Konfigurieren der MAC-basierten Authentifizierung auf einem Switch

Ziel

802.1X ist ein Verwaltungstool, mit dem Sie Listengeräte zulassen können, um unautorisierten Zugriff auf Ihr Netzwerk zu verhindern. Dieses Dokument zeigt, wie Sie die MAC-basierte Authentifizierung auf einem Switch mithilfe der grafischen Benutzeroberfläche (GUI) konfigurieren. Um zu erfahren, wie Sie die MAC-basierte Authentifizierung über die Befehlszeilenschnittstelle (CLI) konfigurieren, klicken Sie hier.

Hinweis: Dieses Handbuch ist in 9 Abschnitten und 1 Abschnitt lang, um zu überprüfen, ob ein Host authentifiziert wurde. Genießen Sie Kaffee, Tee oder Wasser und stellen Sie sicher, dass Sie genügend Zeit haben, die Schritte zu überprüfen und durchzuführen.

Weitere Informationen finden Sie im Glossar.

Wie funktioniert Radius?

Die 802.1X-Authentifizierung besteht aus drei Hauptkomponenten: einer Komponente (Client), einem Authentifizierer (Netzwerkgerät wie einem Switch) und einem Authentifizierungsserver (RADIUS). Der Remote Authentication Dial-In User Service (RADIUS) ist ein Zugriffsserver, der das AAA-Protokoll (Authentication, Authorization, Accounting) verwendet, um den Netzwerkzugriff zu verwalten. RADIUS verwendet ein Client-Server-Modell, in dem sichere Authentifizierungsinformationen zwischen dem RADIUS-Server und einem oder mehreren RADIUS-Clients ausgetauscht werden. Er überprüft die Identität des Clients und benachrichtigt den Switch, ob der Client zum Zugriff auf das LAN autorisiert ist.

Ein Authentifizierer arbeitet zwischen dem Client und dem Authentifizierungsserver. Zunächst fordert sie Identitätsinformationen vom Client an. Als Reaktion darauf überprüft der Authentifizierer die Informationen mit dem Authentifizierungsserver. Schließlich wird eine Antwort an den Kunden weitergeleitet. In diesem Artikel ist der Authentifizierer ein Switch, der den RADIUS-Client enthält. Der Switch kann die EAP-Frames (Extensible Authentication Protocol) kapseln und entkapseln, um mit dem Authentifizierungsserver zu interagieren.

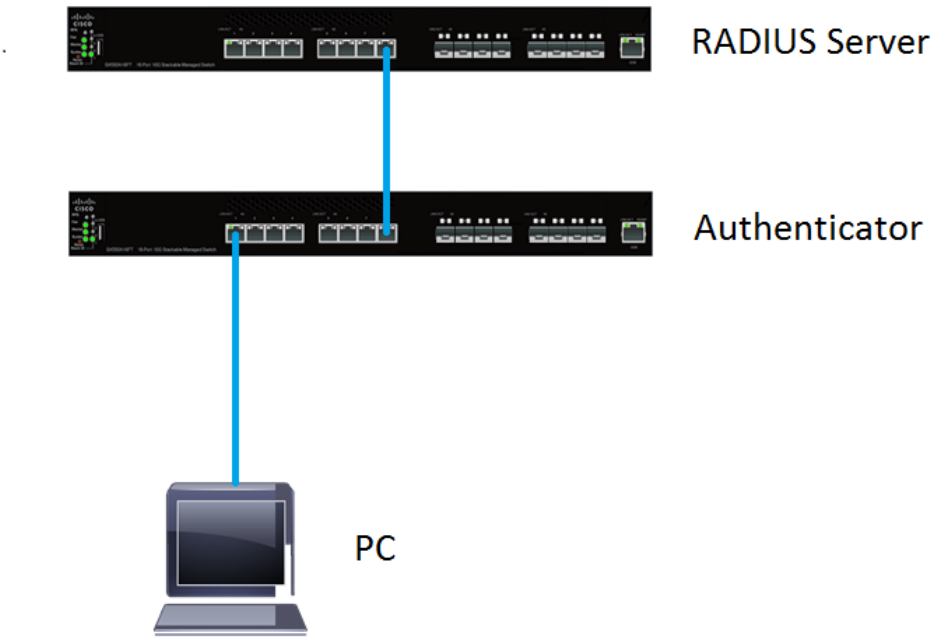
Was ist mit MAC-basierter Authentifizierung?

Bei der MAC-basierten Authentifizierung verwendet der Supplicant zur Authentifizierung die MAC-Adresse des Hosts, wenn er nicht versteht, wie er mit dem Authentifizierer kommuniziert oder nicht. MAC-basierte Supplicants werden mithilfe von reinem RADIUS (ohne EAP) authentifiziert. Der RADIUS-Server verfügt über eine dedizierte Hostdatenbank, die nur die zulässigen MAC-Adressen enthält. Anstatt die MAC-basierte Authentifizierungsanfrage als PAP-Authentifizierung (Password Authentication Protocol) zu behandeln, erkennen die Server eine solche Anforderung mit Attribute 6 [Service-Type] = 10. Sie vergleichen die MAC-Adresse im Attribut "Calling Station-Id" mit den MAC-Adressen, die in der Hostdatenbank gespeichert sind.

Version 2.4 bietet die Möglichkeit, das Format des für MAC-basierte Supplicants gesendeten Benutzernamens zu konfigurieren und entweder die EAP-Authentifizierungsmethode oder den reinen RADIUS zu definieren. In dieser Version können Sie auch das Format des Benutzernamens konfigurieren und ein spezifisches Passwort konfigurieren, das sich von dem

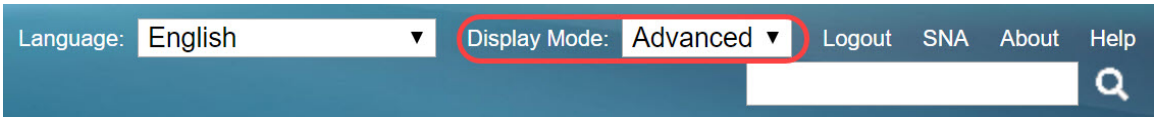
Benutzernamen unterscheidet, für MAC-basierte Supplicants.

Topologie:



Hinweis: In diesem Artikel wird der SG550X-24 sowohl für den RADIUS-Server als auch für den Authentifizierer verwendet. Der RADIUS-Server hat die statische IP-Adresse 192.168.1.100 und der Authentifizierer hat die statische IP-Adresse 192.168.1.101.

Die Schritte in diesem Dokument werden im **erweiterten** Anzeigemodus ausgeführt. Um den Modus in "Erweitert" zu ändern, gehen Sie in die obere rechte Ecke, und wählen Sie in der Dropdown-Liste *Anzeigemodus* **die Option Erweitert** aus.



Inhaltsverzeichnis

Anwendbare Geräte

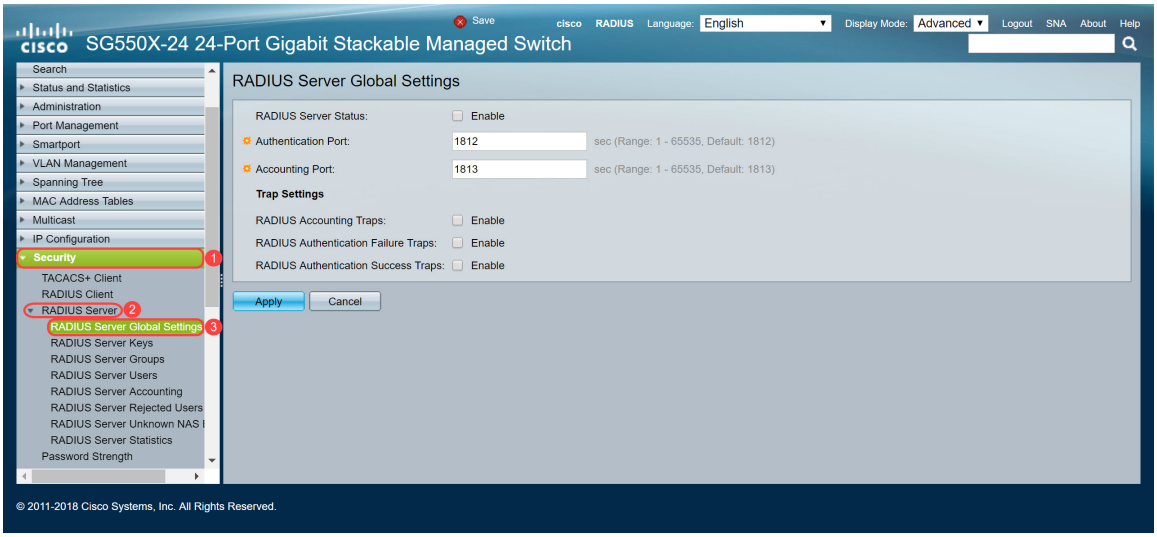
- Serie Sx350X
- SG350XG-Serie
- Serie Sx550X
- SG550XG-Serie

Softwareversion

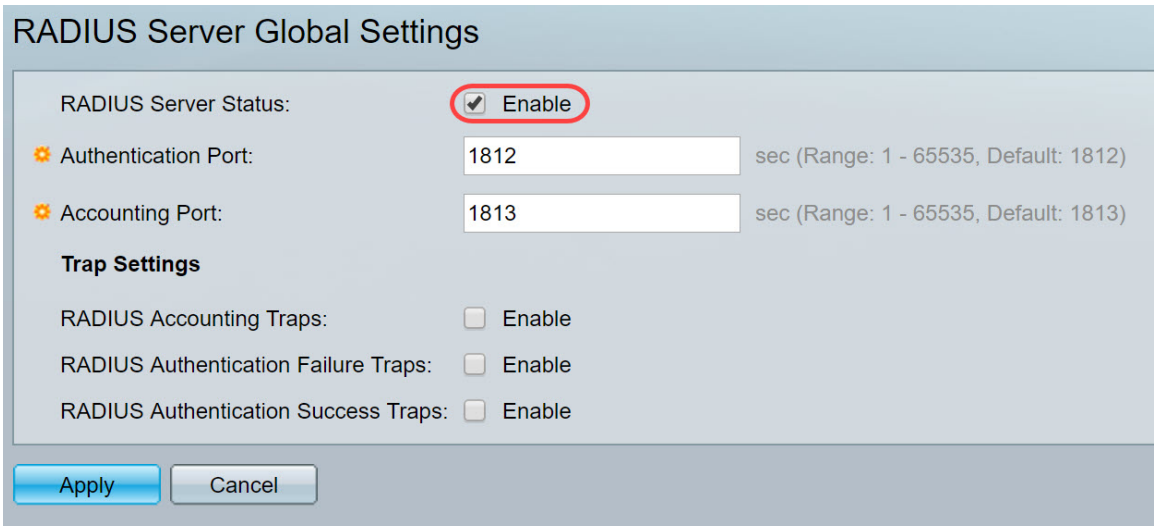
- 2,4 0,94

Globale Einstellungen für RADIUS-Server

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an, das als RADIUS-Server konfiguriert wird, und navigieren Sie zu **Security > RADIUS Server > RADIUS Server Global Settings**.



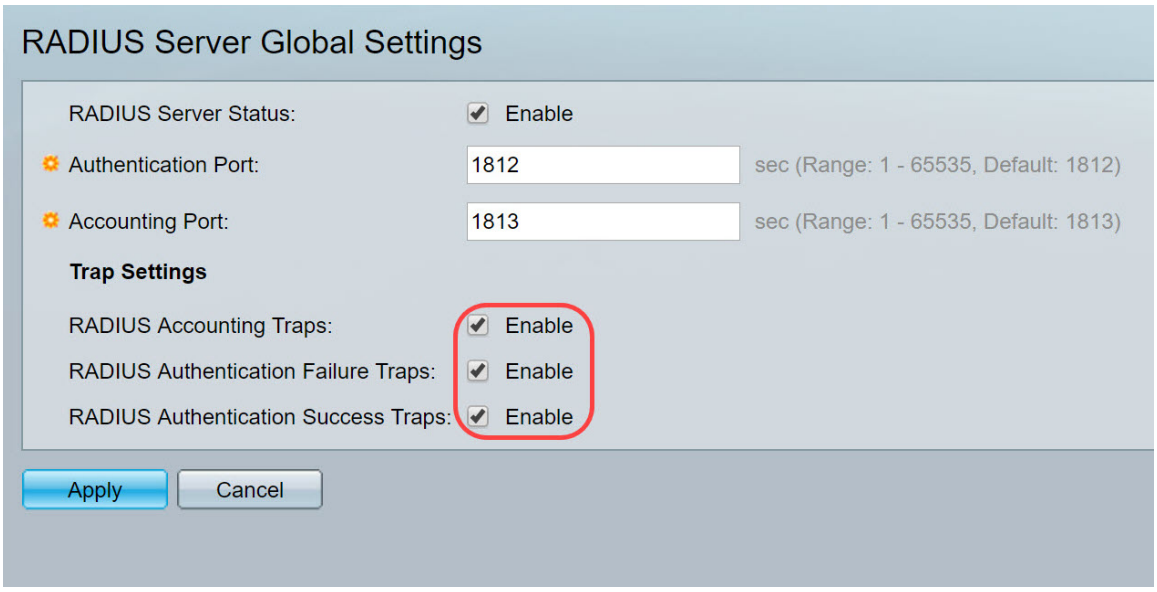
Schritt 2: Um den RADIUS-Serverfunktionsstatus zu aktivieren, aktivieren Sie im Feld *RADIUS-Serverstatus das* Kontrollkästchen **Aktivieren**.



Schritt 3: Um Traps für RADIUS-Accounting-Ereignisse, fehlgeschlagene Anmeldungen oder erfolgreiche Anmeldungen zu generieren, aktivieren Sie das gewünschte Kontrollkästchen **Aktivieren**, um Traps zu generieren. Traps sind über Simple Network Management Protocol (SNMP) generierte Systemereignismeldungen. Beim Auftreten einer Verletzung wird ein Trap an

den SNMP-Manager des Switches gesendet. Die folgenden Trap-Einstellungen sind:

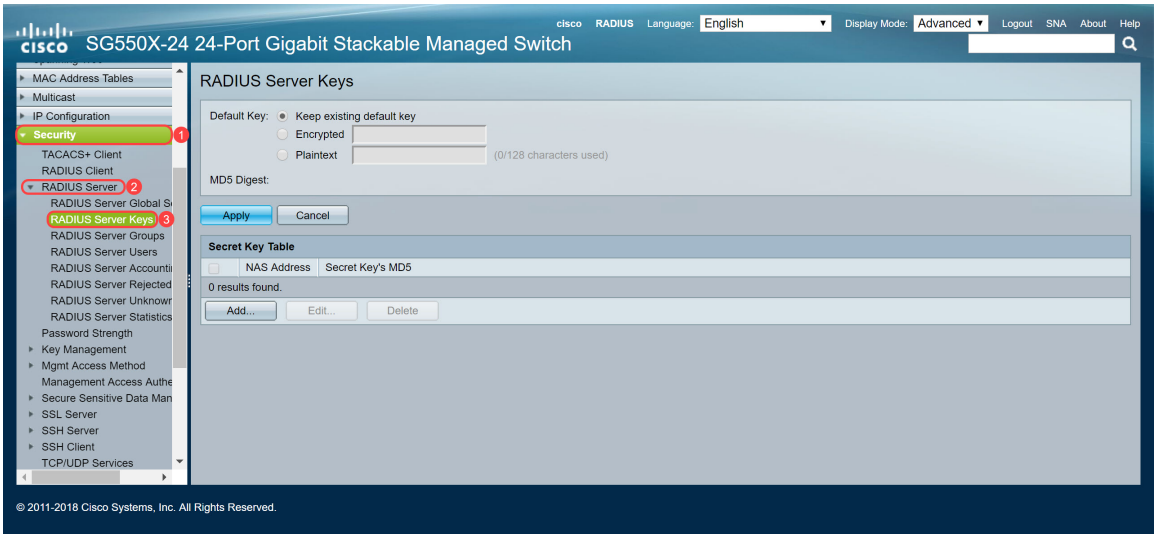
- RADIUS Accounting Traps (RADIUS-Accounting-Traps): Erstellen von Traps für RADIUS-Accounting-Ereignisse.
- RADIUS Authentication Failure Traps (Fehlerhafte RADIUS-Authentifizierung): Überprüfen Sie, ob Traps für fehlgeschlagene Anmeldungen generiert werden.
- RADIUS Authentication Success Traps (Erfolgsfallen für RADIUS-Authentifizierung): Überprüfen Sie, ob Traps für erfolgreich ausgeführte Anmeldungen generiert werden.



