TACACS+-Serverkonfiguration für Managed Switches der Serie 300

Ziel

TACACS+ ist ein proprietäres Protokoll von Cisco, das Authentifizierung und Autorisierung über Benutzername und Kennwort ermöglicht. Um einen TACACS+-Server zu konfigurieren, muss der Benutzer über die Berechtigung 15 verfügen, die dem Benutzer Zugriff auf alle Konfigurationsfunktionen des Switches gewährt. Die Managed Switches der Serie 300 können als TACACS+-Client fungieren, bei dem alle angeschlossenen Benutzer über einen korrekt konfigurierten TACACS+-Server im Netzwerk authentifiziert und autorisiert werden können. In diesem Artikel wird die Konfiguration eines TACACS+-Servers auf den Managed Switches der Serie 300 erläutert.

Hinweis: Weitere Informationen zum Zuweisen von Zugriffsrechten 15 für Benutzer finden Sie im Artikel *Benutzerkontenkonfiguration für Managed Switches der Serie 300.*

Anwendbare Geräte

·Managed Switches der Serie SF/SG 300

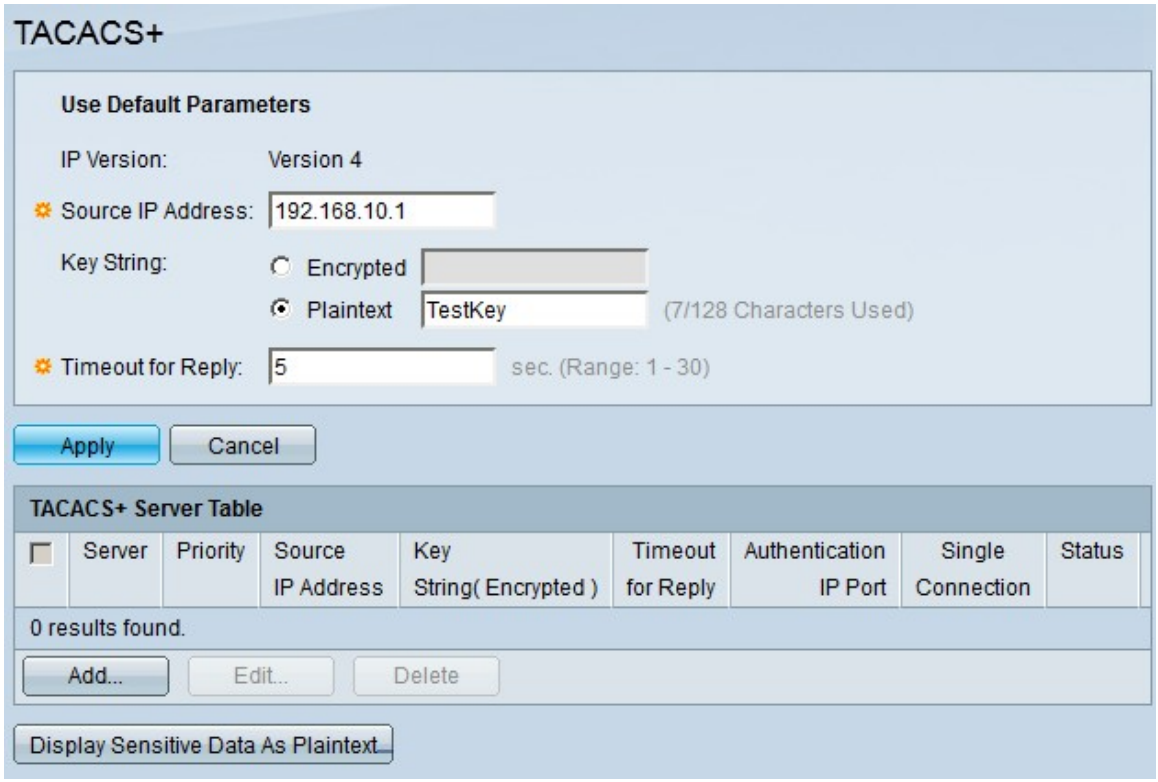
Softwareversion

·v1.2.7.76

Konfigurieren der Standardparameter eines TACACS+-Servers

In diesem Abschnitt wird erläutert, wie die Standardparameter eines TACACS+-Servers konfiguriert werden. Diese Parameter werden verwendet, wenn keine andere benutzerdefinierte Konfiguration für den Server verwendet wird.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > TACACS+** aus. Die Seite *TACACS+* wird geöffnet:



Schritt 2: Geben Sie im Feld Quell-IP-Adresse die gewünschte Standard-IP-Adresse für den TACACS+-Server ein.

