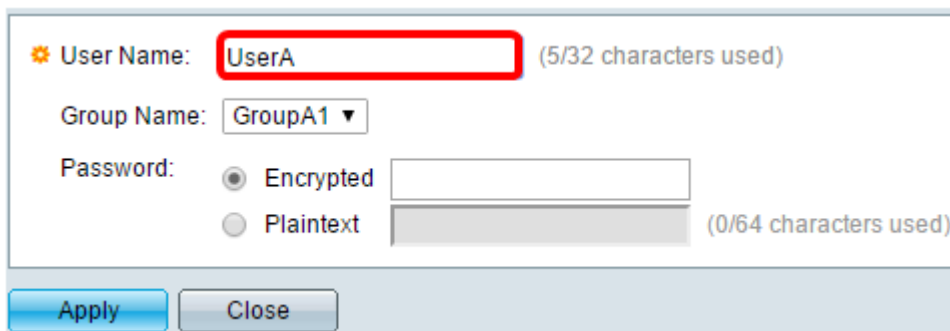


Schritt 2: Klicken Sie unter der RADIUS-Benutzertabelle auf die Schaltfläche **Hinzufügen**.

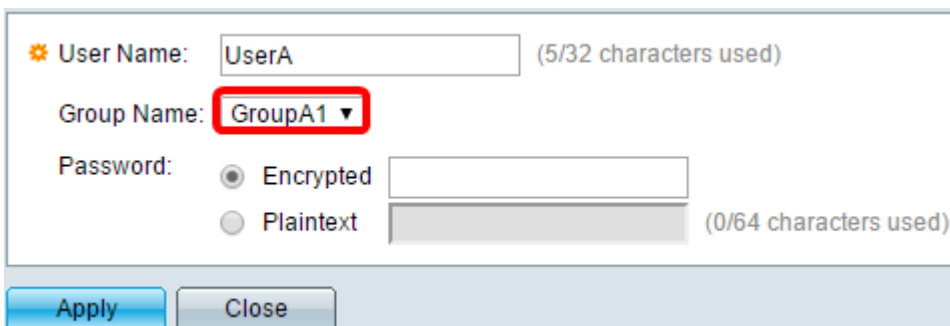


Schritt 3: Geben Sie den Namen des Benutzers in das Feld *Benutzername ein*.

**Hinweis:** In diesem Beispiel wird UserA verwendet.

A screenshot of a user creation form. The 'User Name' field contains 'UserA' and is highlighted with a red box. The 'Group Name' dropdown is set to 'GroupA1'. The 'Password' section has 'Encrypted' selected. The form includes 'Apply' and 'Close' buttons.

Schritt 4: Wählen Sie aus der Dropdown-Liste Gruppenname die Gruppe aus, der der Benutzer angehört.

A screenshot of the user creation form, identical to the previous one, but with the 'Group Name' dropdown menu open and 'GroupA1' selected. The dropdown is highlighted with a red box.

Schritt 5: Klicken Sie im Bereich Kennwort auf ein Optionsfeld.

Schritt 6: Geben Sie Ihr bevorzugtes Kennwort ein.

User Name:  (5/32 characters used)

Group Name:



Password:  Encrypted

Plaintext  (9/64 characters used)

- Verschlüsselt - Eine Schlüsselzeichenfolge wird verwendet, um Kommunikation mit MD5 zu verschlüsseln. Um die Verschlüsselung zu verwenden, geben Sie den Schlüssel in verschlüsselter Form ein.
- Plaintext: Wenn Sie keine verschlüsselte Schlüsselzeichenfolge (von einem anderen Gerät aus) haben, geben Sie die Schlüsselzeichenfolge im Klartextmodus ein. Die verschlüsselte Schlüsselzeichenfolge wird generiert und angezeigt.

**Hinweis:** In diesem Beispiel wird Plaintext gewählt.

Schritt 6: Klicken Sie auf **Übernehmen**.

Schritt 7: Ein  Symbol zeigt an, dass die Konfiguration erfolgreich gespeichert wurde. Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite Dateioperationen auf, oder klicken Sie auf das  Symbol am oberen Seitenrand. Andernfalls klicken Sie auf **Schließen**.

Sie sollten jetzt die RADIUS-Servereinstellungen auf Ihrem Switch erfolgreich konfiguriert haben.

©2016 Cisco Systems, Inc. Alle Rechte vorbehalten.