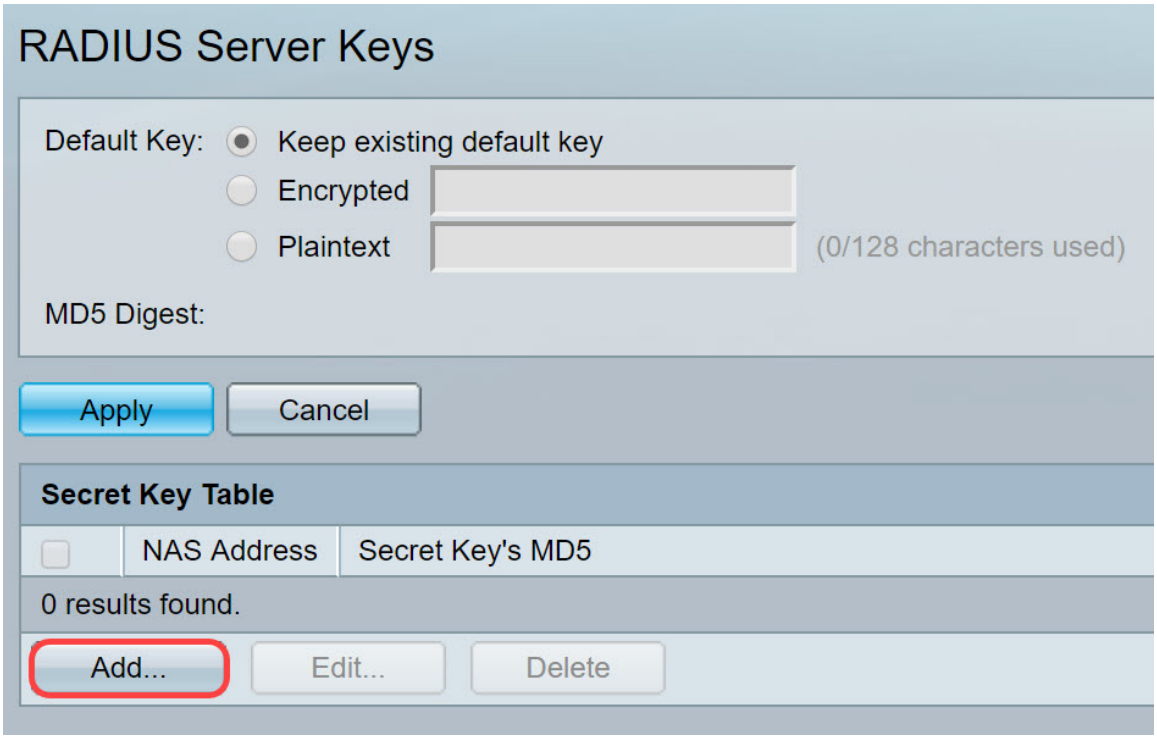
Schritt 4: Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

RADIUS-Serverschlüssel

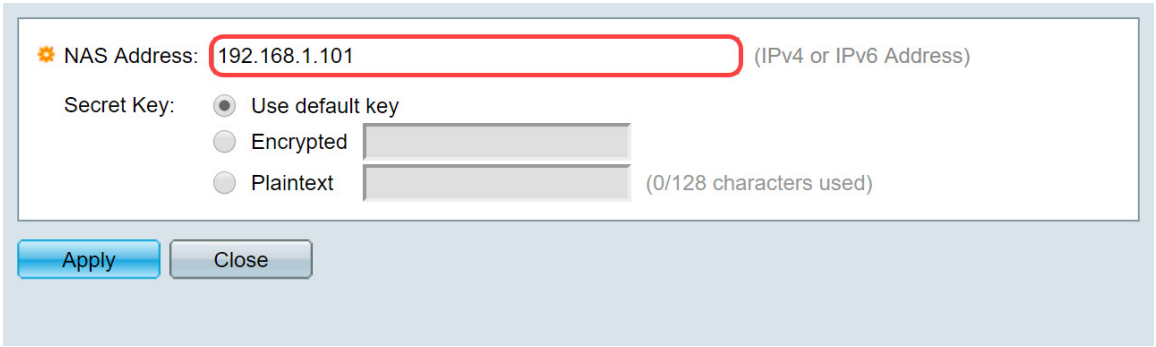
Schritt 1: Navigieren Sie zu **Security > RADIUS Server > RADIUS Server Keys (Sicherheit > RADIUS-Server-Schlüssel)**. Die Seite *RADIUS-Serverschlüssel* wird geöffnet.



Schritt 2: Klicken Sie im Abschnitt *Geheimschlüsseltabelle* auf **Hinzufügen...** um einen geheimen Schlüssel hinzuzufügen.



Schritt 3: Die Seite *Geheimschlüssel hinzufügen* wird geöffnet. Geben Sie im Feld *NAS-Adresse* die Adresse des Switches ein, der den RADIUS-Client enthält. In diesem Beispiel wird die IP-Adresse 192.168.1.101 als RADIUS-Client verwendet.

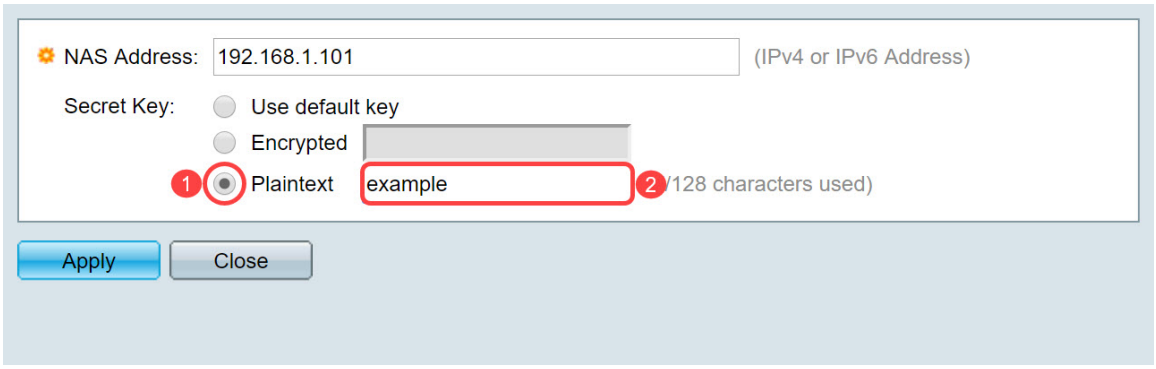


Schritt 4: Wählen Sie eine der Optionsschaltflächen aus, die als *Geheimschlüssel* verwendet wird. Folgende Optionen sind verfügbar:

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

In diesem Beispiel wählen wir *Nur-Text* und verwenden das Wort **Beispiel** als unseren *Geheimschlüssel*. Nach dem Drücken auf Apply wird der Schlüssel verschlüsselt.

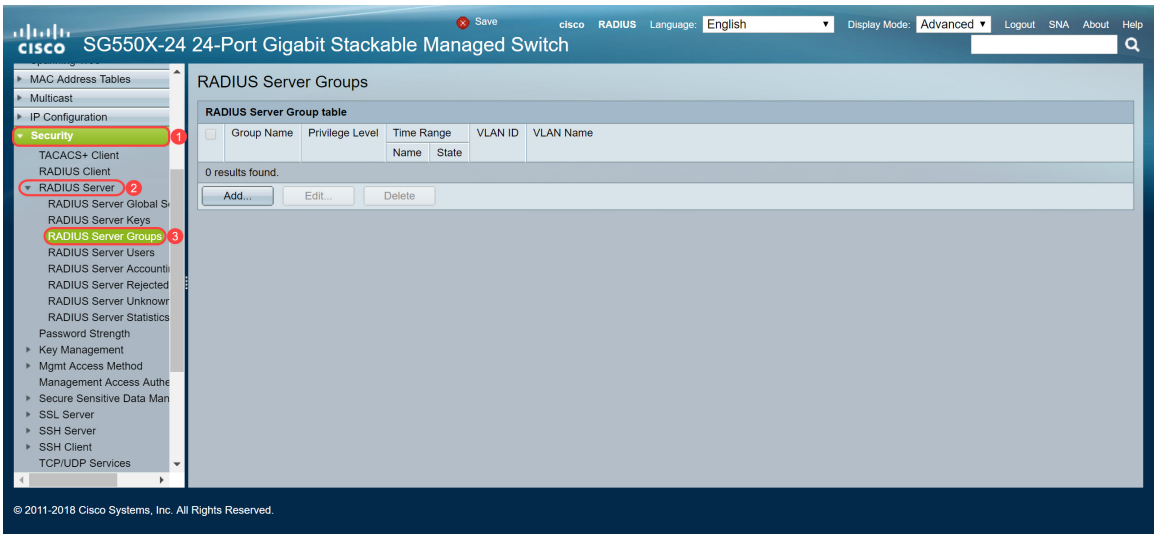
Hinweis: Es wird nicht empfohlen, das Wort **example** als geheimen Schlüssel zu verwenden. Verwenden Sie einen stärkeren Schlüssel. Es können bis zu 128 Zeichen verwendet werden. Wenn Ihr Kennwort zu komplex ist, um sich daran zu erinnern, dann ist es ein gutes Passwort, aber noch besser, wenn Sie das Passwort in eine unvergessliche Passphrase verwandeln können, die durch Sonderzeichen und Zahlen ersetzt wird, die Vokale ersetzen: "P@55w0rds@reH@rdT0Remember". Es ist am besten, kein Wort zu verwenden, das in einem Wörterbuch zu finden ist. Wählen Sie am besten einen Satz aus, und tauschen Sie einige Buchstaben gegen Sonderzeichen und Zahlen aus. Weitere Einzelheiten finden Sie in diesem Cisco Blog-Beitrag.



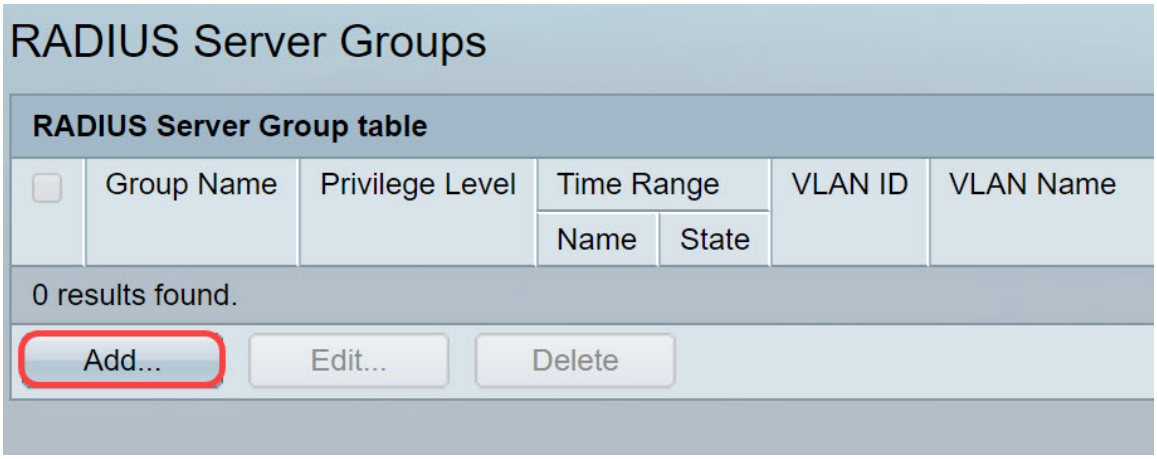
Schritt 5: Klicken Sie auf **Apply**, um die Konfiguration zu speichern. Der geheime Schlüssel wird jetzt mit MD5 verschlüsselt. MD5 ist eine kryptografische Hash-Funktion, die ein Datenstück annimmt und eine eindeutige Hexadezimalausgabe erstellt, die normalerweise nicht reproduzierbar ist. MD5 verwendet einen 128-Bit-Hashwert.

RADIUS-Servergruppen

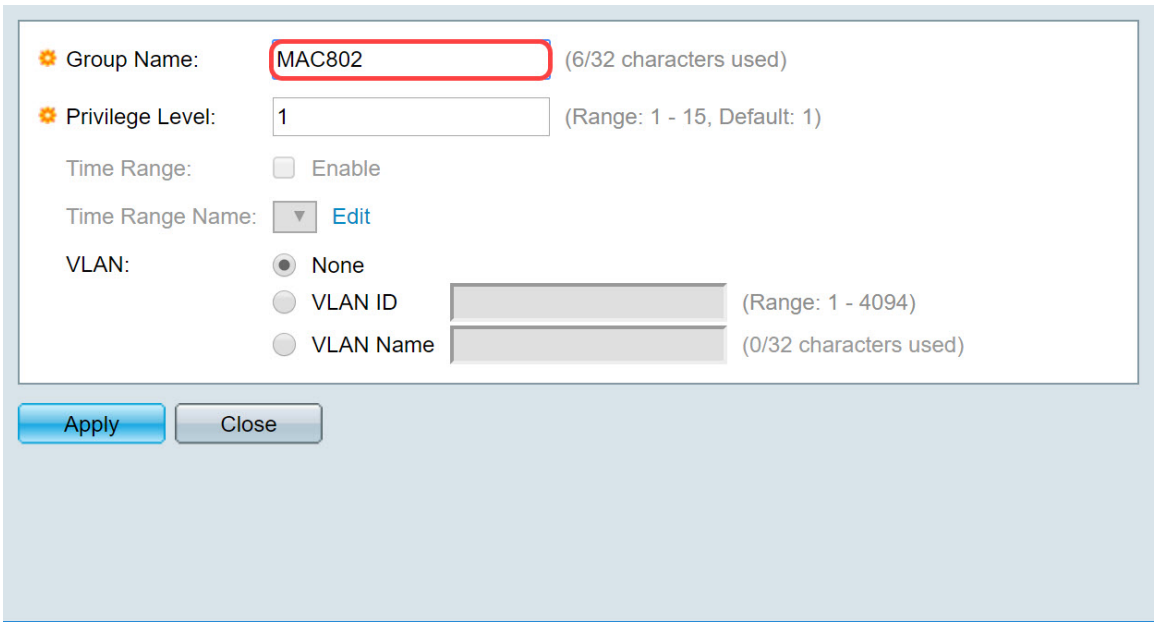
Schritt 1: Navigieren Sie zu **Security > RADIUS Server > RADIUS Server Groups**.



Schritt 2: Klicken Sie auf **Hinzufügen...** um eine neue RADIUS-Servergruppe hinzuzufügen.

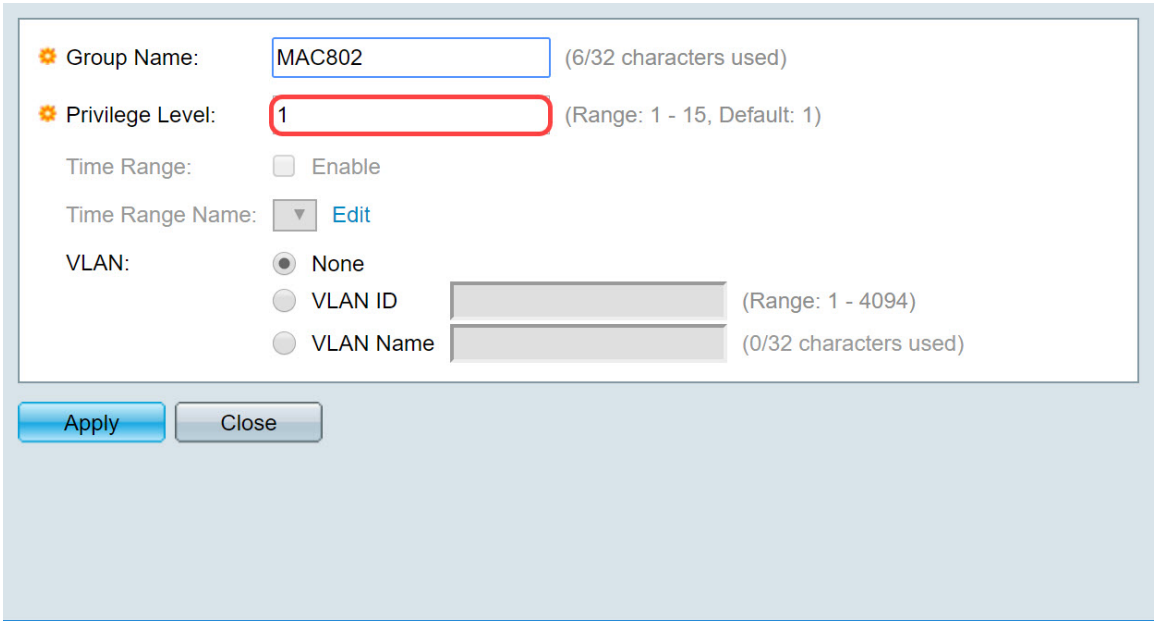


Schritt 3: Die Seite *RADIUS-Servergruppe hinzufügen* wird geöffnet. Geben Sie einen Namen für die Gruppe ein. In diesem Beispiel wird **MAC802** als unser Gruppenname verwendet.



Schritt 4: Geben Sie im Feld *Berechtigungsstufe* die Berechtigungsstufe für die Verwaltung der Gruppe ein. Der Bereich liegt zwischen 1 und 15, 15 ist der privilegierteste und der Standardwert ist 1. In diesem Beispiel belassen wir die Privilegienebene mit 1.