Schritt 3: Wählen Sie im Feld Key String (Schlüsselzeichenfolge) aus, wie der Schlüssel eingegeben wird. Dieser Schlüssel wird zum Austausch von Nachrichten zwischen dem Switch und den TACACS+-Servern verwendet. Dies ist die verwendete Standardschlüsselzeichenfolge. Dieser Schlüssel muss der gleiche Schlüssel sein, der auf dem TACACS+-Server konfiguriert wurde. Wenn ein TACAS+-Server mit einer neuen Schlüsselzeichenfolge hinzugefügt wird, hat die neu hinzugefügte Schlüsselzeichenfolge Vorrang vor der Standardschlüsselzeichenfolge. Klicken Sie auf das Optionsfeld für eine der folgenden Optionen:

·Encrypted (Verschlüsselt): Mit dieser Option können Sie einen verschlüsselten Schlüssel eingeben.

·Nur Text: Mit dieser Option können Sie einen Schlüssel im Textformat eingeben.

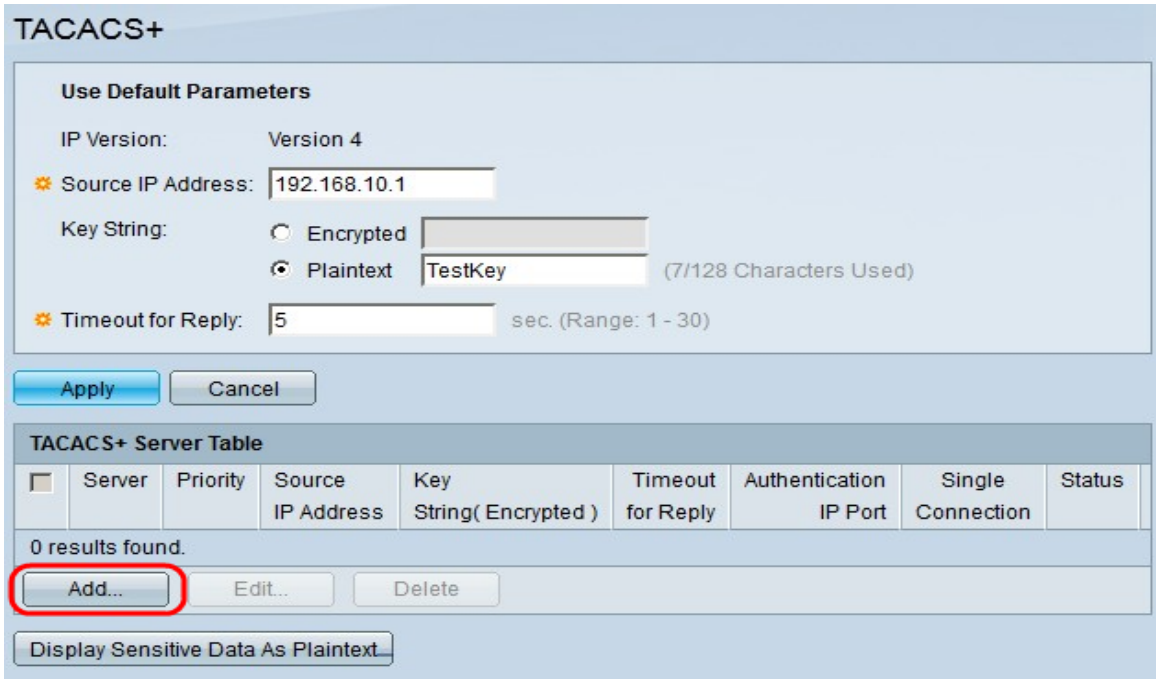
Schritt 4: Geben Sie im Feld Timeout for Reply (Zeitüberschreitung für Antwort) die Zeit in Sekunden ein, die vergehen sollte, bevor die Verbindung zwischen einem TACACS+-Server und dem Switch abläuft.

Schritt 5: Klicken Sie auf **Apply**, um die Standardparameter des TACACS+-Servers zu speichern.

