

RADIUS-Konfiguration der Managed Switches der Serien 200 und 300

Ziel

RADIUS (Remote Authorization Dial-In User Service) ist ein Sicherheitsdienst zur Authentifizierung von Benutzern in Netzwerken mit zentralisierter Sicherheitsarchitektur. Die Managed Switches der Serien 200 und 300 können in Ihrem Netzwerk als RADIUS-Client fungieren. In Verbindung mit einem RADIUS-Server können Sie ein zentralisiertes System zur Authentifizierung von Benutzern in Ihrem Netzwerk einrichten. In diesem Artikel wird erläutert, wie Sie einen RADIUS-Server konfigurieren und Authentifizierungsmethoden auf die Managed Switches der Serien 200 und 300 anwenden.

Unterstützte Geräte | Software-Version

- SF/SG 200-Serie - 1.2.9.x
- SF/SG-Serie 300 - 1.2.9.x

RADIUS-Standardkonfiguration

Dieser Abschnitt führt Sie durch die Standardkonfiguration eines RADIUS-Servers. Diese Standardwerte können für jeden RADIUS-Server verwendet werden, den Sie einem Switch hinzufügen möchten.

Schritt 1

Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > RADIUS aus**. Die Seite *RADIUS* wird geöffnet:

RADIUS

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based)
 Management Access
 Both Port Based Access Control and Management Access
 None

Use Default Parameters

IP Version: Version 6 Version 4

Retries: (Range: 1 - 10, Default: 3)

Timeout for Reply: sec. (Range: 1 - 30, Default: 3)

Dead Time: min. (Range: 0 - 2000, Default: 0)

Key String: Encrypted
 Plaintext (0/128 Characters Used)

RADIUS Table									
<input type="checkbox"/>	Server	Priority	Key String(Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.									
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>									

Die Bilder in diesem Artikel stammen von einem SG300-Switch.

Schritt 2

Klicken Sie im Feld "RADIUS Accounting" auf eine der folgenden Optionen:

- Port Based Access Control (802.1x, MAC-basiert) - Zur Verwendung des RADIUS-Servers für die 802.1x-Port-Accounting.
- Verwaltungszugriff - Zur Verwendung des RADIUS-Servers für die Anmeldeabrechnung.
- Port Based Access Control und Management Access: Zur Verwendung des RADIUS-Servers sowohl für die 802.1x- als auch für die Anmeldeabrechnung.
- Keine: Der RADIUS-Server wird nicht für die Kontoführung verwendet.

Radius Accounting ist auf den Switches der SG200-Serie nicht verfügbar.

Schritt 3

Geben Sie im Abschnitt Use Default Parameters (Standardparameter verwenden) im Feld Retries (Wiederholungen) die Anzahl der erneuten Versuche ein, die der Switch zur Authentifizierung des RADIUS-Servers durchgeführt hat.

Schritt 4

Geben Sie im Feld Timeout for Reply (Zeitüberschreitung für Antwort) die Zeit in Sekunden für jeden Authentifizierungsversuch beim RADIUS-Server ein.

Schritt 5

Geben Sie im Feld Dead Time (Totzeit) die Zeit in Minuten ein, bevor der Switch einen nicht reagierenden RADIUS-Server als ausgefallen deklariert und zum nächsten verfügbaren Server wechselt, um eine Verbindung herzustellen.

Schritt 6

Geben Sie im Feld Key String (Schlüsselzeichenfolge) den Schlüssel ein, der für die Authentifizierung und Verschlüsselung zwischen dem Switch und dem RADIUS-Server verwendet wird. Dieser Schlüssel muss sowohl auf dem RADIUS-Server als auch auf dem Switch übereinstimmen. Klicken Sie auf eine der folgenden Optionen:

- Verschlüsselt - Wenn Sie einen verschlüsselten Schlüssel von einem anderen Gerät haben, geben Sie den Schlüssel ein.
- Nur-Text: Wenn Sie keinen verschlüsselten Schlüssel von einem anderen Gerät haben, geben Sie den Schlüssel als Nur-Text ein.

Schritt 7

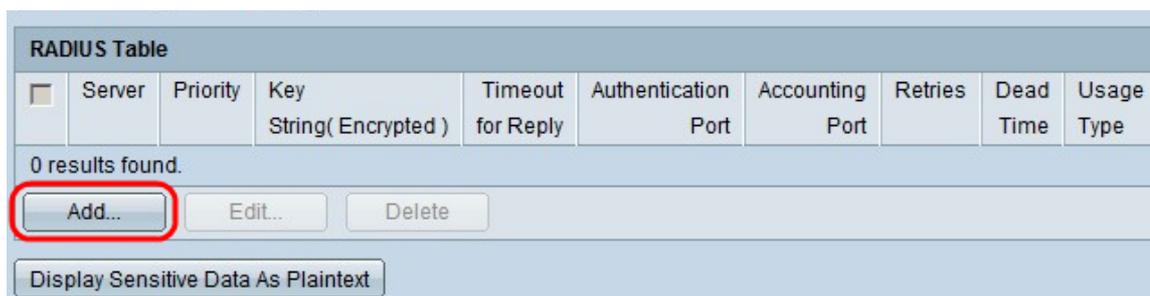
Klicken Sie auf **Apply**, um diese Standardwerte zu speichern und sie für einen RADIUS-Server verfügbar zu machen.