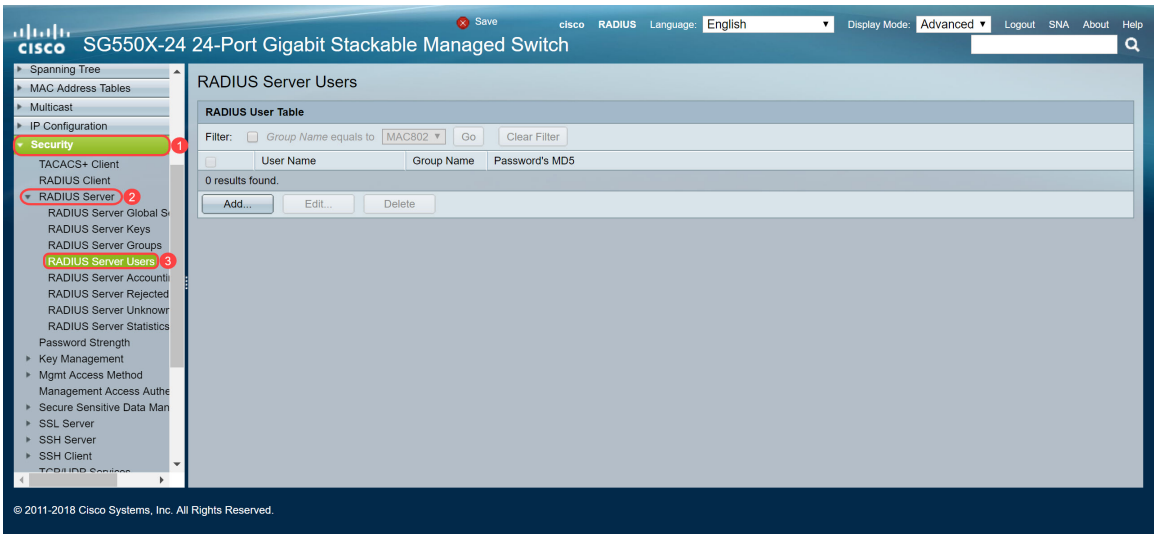
Hinweis: In diesem Artikel werden keine *Zeitbereiche* oder *VLANs* konfiguriert.



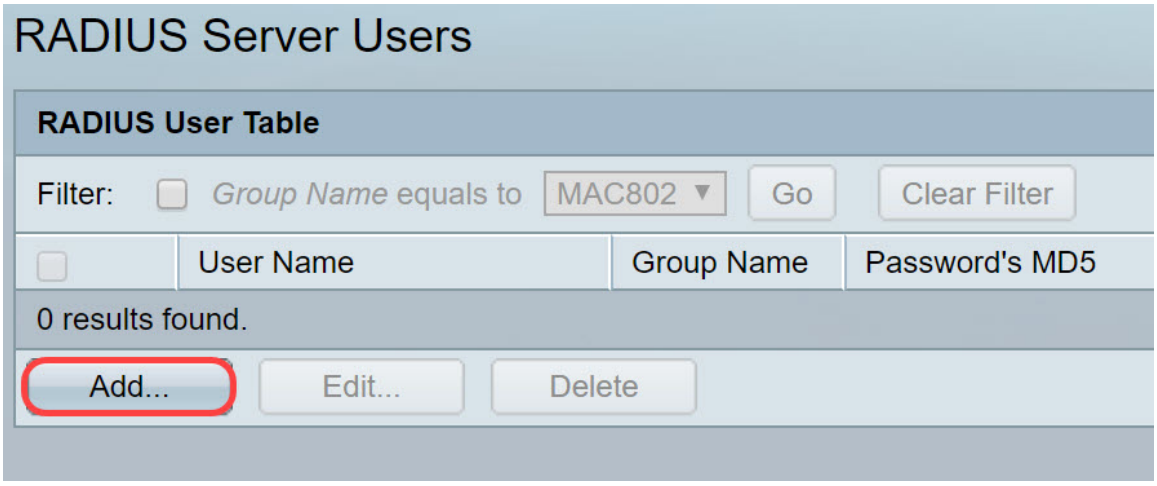
Schritt 5: Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

RADIUS-Serverbenutzer

Schritt 1: Navigieren Sie zu **Security > RADIUS Server > RADIUS Server Users**, um die Benutzer für RADIUS zu konfigurieren.

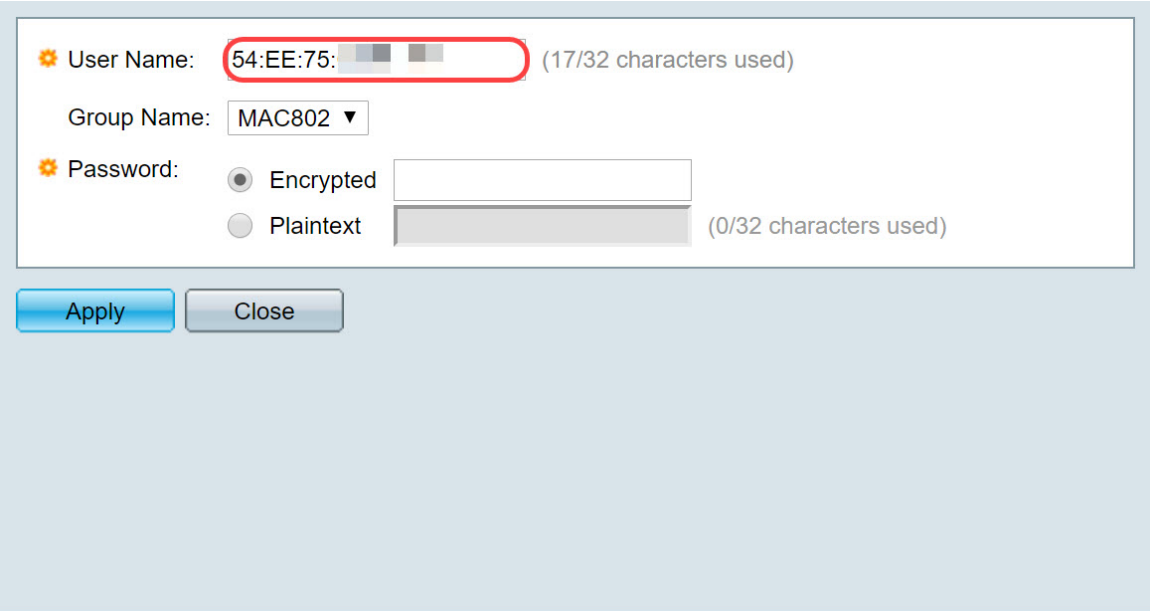


Schritt 2: Klicken Sie auf **Hinzufügen...** um einen neuen Benutzer hinzuzufügen.

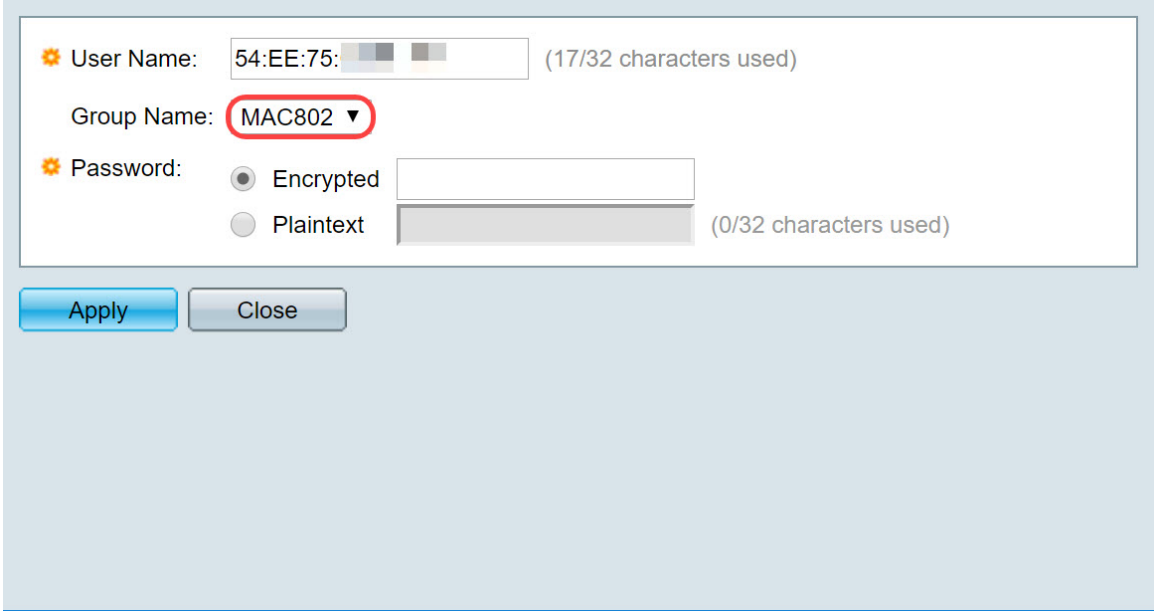


Schritt 3: Die Seite *RADIUS-Server-Benutzer hinzufügen* wird geöffnet. Geben Sie im Feld *Benutzername* die MAC-Adresse eines Benutzers ein. In diesem Beispiel verwenden wir unsere Ethernet-MAC-Adresse auf unserem Computer.

Hinweis: Ein Teil der MAC-Adresse ist verschwommen.



Schritt 4: Wählen Sie in der Dropdown-Liste *Gruppenname* eine Gruppe aus. Wie in Schritt 3 des Abschnitts "RADIUS Server Group" hervorgehoben, wird **MAC802** als unser Gruppenname für diesen Benutzer ausgewählt.

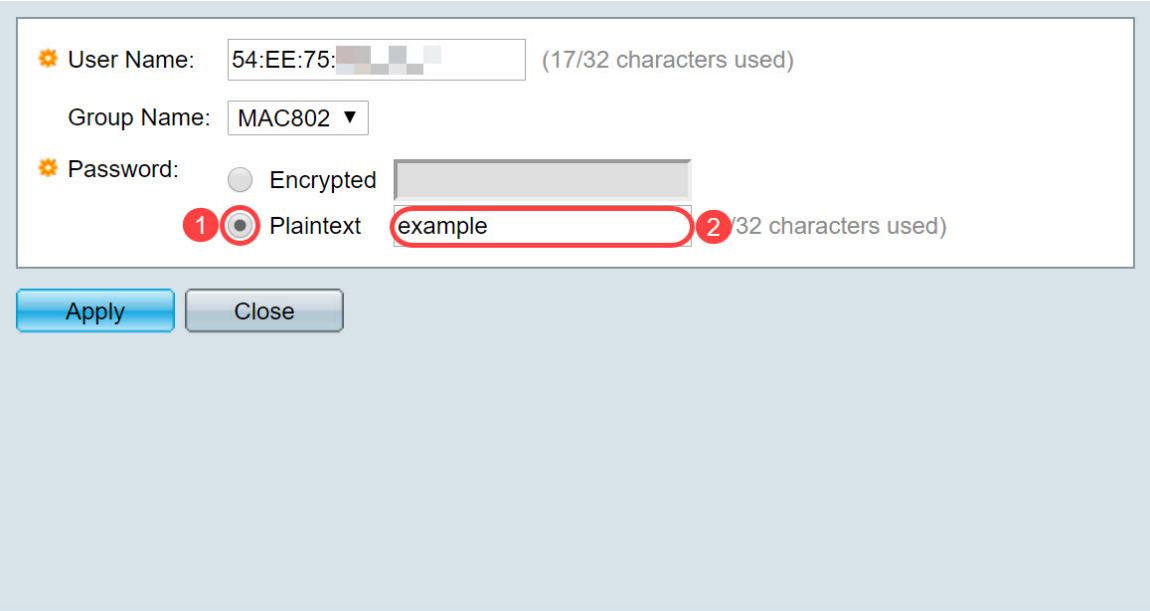


Schritt 5: Wählen Sie eine der folgenden Optionsschaltflächen aus:

- Encrypted (Verschlüsselt) - Ein Schlüssel 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.

Wir werden *Plaintext* als Kennwort für diesen Benutzer auswählen und **z.B.** als Klartext-Passwort eingeben.

Hinweis: Es wird nicht empfohlen, ein **Beispiel** als Klartext-Kennwort zu verwenden. Wir empfehlen die Verwendung eines sicheren Kennworts.

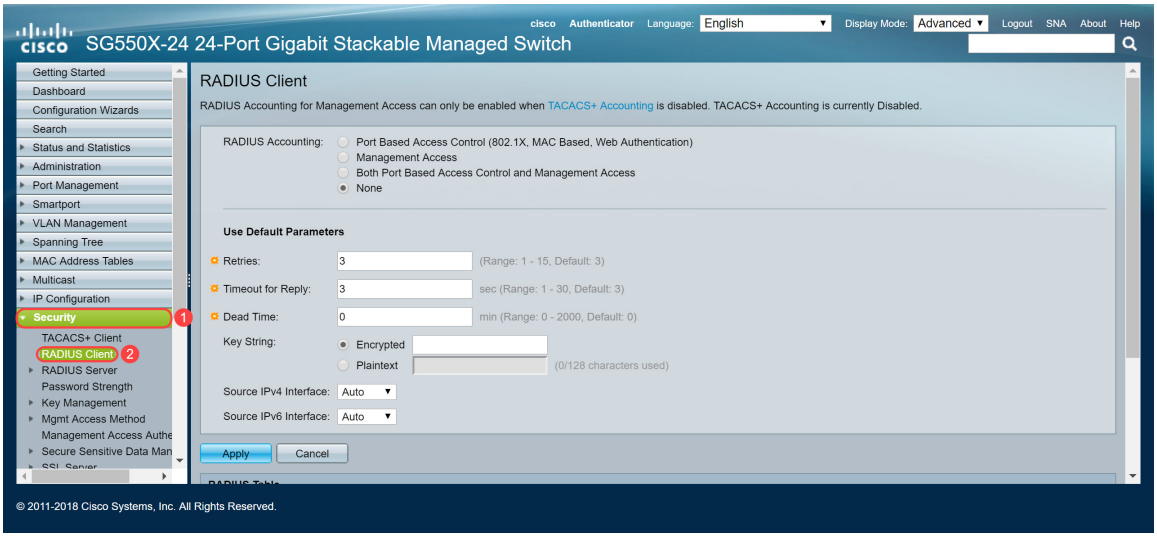


Schritt 6: Klicken Sie nach Abschluss der Konfiguration auf **Apply**.

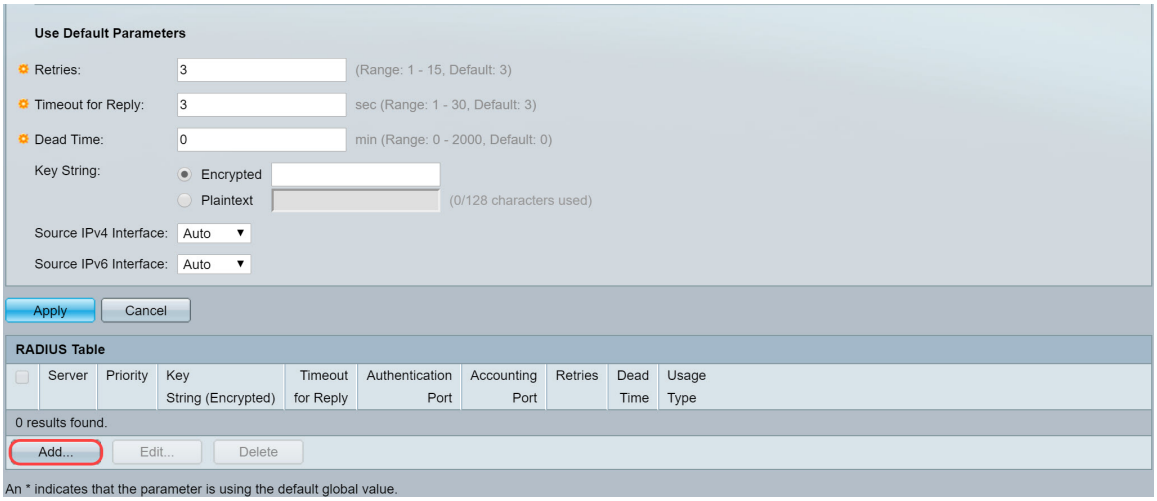
Jetzt haben Sie die Konfiguration des RADIUS-Servers abgeschlossen. Im nächsten Abschnitt wird der zweite Switch als Authentifizierer konfiguriert.

RADIUS-Client

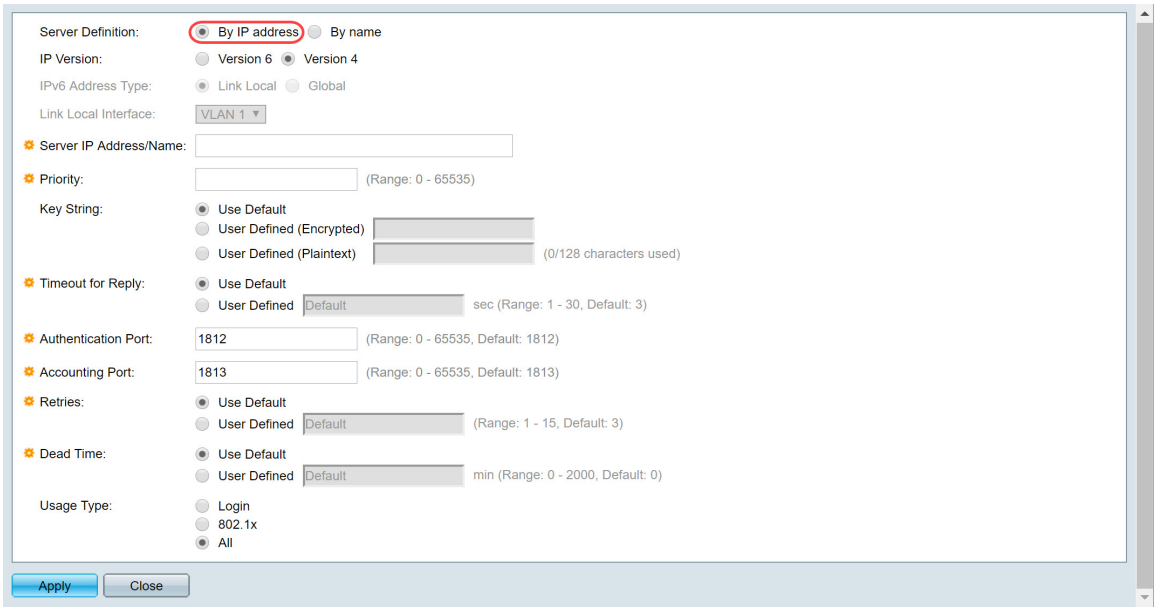
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an, das als Authentifizierer konfiguriert wird, und navigieren Sie zu **Security > RADIUS Client**.