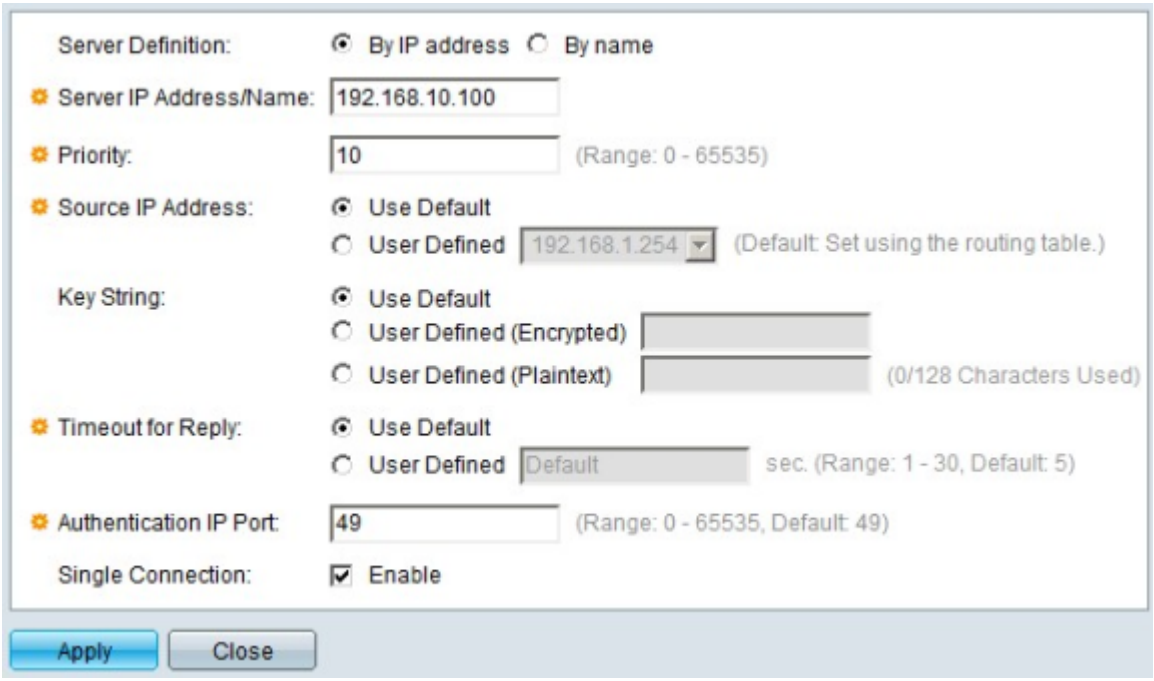
Hinzufügen eines TACACS+-Servers

In diesem Abschnitt wird erläutert, wie Sie einem Managed Switch der Serie 300 einen TACACS+-Server hinzufügen.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > TACACS+** aus. Die Seite *TACACS+* wird geöffnet:



Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *TACACS+Server hinzufügen* wird angezeigt:



Schritt 3: Wählen Sie im Feld Serverdefinition aus, wie der Server definiert ist. Klicken Sie auf das Optionsfeld für eine der folgenden Optionen:

·Nach IP-Adresse: Mit dieser Option können Sie den Server mit einer IP-Adresse definieren.

·By Name (Name): Mit dieser Option können Sie den Server mit einem vollqualifizierten Domänennamen (FQDN) definieren.

Schritt 4: Geben Sie in Schritt 3 im Feld Server IP Address/Name (IP-Adresse/Name des Servers) die IP-Adresse oder den Domänennamen des TACACS+-Servers ein.

Schritt 5: Geben Sie im Feld Priorität die gewünschte Priorität für den Server ein. Wenn der Switch keine Sitzung mit dem Server mit der höchsten Priorität herstellen kann, versucht der

Switch den Server mit der nächsthöchsten Priorität. Null gilt als höchste Priorität.

Schritt 6: Klicken Sie im Feld Quell-IP-Adresse auf eine Option, um die Quell-IP-Adresse zu definieren. Folgende Optionen stehen zur Verfügung:

·User Default (Benutzerstandard): Diese Option verwendet die im Abschnitt "Default Parameter" (Standardparameter) konfigurierte Quell-IP-Adresse.

·User Defined (Benutzerdefiniert) - Diese Option verwendet eine benutzerdefinierte Quell-IP-Adresse des Switches. Wählen Sie aus der Dropdown-Liste eine der verfügbaren benutzerdefinierten IP-Adressen aus.

Schritt 7: Geben Sie im Feld Key String (Schlüsselzeichenfolge) den Verschlüsselungsschlüssel zwischen dem TACACS+-Server und dem Switch ein. Dieser Schlüssel muss der gleiche Schlüssel sein, der auf dem TACACS+-Server konfiguriert wurde. Klicken Sie auf das Optionsfeld einer der verfügbaren Optionen, um diese Informationen einzugeben:

·Standard verwenden: Diese Option verwendet den zuvor konfigurierten Standardparameter.

·Benutzerdefiniert (verschlüsselt) - Mit dieser Option können Sie einen neuen verschlüsselten Schlüssel eingeben.