Hinzufügen/Bearbeiten eines RADIUS-Servers

In diesem Abschnitt wird Schritt für Schritt beschrieben, wie Sie einen RADIUS-Server zu einem Managed Switch der Serien 200/300 hinzufügen oder bearbeiten.

Schritt 1

Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > RADIUS** aus. Die Seite *RADIUS* wird geöffnet:



Schritt 2

Klicken Sie im Abschnitt "RADIUS Table" auf **Add**. Das Fenster *Radius-Server hinzufügen* wird angezeigt.

Um einen aktuellen Radius-Server zu bearbeiten, klicken Sie auf **Bearbeiten**, und bearbeiten Sie die gewünschten Eigenschaften des RADIUS-Servers.



Schritt 3

Klicken Sie im Feld "Serverdefinition" auf eine der folgenden Optionen:

- By Name (Nach Name): Wenn der RADIUS-Server mit einem Namen definiert ist.
- By IP Address (Nach IP-Adresse) - Wenn der RADIUS-Server mit einer IP-Adresse definiert ist.

Schritt 4

Klicken Sie im Feld "IP Version" auf **Version 6** oder **Version 4** als Typ der IP-Adresse des RADIUS-Servers.

Schritt 5

Wenn **Version 6** als IP-Adresse im IPv6-Adresstyp ausgewählt ist, klicken Sie auf eine der folgenden Optionen:

- Link Local (Lokal verknüpfen) - Eine IPv6-Adresse, die nur Hosts auf einer einzelnen Netzwerkverbindung identifiziert.
- Global - Eine IPv6-Adresse, die von anderen Netzwerken aus erreichbar ist.

Schritt 6

Wenn Link Local (Lokale Verbindung) als IPv6-Adresstyp ausgewählt ist, wählen Sie in der Dropdown-Liste Link Local Interface (Lokale Verbindung) die entsprechende Schnittstelle aus.

Schritt 7

Geben Sie im Feld Server IP Address/Name (IP-Adresse/Name des Servers) die IP-Adresse oder den Namen des RADIUS-Servers ein.

Schritt 8

Geben Sie im Feld Priority (Priorität) die Priorität des RADIUS-Servers ein, den der Switch verwenden soll. Der Server mit der höchsten Priorität wird zuerst im Switch abgefragt. Null (0) gibt die höchste Priorität.

Schritt 9

Klicken Sie im Feld Schlüsselzeichenfolge auf eine der folgenden Optionen:

- Use Default (Standard verwenden) - Zur Verwendung des Standardschlüssels für die Authentifizierung.
- Benutzerdefiniert (verschlüsselt) - Wenn verfügbar, geben Sie den verschlüsselten Schlüssel ein.
- Benutzerdefiniert (Klartext) - Wenn nicht verfügbar, geben Sie den Schlüssel als Klartext ein.

Schritt 10

Klicken Sie im Feld "Timeout für Antwort" auf eine der folgenden Optionen:

- Use Default (Standard verwenden) - Den Standardwert verwenden.
- Benutzerdefiniert - Geben Sie die Anzahl in Sekunden ein, die der Switch auf jeden Verbindungsversuch mit dem RADIUS-Server wartet.

Schritt 11

Geben Sie im Feld Authentication Port (Authentifizierungsport) den UDP-Port ein, den der RADIUS-Server für die Authentifizierung verwendet.

Schritt 12

Geben Sie im Feld Accounting Port (Buchungsport) den UDP-Port ein, den der RADIUS-Server für die Buchhaltung verwendet.

Schritt 13

Klicken Sie im Feld "Retries" (Wiederholungen) auf eine der folgenden Optionen:

- Use Default (Standard verwenden) - Den Standardwert verwenden.
- Benutzerdefiniert - Einen anderen Wert verwenden. Geben Sie die Anzahl der Versuche ein, die der Switch unternimmt, bevor eine Verbindung mit dem RADIUS-Server als fehlgeschlagen betrachtet wird.

Schritt 14

Klicken Sie im Feld "Dead Time" (Totzeit) auf eine der folgenden Optionen:

- Use Default (Standard verwenden) - Den Standardwert verwenden.
- Benutzerdefiniert - Einen anderen Wert verwenden. Geben Sie die Zeit in Minuten ein, bevor der Switch einen nicht reagierenden RADIUS-Server als ausgefallen deklariert und zum nächsten verfügbaren Server wechselt, um eine Verbindung herzustellen.