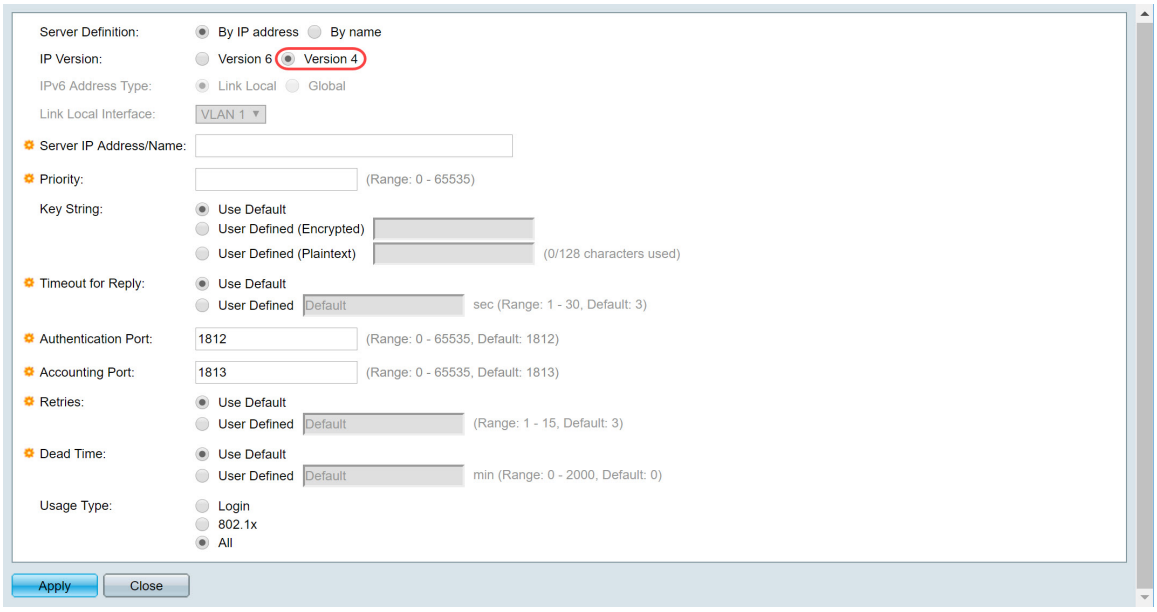
Schritt 2: Blättern Sie nach unten zum Abschnitt *RADIUS Table* (RADIUS-Tabelle), und klicken Sie dann auf **Add.. (Hinzufügen).** um einen RADIUS-Server hinzuzufügen.



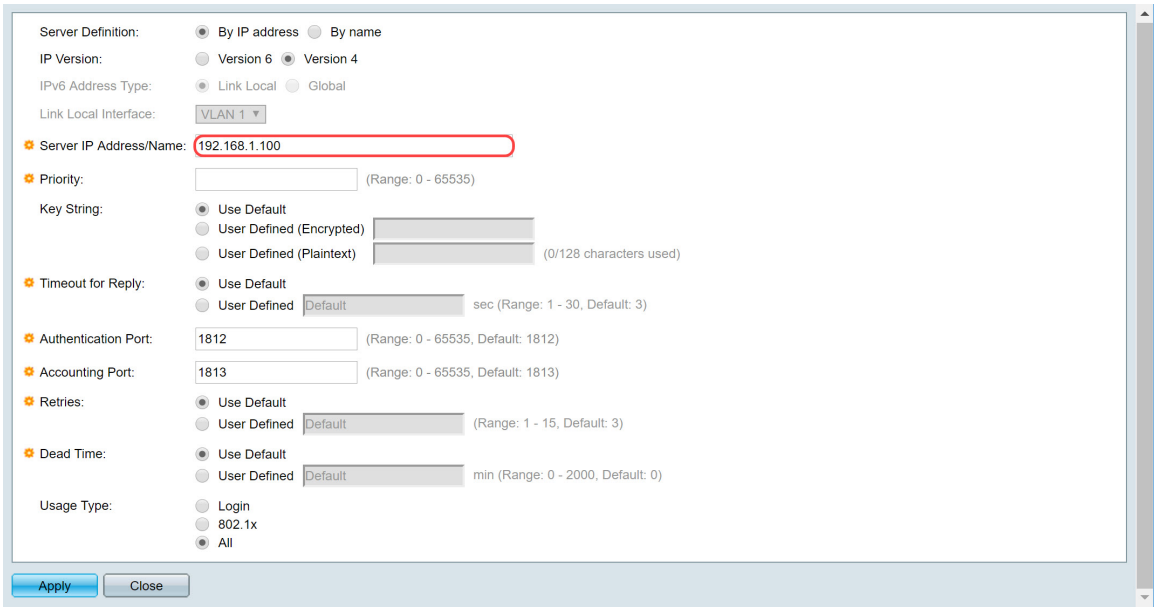
Schritt 3: (Optional) Wählen Sie im Feld *Serverdefinition* aus, ob der RADIUS-Server nach IP-Adresse oder Name angegeben werden soll. In diesem Beispiel behalten wir die Standardauswahl von **By IP address bei**.



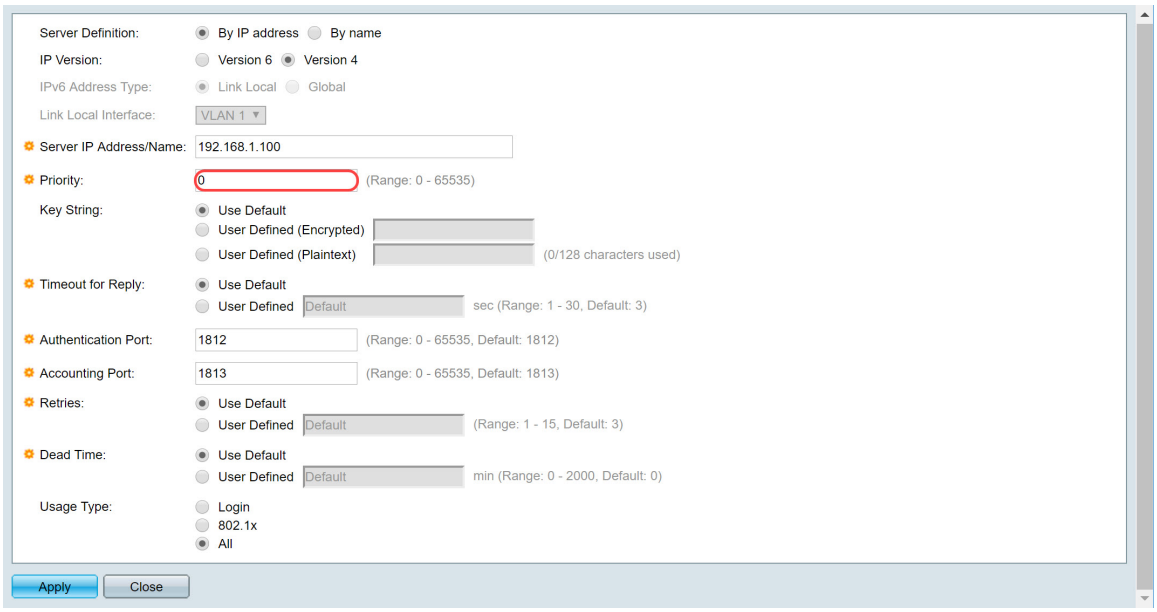
Schritt 4: (Optional) Wählen Sie im Feld *IP-Version* die Version der IP-Adresse des RADIUS-Servers aus. Wir behalten die Standardauswahl von **Version 4** für dieses Beispiel bei.



Schritt 5: Geben Sie im RADIUS-Server die IP-Adresse oder den Namen ein. Wir geben die IP-Adresse **192.168.1.100** in das Feld *IP-Adresse/Name* des *Servers ein*.

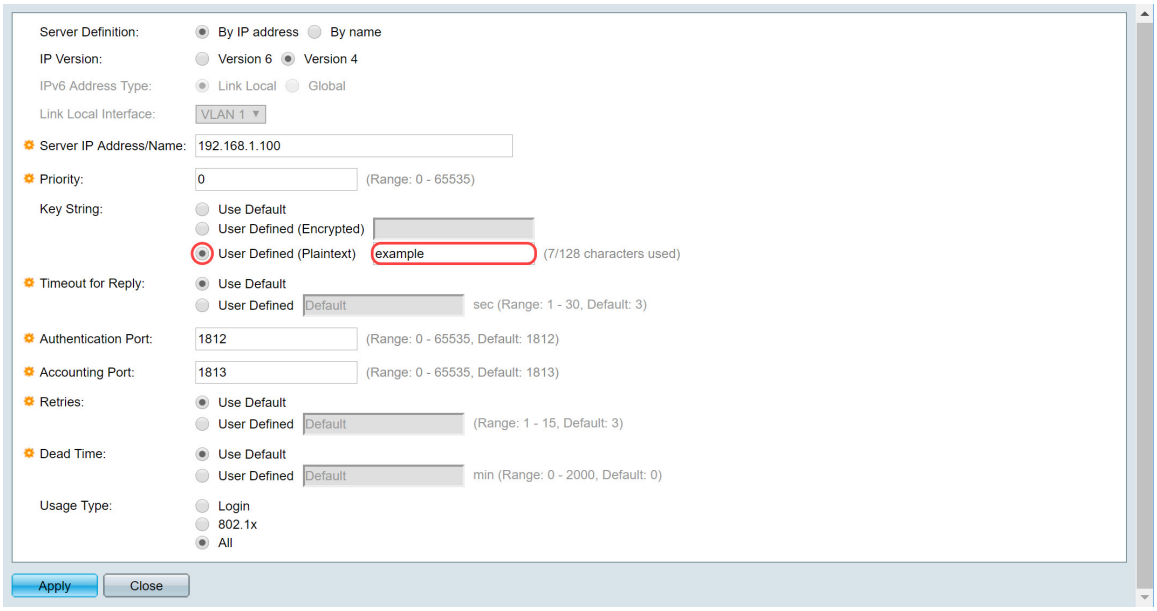


Schritt 6: Geben Sie die Priorität des Servers ein. Die Priorität legt die Reihenfolge fest, in der das Gerät versucht, die Server zu kontaktieren, um einen Benutzer zu authentifizieren. Das Gerät beginnt zuerst mit dem RADIUS-Server mit der höchsten Priorität. "Null" ist die höchste Priorität.



Schritt 7: Geben Sie die Schlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung der Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Sie kann im **verschlüsselten** oder **Klartext-**Format eingegeben werden. Wenn **Use Default** (Standard verwenden) ausgewählt ist, versucht das Gerät, sich mithilfe der Standardschlüsselzeichenfolge beim RADIUS-Server zu authentifizieren. Wir verwenden den **User Defined (Plaintext)** und geben das Schlüsselbeispiel **ein**.

Hinweis: Der Rest der Konfiguration bleibt als Standard erhalten. Sie können sie konfigurieren, wenn Sie möchten.

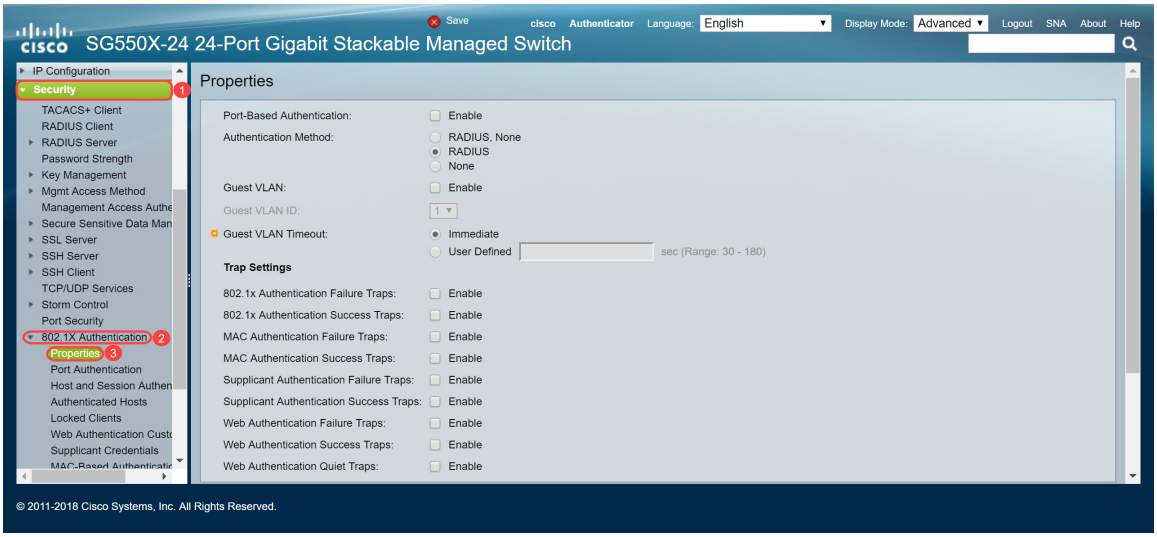


Schritt 8: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

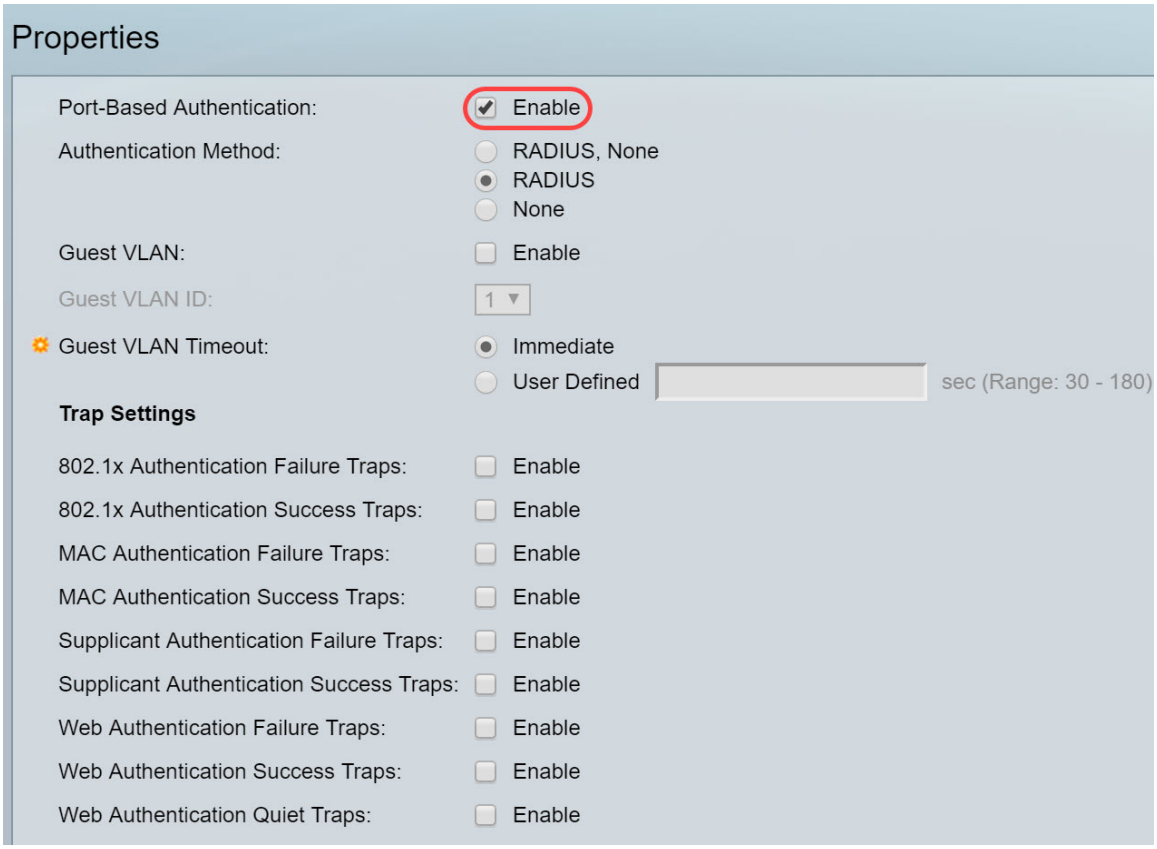
802.1X-Authentifizierungseigenschaften

Die Eigenschaftenseite wird verwendet, um die Port-/Geräteauthentifizierung global zu aktivieren. Damit die Authentifizierung funktioniert, muss sie sowohl global als auch einzeln auf jedem Port aktiviert werden.