·Benutzerdefiniert (Nur-Text): Mit dieser Option können Sie einen Schlüssel in einem Textformat eingeben.

Schritt 8: Geben Sie im Feld Timeout for Reply (Zeitlimit für Antwort) die Zeit in Sekunden ein, die vergehen sollte, bevor die Verbindung zwischen Server und Switch abläuft. Klicken Sie auf das Optionsfeld für eine der folgenden Optionen:

·Standard verwenden: Diese Option verwendet den zuvor konfigurierten Standardparameter.

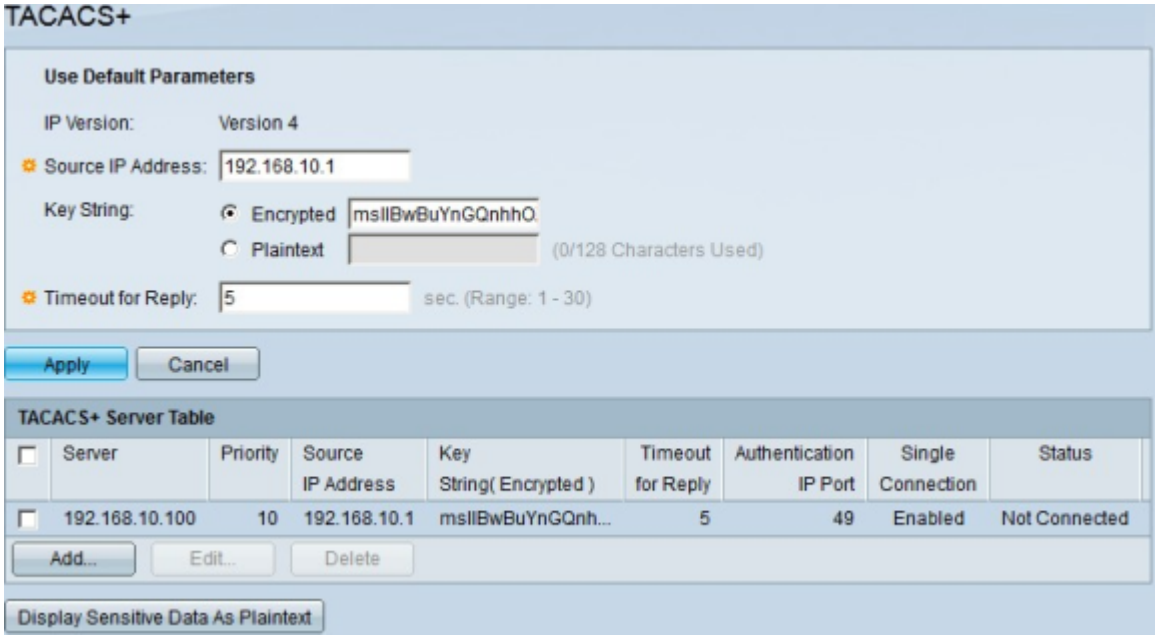
·Benutzerdefiniert - Mit dieser Option können Sie einen neuen Wert eingeben.

Schritt 9: Geben Sie im Feld Authentication Port (Authentifizierungsport) die Portnummer ein, die zum Einrichten einer TACACS+-Sitzung verwendet wird.

Schritt 10: (Optional) Aktivieren Sie im Feld Single Connection (Einzelverbindung) das Kontrollkästchen **Enable (Aktivieren)**, damit der Switch eine einzige offene Verbindung zwischen TACACS+ und dem Switch aufrechterhalten kann. Diese Option ist effizienter, da der Switch die Verbindung nicht für jeden TACACS+-Vorgang öffnet oder schließt. Stattdessen kann der Switch mit einer einzigen Verbindung mehrere TACACS+-Vorgänge verarbeiten.

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

Hinweis: Das nachfolgende Bild zeigt die Änderungen nach der Konfiguration:


TACACS+
Use Default Parameters
IP Version:
Version 4
Source IP Address:
192.168.10.1
Key String:
Encrypted
msIIBwBuYnGQnhhO
Plaintext
(0/128 Characters Used)
Timeout for Reply:
5
sec. (Range: 1 - 30)
Apply
Cancel
TACACS+ Server Table
Server
Priority
Source IP Address
Key String(Encrypted)
Timeout for Reply
Authentication IP Port
Single Connection
Status
192.168.10.100
10
192.168.10.1
msIIBwBuYnGQnh...
5
49
Enabled
Not Connected
Add...
Edit...
Delete
Display Sensitive Data As Plaintext