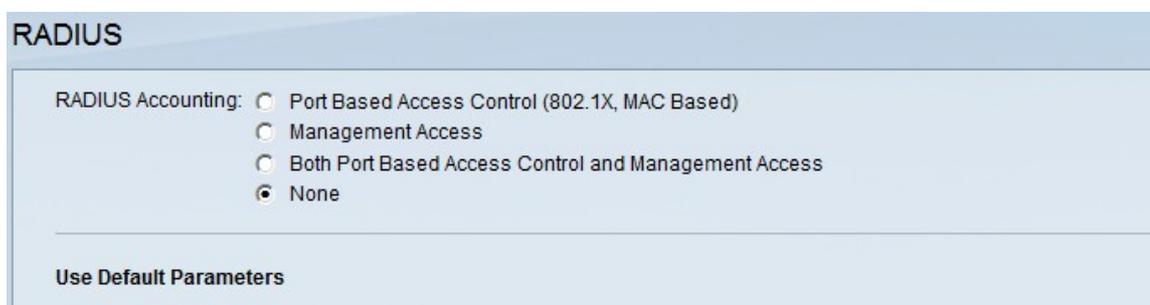
Schritt 15

Klicken Sie im Feld Verwendungstyp auf eine der folgenden Optionen:

- Anmeldung - Authentifiziert die Administratoren des Switches.
- 802.1x - Der RADIUS-Server überprüft die Sicherheitsanmeldedaten von Benutzern, die Netzwerkzugriff auf Basis des 802.1x Port-basierten Netzwerkzugriffskontrollschemas (Network Access Control, PNAC) anfordern.
- Alle - Verwendet beide Authentifizierungstypen.

Schritt 16

Klicken Sie auf **Apply** (Anwenden).



RADIUS

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based)
 Management Access
 Both Port Based Access Control and Management Access
 None

Use Default Parameters

Schritt 17

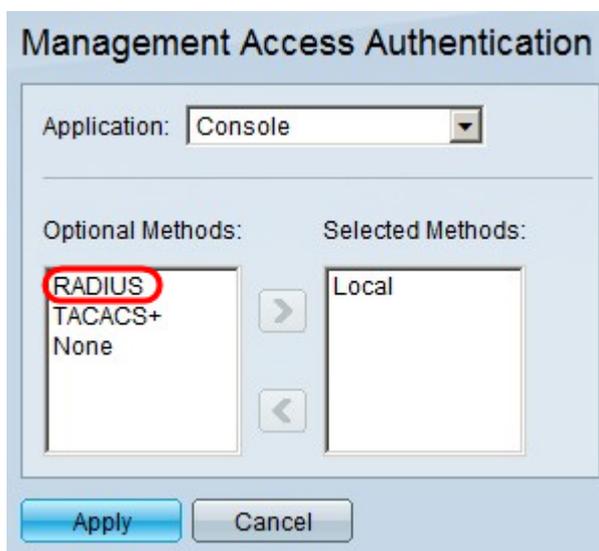
(Optional) Um einen RADIUS-Server zu löschen, aktivieren Sie im Abschnitt RADIUS-Tabelle das Kontrollkästchen des RADIUS-Servers, den Sie löschen möchten, und klicken Sie auf **Löschen**.

RADIUS-Authentifizierung

Sobald der RADIUS-Server entsprechend konfiguriert ist, müssen Sie ihn auf dem Switch authentifizieren. In diesem Abschnitt wird erläutert, wie Sie einen RADIUS-Server auf den Managed Switches der Serien 200 und 300 authentifizieren.

Schritt 1

Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Management Access Authentication** aus. Die Seite *Management Access Authentication* wird geöffnet:



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

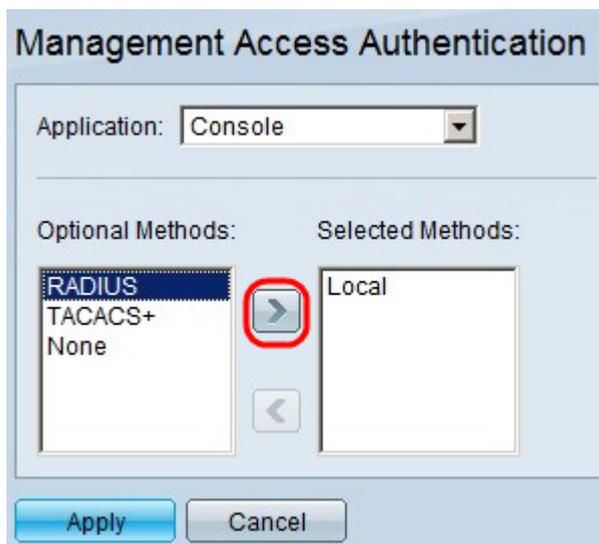
RADIUS
TACACS+
None

Local

Apply Cancel

Schritt 2

Wählen Sie in der Liste Optionale Methoden die Option RADIUS aus.



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

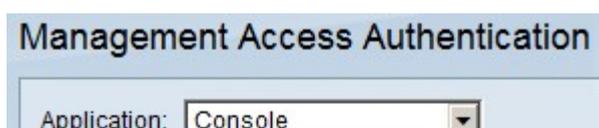
RADIUS
TACACS+
None

Local

Apply Cancel

Schritt 3

Klicken Sie auf die Schaltfläche >.



Management Access Authentication

Application: Console

Schritt 4

Klicken Sie auf **Apply** (Anwenden).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.