Schritt 1: Navigieren Sie zu **Sicherheit > 802.1X Authentication > Properties**.

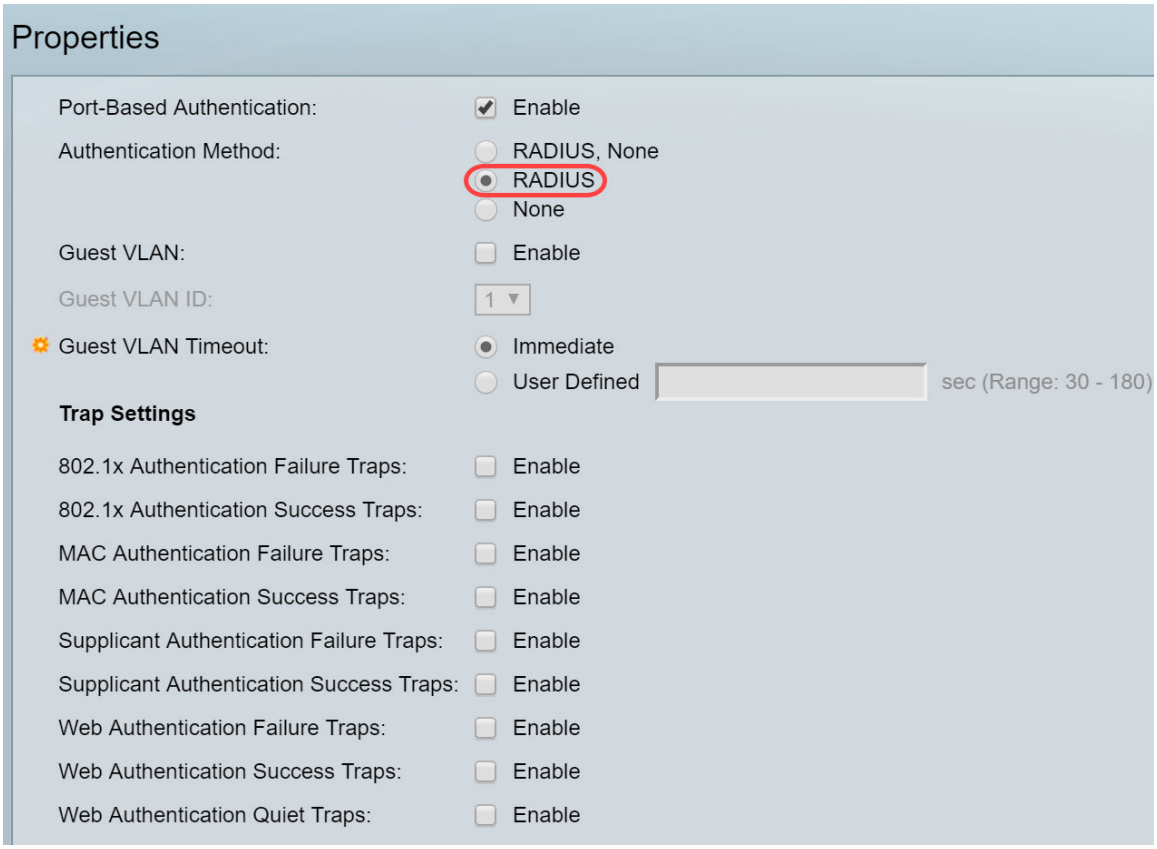


Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Port-basierte Authentifizierung zu aktivieren.

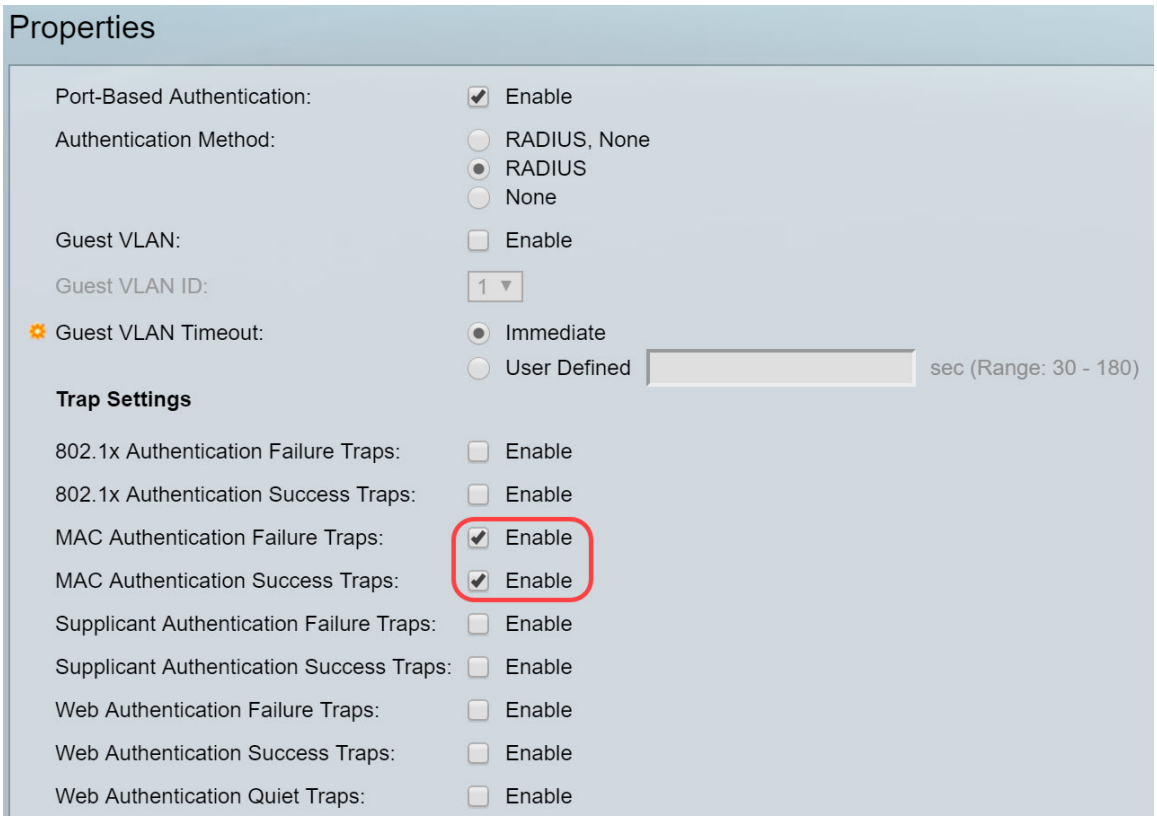


Schritt 3: Wählen Sie die Benutzerauthentifizierungsmethoden aus. Wählen Sie RADIUS als Authentifizierungsmethode aus. Folgende Optionen sind verfügbar:

- RADIUS, None (RADIUS, Keine): Führen Sie zuerst die Port-Authentifizierung mithilfe des RADIUS-Servers durch. Wenn von RADIUS keine Antwort empfangen wird (z. B. wenn der Server ausgefallen ist), wird keine Authentifizierung durchgeführt, und die Sitzung ist zulässig. Wenn der Server verfügbar ist, die Benutzeranmeldeinformationen jedoch nicht korrekt sind, wird der Zugriff verweigert und die Sitzung beendet.
- RADIUS (RADIUS) - Authentifizierung des Benutzers auf dem RADIUS-Server. Wenn keine Authentifizierung durchgeführt wird, ist die Sitzung nicht zulässig.
- None (Keine): Authentifizierung des Benutzers nicht. Zulassen der Sitzung



Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** für *MAC Authentication Failure Traps* und *MAC Authentication Success Traps*. Dadurch wird ein Trap generiert, wenn die MAC-Authentifizierung fehlschlägt oder erfolgreich ist. In diesem Beispiel aktivieren wir sowohl *MAC Authentication Failure Traps* als auch *MAC Authentication Success Traps*.

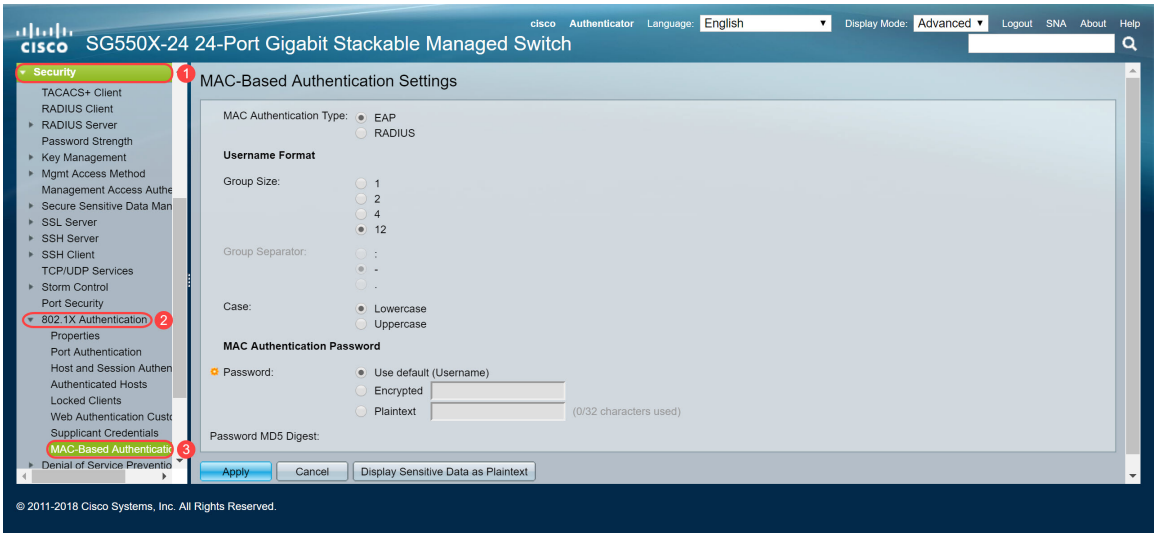


Schritt 5: Klicken Sie auf **Übernehmen**.

MAC-basierte Authentifizierungseinstellungen für 802.1X-Authentifizierung

Auf dieser Seite können Sie verschiedene Einstellungen für die MAC-basierte Authentifizierung konfigurieren.

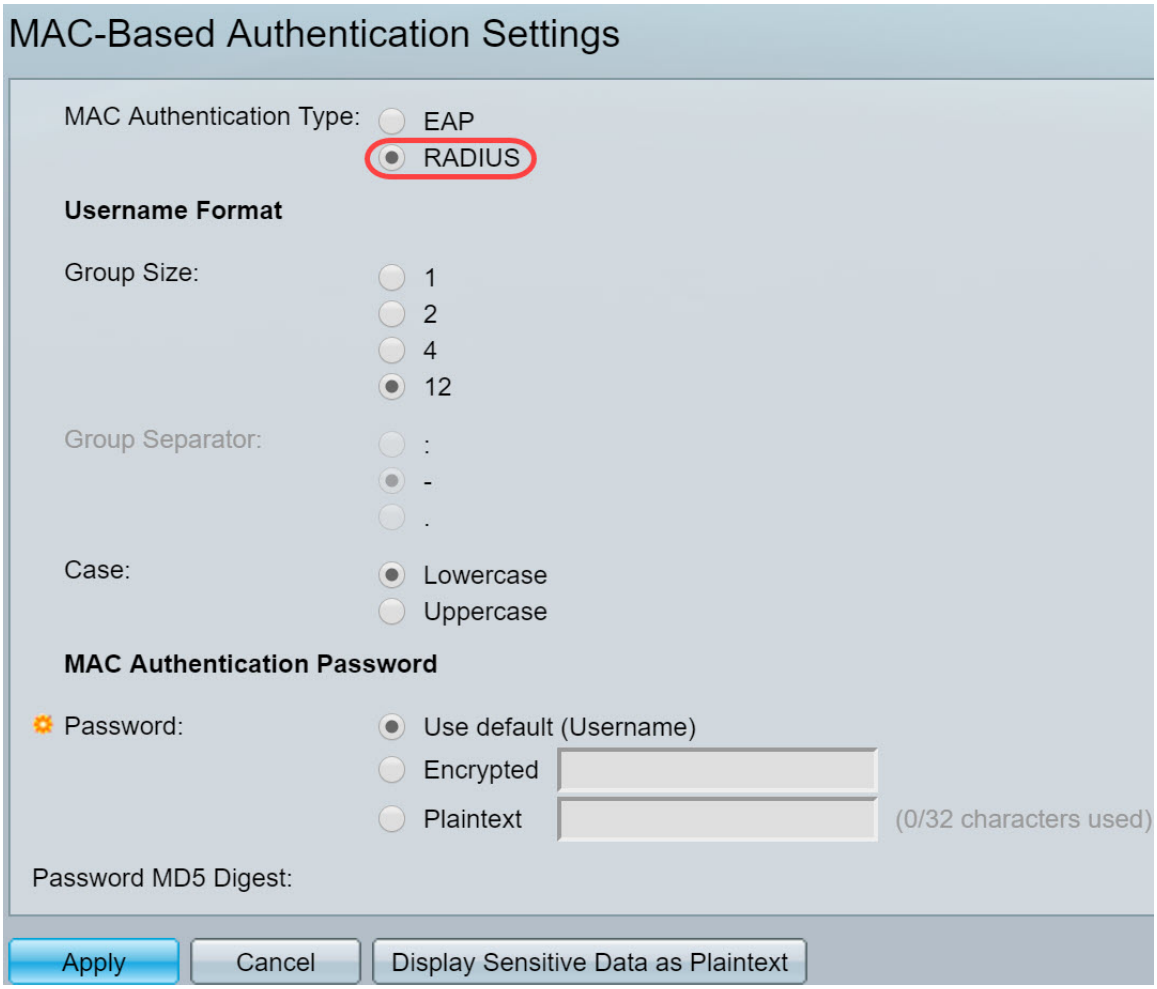
Schritt 1: Navigieren Sie zu **Sicherheit > 802.1X Authentication > MAC-Based Authentication Settings**.



Schritt 2: Wählen Sie im *MAC Authentication Type (MAC-Authentifizierungstyp*) eine der folgenden Optionen aus:

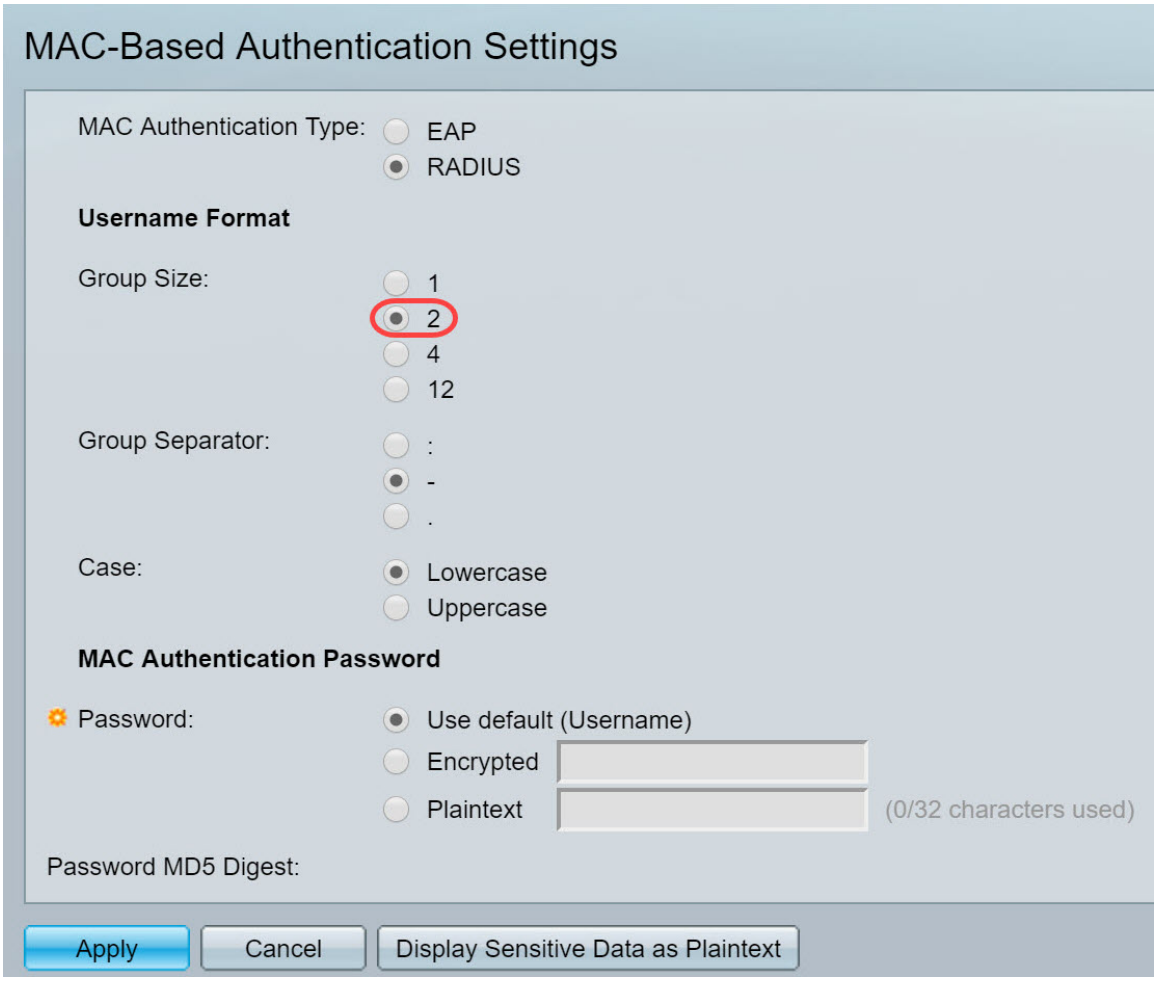
- EAP - Verwenden Sie RADIUS mit EAP-Kapselung für den Datenverkehr zwischen dem Switch (RADIUS-Client) und dem RADIUS-Server, der eine MAC-basierte Komponente authentifiziert.
- RADIUS - Verwenden Sie RADIUS ohne EAP-Kapselung für den Datenverkehr zwischen dem Switch (RADIUS-Client) und dem RADIUS-Server, der eine MAC-basierte Komponente authentifiziert.

In diesem Beispiel wählen wir RADIUS als unseren MAC-Authentifizierungstyp aus.

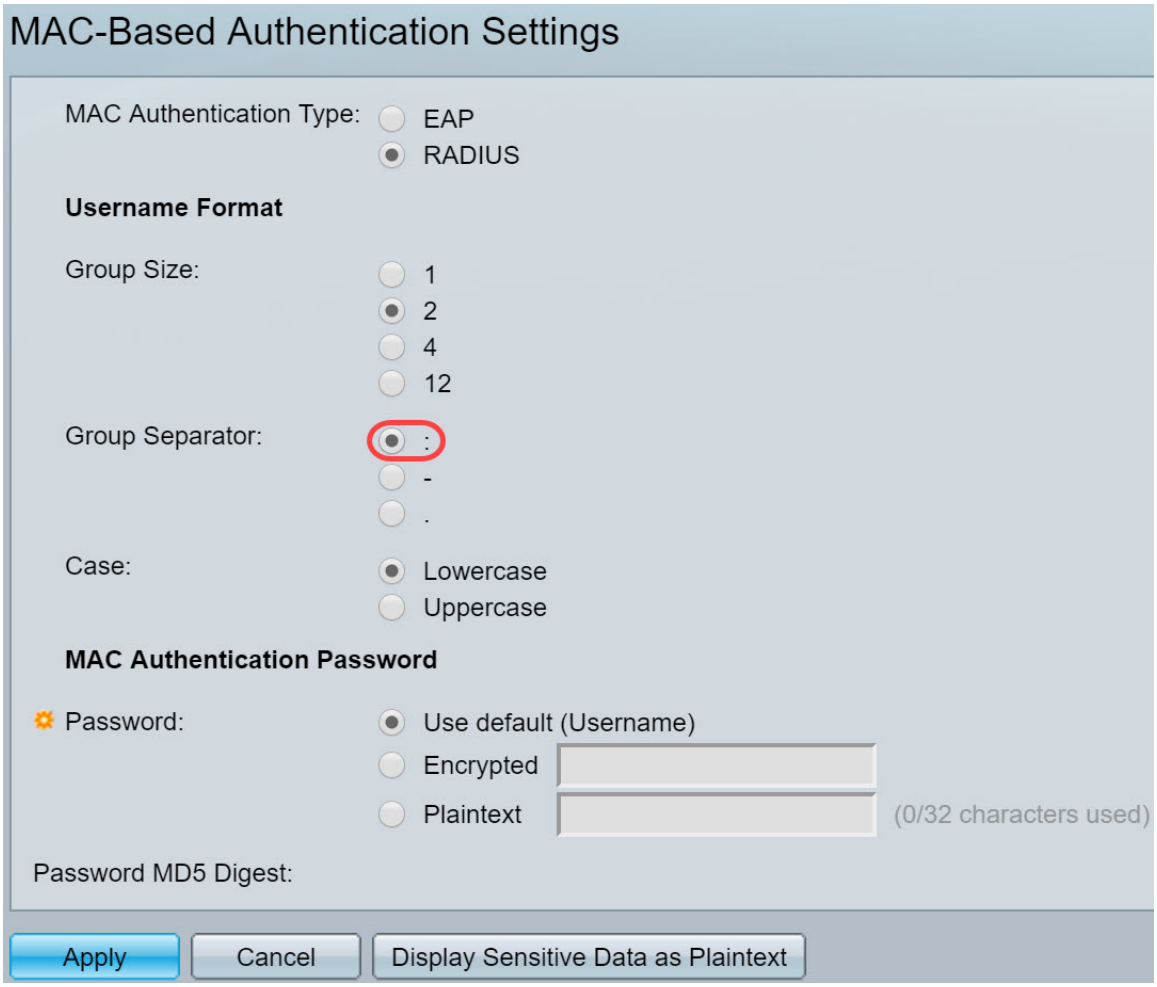


Schritt 3: Wählen Sie im *Username Format* die Anzahl der ASCII-Zeichen zwischen Trennzeichen der als Benutzername gesendeten MAC-Adresse aus. In diesem Fall wählen wir 2 als Gruppengröße.

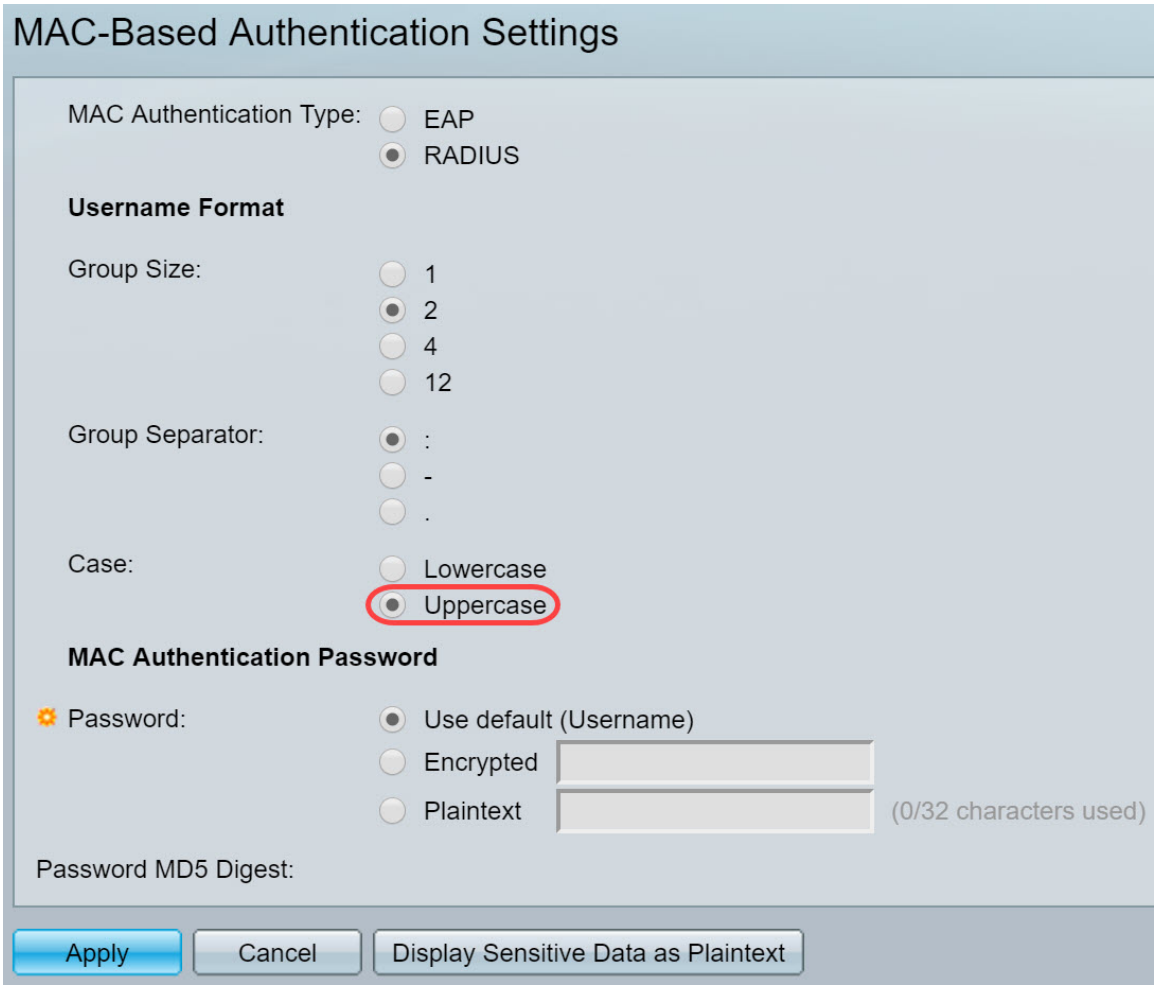
Hinweis: Stellen Sie sicher, dass das Format des Benutzernamens mit der MAC-Adresse übereinstimmt, die Sie im Abschnitt *Radius Server Users* eingeben.



Schritt 4: Wählen Sie das Zeichen aus, das als Trennzeichen zwischen den definierten Zeichengruppen in der MAC-Adresse verwendet wird. In diesem Beispiel wählen Sie **Folgendes aus:** als unser Gruppentrennzeichen.

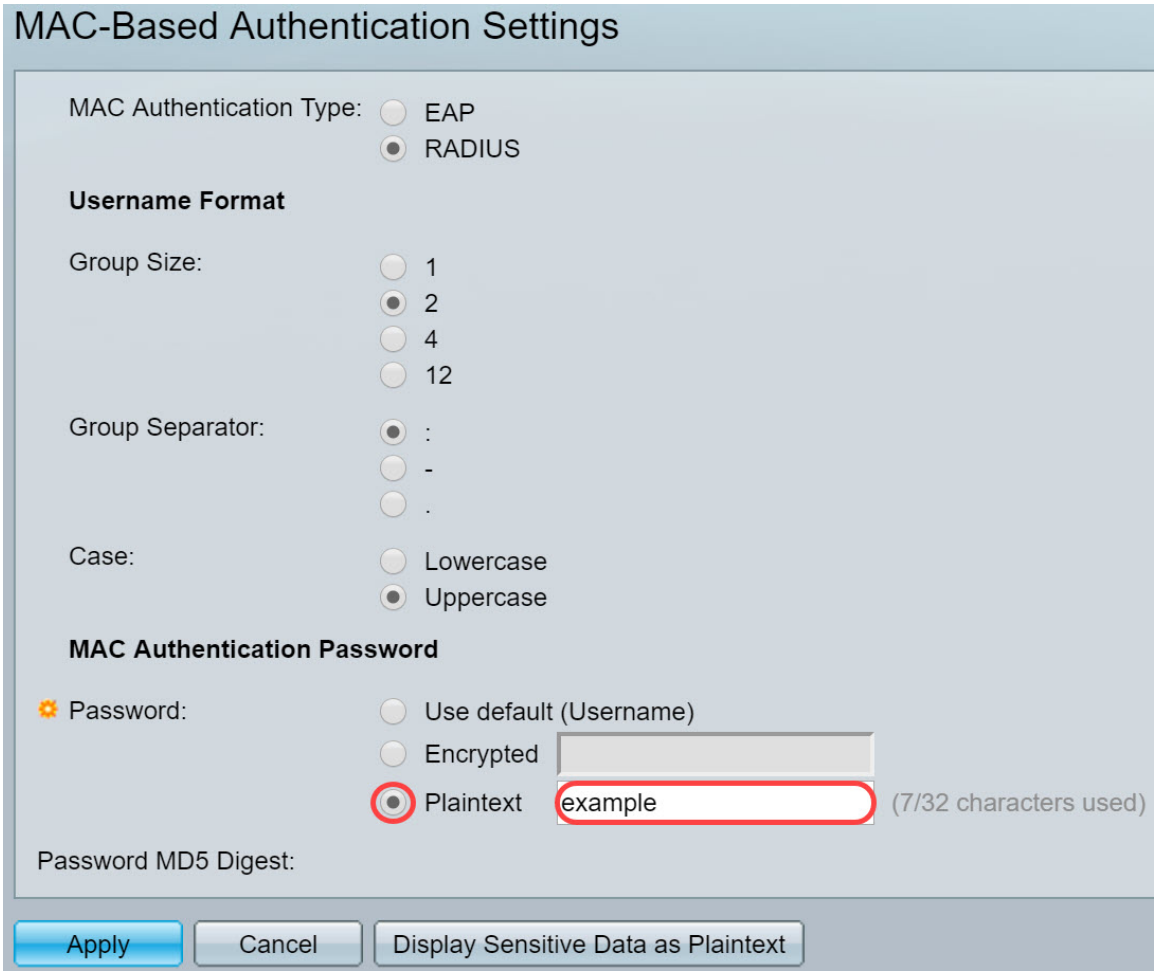


Schritt 5: Wählen Sie im Feld *Case (Groß-*/Kleinschreibung) die Option **Lowercase** oder **Uppercase**, um den Benutzernamen in Groß- oder Kleinschreibung zu senden.



Schritt 6: Das Kennwort legt fest, wie der Switch die Authentifizierung über den RADIUS-Server verwendet. Wählen Sie eine der folgenden Optionen aus:

- Standard verwenden (Benutzername): Wählen Sie diese Option aus, um den definierten Benutzernamen als Kennwort zu verwenden.
- Encrypted (Verschlüsselt): Legen Sie ein Kennwort im verschlüsselten Format fest.
- Plaintext: Legen Sie ein Kennwort im Klartextformat fest.



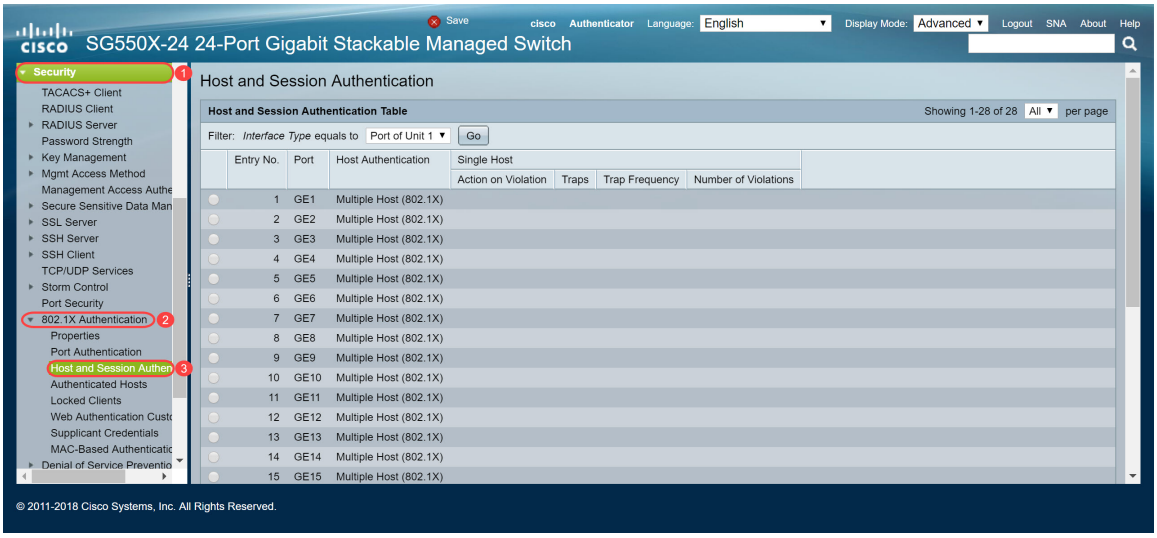
Hinweis:*Password Message-Digest Algorithm 5 (MD5) Digest* zeigt das MD5-Digest-Kennwort an. MD5 ist eine kryptografische Hash-Funktion, die ein Datenstück annimmt und eine eindeutige Hexadezimalausgabe erstellt, die normalerweise nicht reproduzierbar ist. MD5 verwendet einen 128-Bit-Hashwert.

Schritt 7: Klicken Sie auf **Übernehmen**, und die Einstellungen werden in der Konfigurationsdatei Ausführen gespeichert.

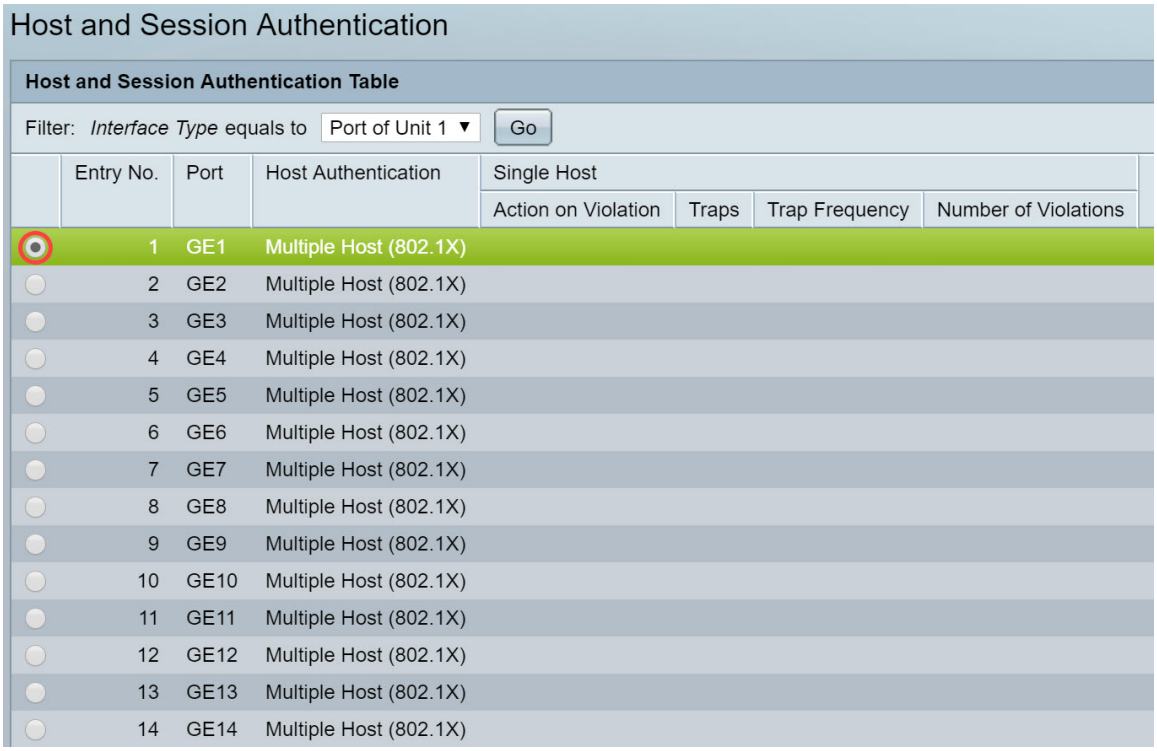
802.1X-Authentifizierungshost und Sitzungsauthentifizierung

Auf der Seite *Host und Session Authentication* können Sie festlegen, in welchem Modus 802.1X auf dem Port betrieben wird und welche Aktionen ausgeführt werden sollen, wenn eine Verletzung erkannt wurde.

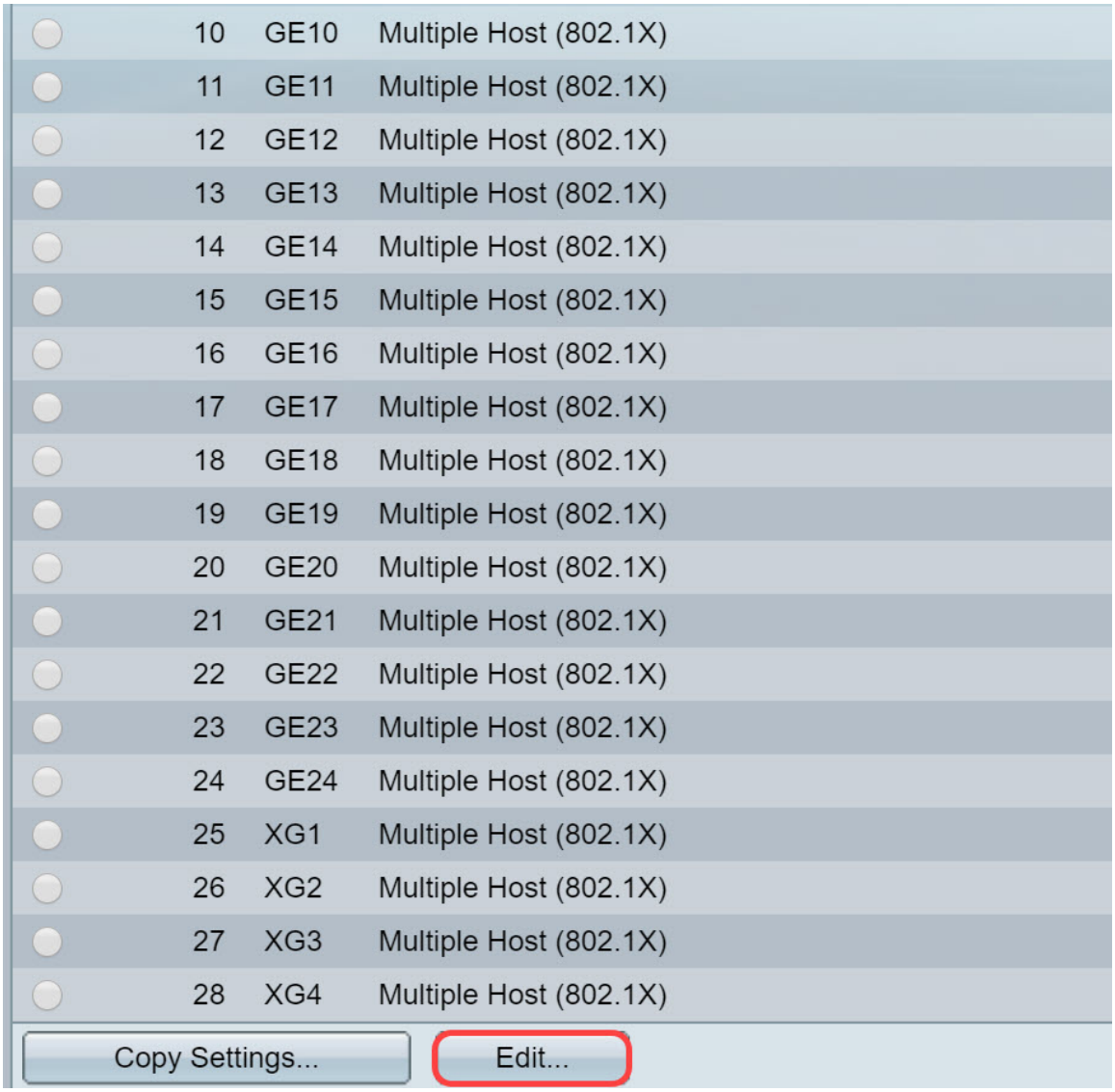
Schritt 1: Navigieren Sie zu **Sicherheit > 802.1X Authentication > Host and Session Authentication**.



Schritt 2: Wählen Sie den Port aus, für den die Host-Authentifizierung konfiguriert werden soll. In diesem Beispiel wird GE1 konfiguriert, da es mit einem End-Host verbunden ist.



Schritt 3: Klicken Sie auf **Bearbeiten...** um den Port zu konfigurieren.



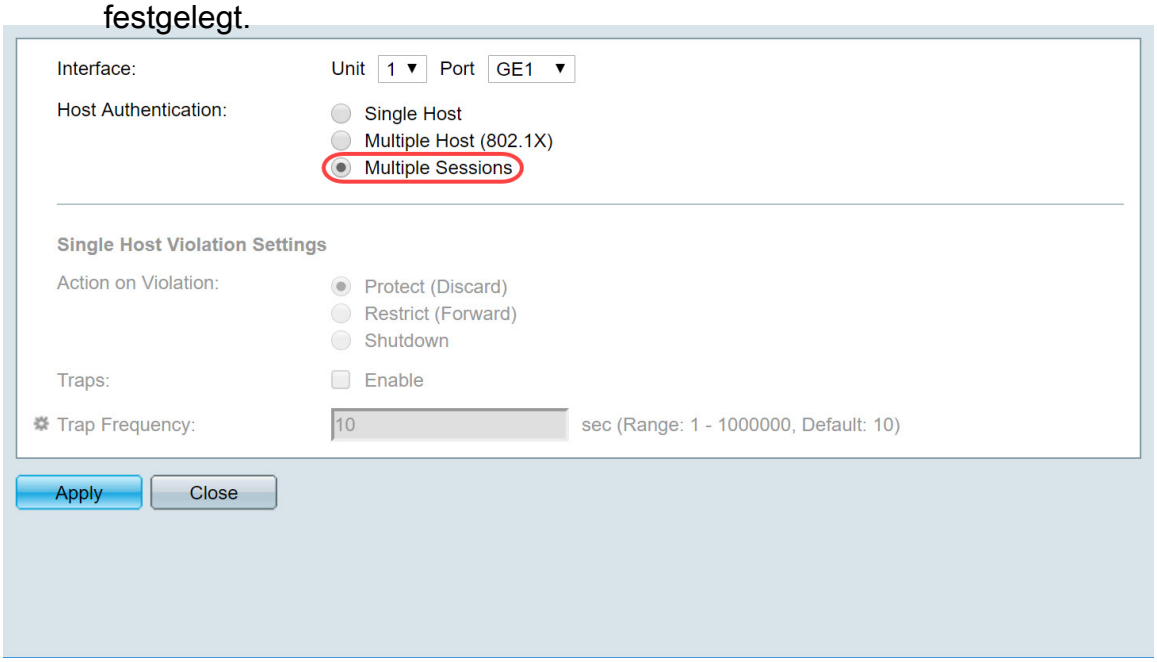
Schritt 4: Wählen Sie im Feld *Hostauthentifizierung* eine der folgenden Optionen aus:

1. Single-Host-Modus
   - Ein Port ist autorisiert, wenn ein autorisierter Client vorhanden ist. Auf einem Port kann nur ein Host autorisiert werden.
   - Wenn ein Port nicht autorisiert ist und das Gast-VLAN aktiviert ist, wird nicht markierter Datenverkehr dem Gast-VLAN neu zugeordnet. Tagged Datenverkehr wird verworfen, es sei denn, er gehört zum Gast-VLAN oder zu einem nicht authentifizierten VLAN. Wenn ein Gast-VLAN auf dem Port nicht aktiviert ist, wird nur markierter Datenverkehr überbrückt, der zu den nicht authentifizierten VLANs gehört.
   - Wenn ein Port autorisiert ist, wird der nicht getaggte und getaggte Datenverkehr vom autorisierten Host basierend auf der Konfiguration des statischen Ports für die VLAN-Mitgliedschaft überbrückt. Datenverkehr von anderen Hosts wird verworfen.
   - Ein Benutzer kann festlegen, dass nicht markierter Datenverkehr vom autorisierten Host einem VLAN zugeordnet wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der *Port*-Authentifizierungsseite festgelegt.
2. Multi-Host-Modus
   - Ein Port ist autorisiert, wenn mindestens ein autorisierter Client vorhanden ist.
   - Wenn ein Port nicht autorisiert ist und ein Gast-VLAN aktiviert ist, wird nicht markierter

Datenverkehr dem Gast-VLAN neu zugeordnet. Tagged Datenverkehr wird verworfen, es sei denn, er gehört zum Gast-VLAN oder zu einem nicht authentifizierten VLAN. Wenn das Gast-VLAN auf einem Port nicht aktiviert ist, wird nur markierter Datenverkehr überbrückt, der zu nicht authentifizierten VLANs gehört.

- Wenn ein Port autorisiert ist, wird der nicht getaggte und getaggte Datenverkehr aller Hosts, die mit dem Port verbunden sind, je nach der Konfiguration des statischen Ports für die VLAN-Mitgliedschaft überbrückt.
- Sie können festlegen, dass nicht markierter Datenverkehr vom autorisierten Port einem VLAN zugewiesen wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der Seite *Port Authentication (Portauthentifizierung)* festgelegt.

3. Modus für mehrere Sitzungen
   - Im Gegensatz zum Single-Host- und Multi-Host-Modus besitzt ein Port im Multi-Session-Modus keinen Authentifizierungsstatus. Dieser Status wird jedem Client zugewiesen, der mit dem Port verbunden ist.
   - Tagged-Datenverkehr, der zu einem nicht authentifizierten VLAN gehört, wird immer überbrückt, unabhängig davon, ob der Host autorisiert ist oder nicht.
   - Getaggte und nicht getaggte Zugriffe von nicht autorisierten Hosts, die nicht zu einem nicht authentifizierten VLAN gehören, werden dem Gast-VLAN neu zugeordnet, wenn sie im VLAN definiert und aktiviert sind, oder verworfen, wenn das Gast-VLAN auf dem Port nicht aktiviert ist.
   - Sie können festlegen, dass nicht markierter Datenverkehr vom autorisierten Port einem VLAN zugewiesen wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der Seite *Port Authentication* festgelegt.



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

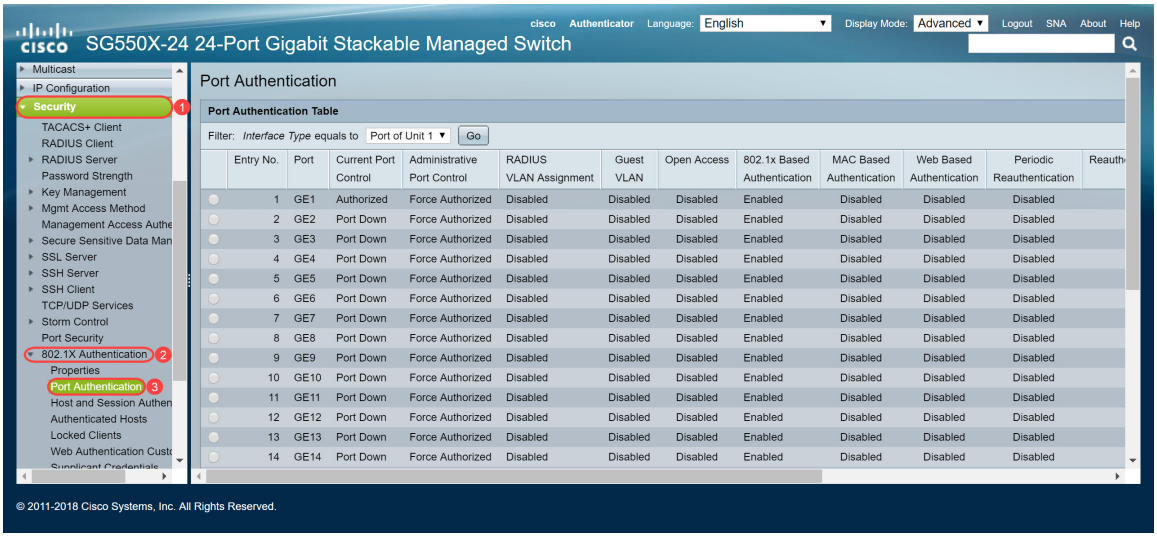
Hinweis: *Kopiereinstellungen* verwenden... um dieselbe GE1-Konfiguration auf mehrere Ports anzuwenden. Lassen Sie den Port, der mit dem RADIUS-Server verbunden ist, als *Multiple Host (802.1X)* belassen.

Authentifizierung des 802.1X-Authentifizierungsports

Die Seite *"Port Authentication*" (Portauthentifizierung) ermöglicht die Konfiguration von Parametern für jeden Port. Da einige Konfigurationsänderungen nur möglich sind, während sich der Port im Force Authorized-Status befindet, z. B. die Host-Authentifizierung, wird empfohlen, das Port-Steuerelement vor Änderungen in Force Authorized (Autorisiert erzwingen) zu ändern. Wenn die Konfiguration abgeschlossen ist, setzen Sie die Port-Steuerung in den vorherigen Zustand zurück.

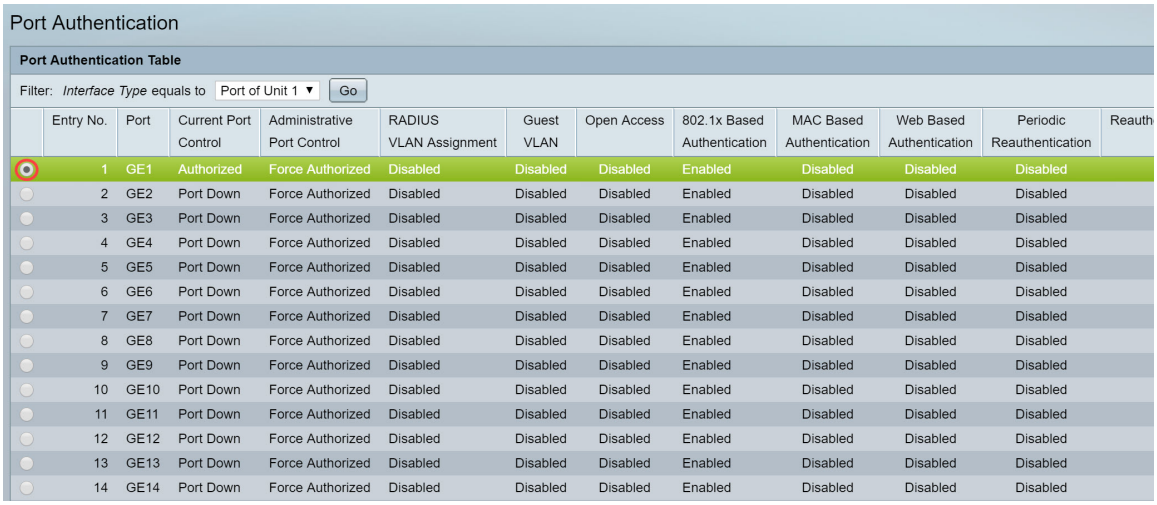
Hinweis: Wir konfigurieren nur Einstellungen, die für die MAC-basierte Authentifizierung erforderlich sind. Der Rest der Konfiguration bleibt als Standard erhalten.

Schritt 1: Navigieren Sie zu **Security > 802.1X Authentication > Port Authentication (Sicherheit > 802.1X-Authentifizierung > Portauthentifizierung)**.

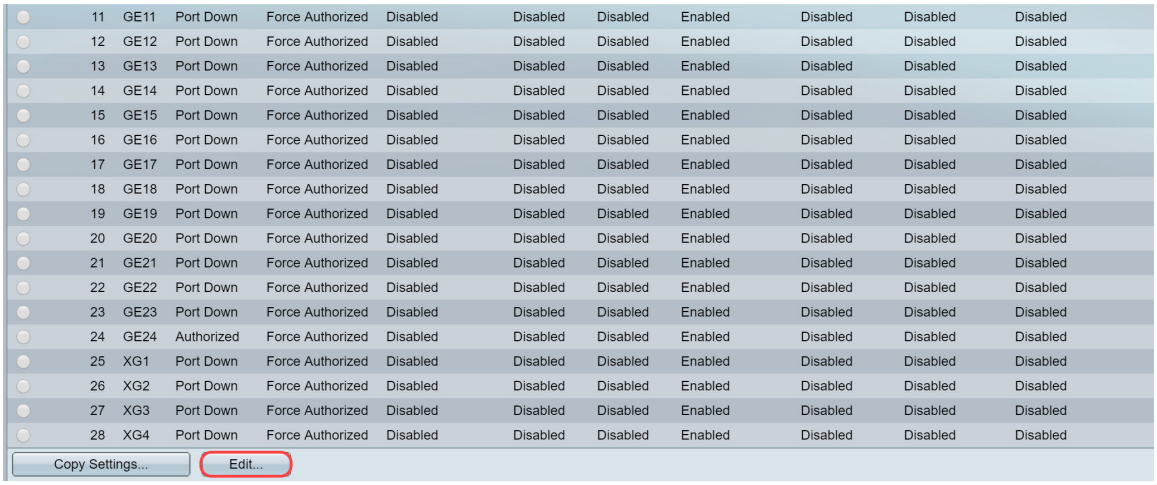


Schritt 2: Wählen Sie den Port aus, den Sie für die Port-Autorisierung konfigurieren möchten.

Hinweis: Konfigurieren Sie nicht den Port, an den der Switch angeschlossen ist. Der Switch ist ein vertrauenswürdiges Gerät. Lassen Sie diesen Port also als *autorisiert*, um *ihn zu autorisieren*.



Schritt 3: Blättern Sie dann nach unten, und klicken Sie auf **Bearbeiten...** um den Port zu konfigurieren.



11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
15	GE15	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
16	GE16	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
17	GE17	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
18	GE18	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
19	GE19	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
20	GE20	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
21	GE21	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
22	GE22	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
23	GE23	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
24	GE24	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
25	XG1	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
26	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
27	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

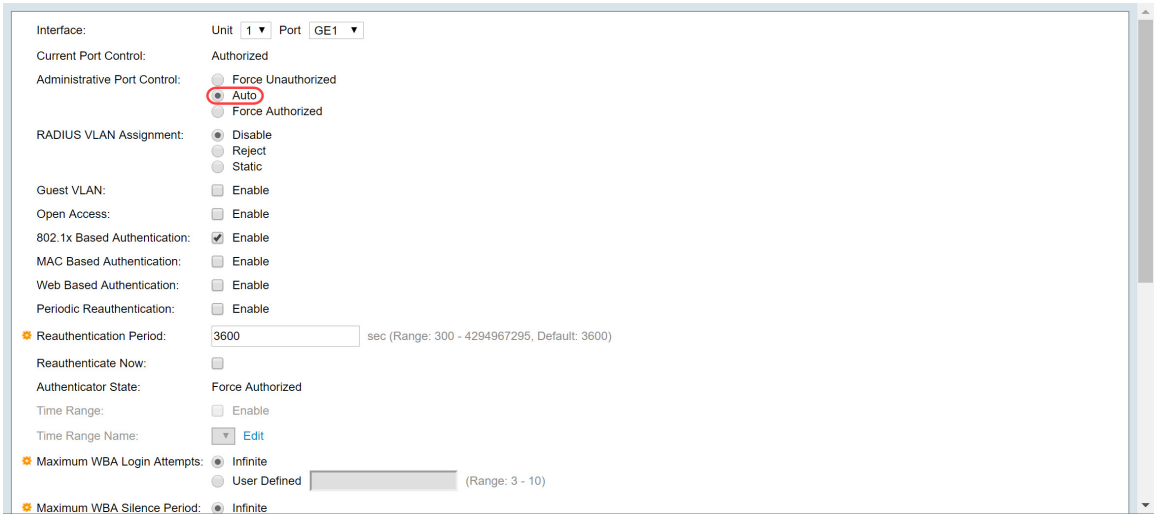
Copy Settings... Edit...

Auf der Seite *"Edit Port Authentication"* (*Portauthentifizierung bearbeiten)* wird im Feld *Current Port Control* der aktuelle Autorisierungsstatus angezeigt. Wenn der Status *Authorized* ist, wird der Port entweder authentifiziert oder die *Administrative Port Control* ist *Force Authorized*. Umgekehrt wird der Port entweder nicht authentifiziert, wenn der Status *nicht autorisiert* ist oder der *Administrative Port Control* ist *Force Unauthorized*. Wenn Supplicant auf einer Schnittstelle aktiviert ist, ist die aktuelle Port-Steuerung Supplicant.

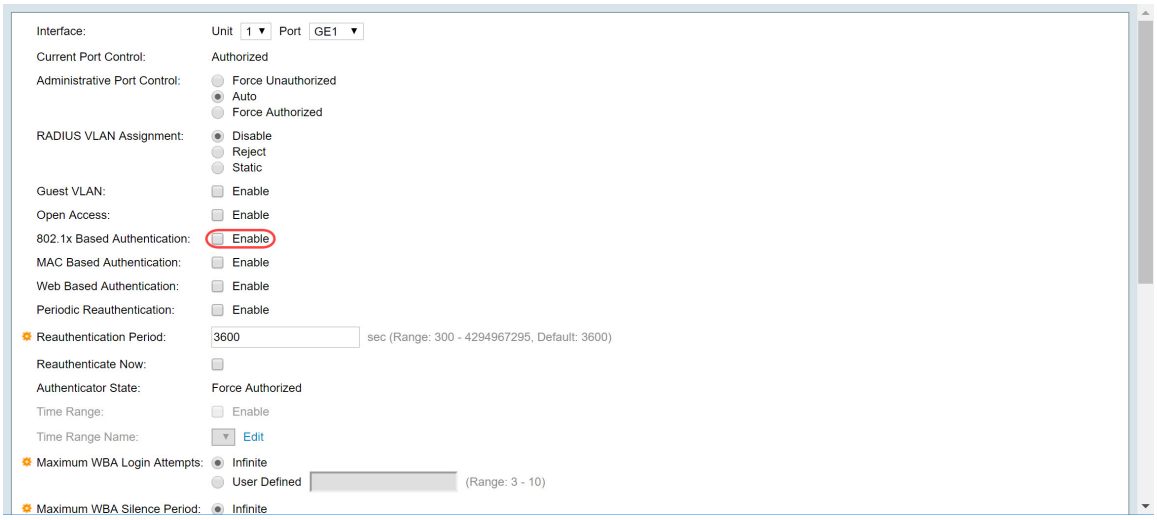
Schritt 4: Wählen Sie den Autorisierungsstatus des administrativen Ports aus. Konfigurieren Sie den Port auf **Auto (Automatisch)**. Folgende Optionen stehen zur Verfügung:

- Forced Unauthorized (Nicht autorisiert erzwingen): Verweigert den Schnittstellenzugriff, indem die Schnittstelle in den nicht autorisierten Zustand verschoben wird. Das Gerät stellt dem Client über die Schnittstelle keine Authentifizierungsdienste zur Verfügung.
- Auto (Automatisch): Aktiviert die Port-basierte Authentifizierung und Autorisierung auf dem Gerät. Die Schnittstelle wechselt zwischen einem autorisierten oder einem nicht autorisierten Zustand, der auf dem Authentifizierungsaustausch zwischen Gerät und Client basiert.
- Forced Authorized - Autorisiert die Schnittstelle ohne Authentifizierung.

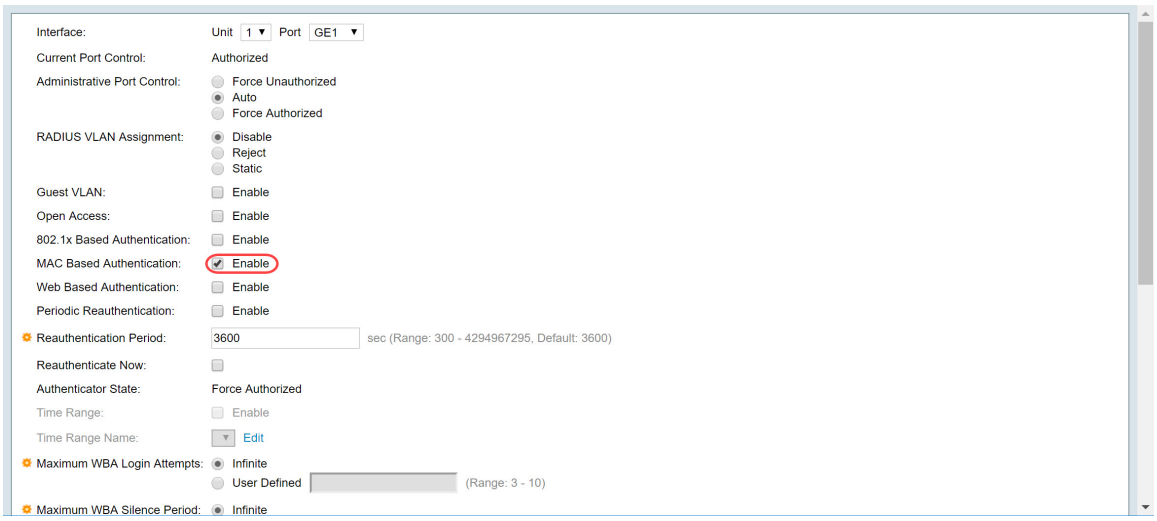
Hinweis: *Forced Authorized* ist der Standardwert.



Schritt 5: Deaktivieren Sie im Feld *802.1X Based Authentication* das **Kontrollkästchen Enable (Aktivieren)**, da 802.1X nicht als Authentifizierung verwendet wird. Der Standardwert für die *802.1x-basierte Authentifizierung* ist aktiviert.



Schritt 6: Aktivieren Sie das Kontrollkästchen **Aktivieren** für *MAC-basierte Authentifizierung*, da die Port-Authentifizierung auf Basis der zugehörigen MAC-Adresse aktiviert werden soll. Auf dem Port können nur 8 MAC-basierte Authentifizierungen verwendet werden.



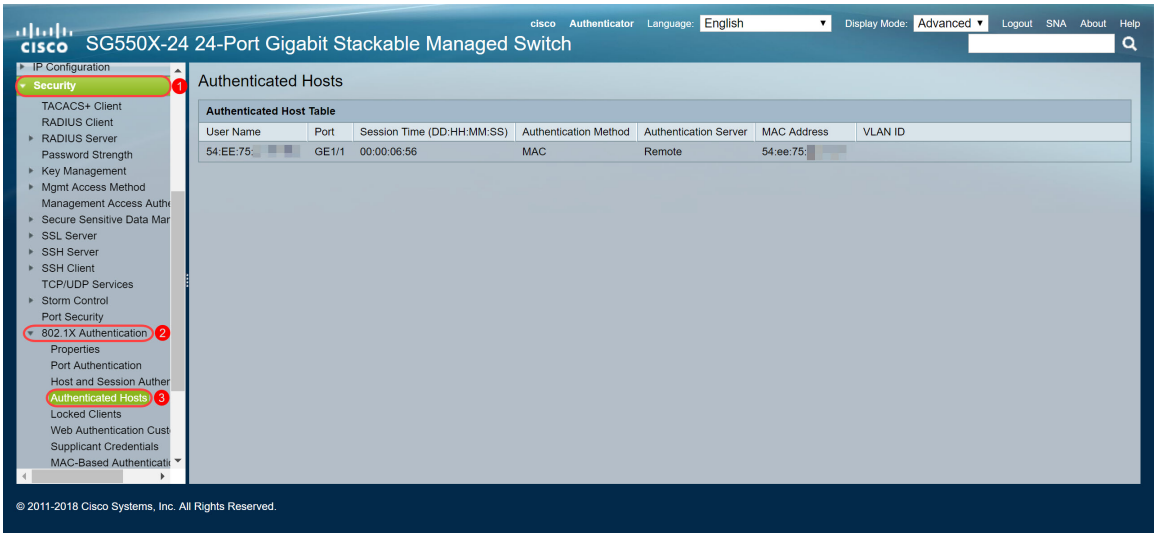
Schritt 7: Klicken Sie auf **Apply**, um die Änderungen zu speichern.

Wenn Sie Ihre Konfiguration speichern möchten, drücken Sie die **Save**-Taste am oberen Bildschirmrand.

Schlussfolgerung

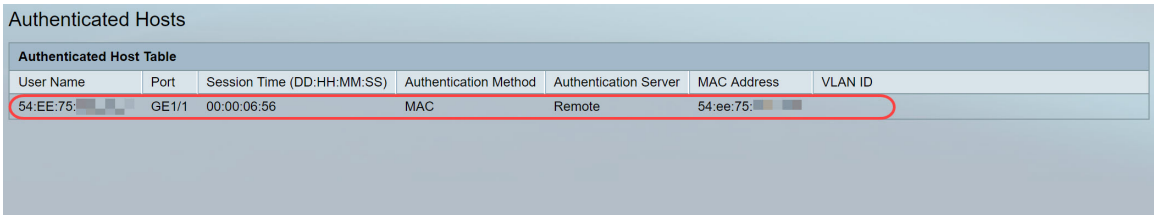
Sie haben nun erfolgreich die MAC-basierte Authentifizierung auf Ihrem Switch konfiguriert. Um zu überprüfen, ob die MAC-basierte Authentifizierung funktioniert, gehen Sie wie folgt vor.

Schritt 1: Navigieren Sie zu **Sicherheit > 802.1X Authentication > Authenticated Hosts**, um Details zu authentifizierten Benutzern anzuzeigen.

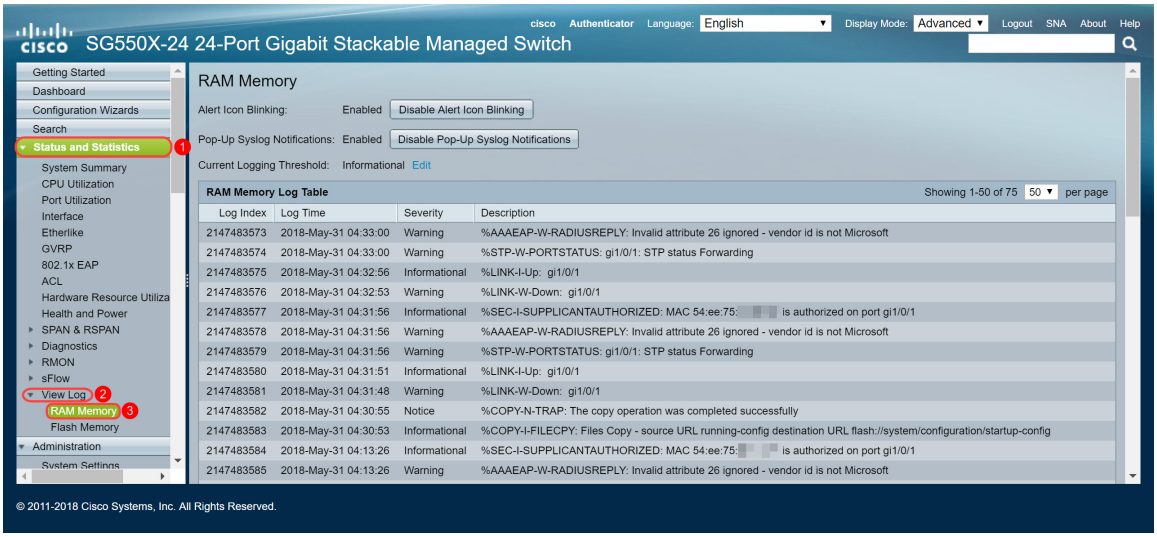


Schritt 2: In diesem Beispiel sehen Sie, dass unsere Ethernet-MAC-Adresse in der *Authenticated Host Table* authentifiziert wurde. Die folgenden Felder sind definiert als:

- Benutzername - Supplicant-Namen, die sich an jedem Port authentifiziert haben.
- Port - Anzahl der Ports.
- Sitzungszeit (DD:HH:MM:SS) - Zeitraum, innerhalb dessen der Supplicant authentifiziert und autorisiert wurde.
- Authentifizierungsmethode - Methode, mit der die letzte Sitzung authentifiziert wurde.
- Authentifizierter Server - RADIUS-Server.
- MAC Address (MAC-Adresse): Zeigt die ergänzende MAC-Adresse an.
- VLAN-ID - VLAN des Ports



Schritt 3: (Optional) Navigieren Sie zu **Status und Statistiken > Protokoll anzeigen > RAM-Speicher**. Die Seite *RAM-Speicher* zeigt alle im RAM (Cache) gespeicherten Meldungen in chronologischer Reihenfolge an. Einträge werden entsprechend der Konfiguration auf der Seite *Protokolleinstellungen* im RAM-Protokoll gespeichert.



Schritt 4: In der *RAM-Speicherprotokolltabelle* sollte eine Informationsprotokollmeldung angezeigt werden, die angibt, dass Ihre MAC-Adresse auf Port gi1/0/1 autorisiert ist.

Hinweis: Ein Teil der MAC-Adresse ist verschwommen.

2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1

Video-Version dieses Artikels anzeigen...

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.