Konfigurieren von 802.1X auf Switches der Serie SG300

Ziel

802.1X ist ein IEEE-Standard, der eine portbasierte Authentifizierung implementiert. Wenn ein Port 802.1X verwendet, muss jeder Client, der diesen Port verwendet (der so genannte Supplicant), korrekte Anmeldeinformationen vorlegen, bevor ihm der Zugriff auf das Netzwerk gewährt wird. Ein Gerät, das 802.1X implementiert (als Authentifizierer bezeichnet), muss mit einem RADIUS-Server (Remote Authentication Dial-In User Service, RADIUS (Remote-Authentifizierungs-Einwahldienst) kommunizieren können, der sich an einem anderen Ort im Netzwerk befindet. Dieser Server enthält eine Liste gültiger Benutzer, denen der Zugriff auf das Netzwerk gestattet ist. Alle vom Authentifizierer (vom Supplicant an ihn weitergegebenen) Anmeldeinformationen müssen mit den Anmeldeinformationen des RADIUS-Servers übereinstimmen. Wenn ja, weist der Server den Authentifizierer an, dem Benutzer Zugriff zu gewähren. Andernfalls verweigert der Authentifizierer den Zugriff.

Der 802.1X-Standard ist eine gute Sicherheitsmaßnahme, um unerwünschten Benutzern den Zugriff auf das Netzwerk zu verwehren, indem sie sich an einen physischen Port anschließen. Bitte beachten Sie, dass für die Funktion von 802.1X bereits ein RADIUS-Server an einer anderen Stelle im Netzwerk konfiguriert sein muss und der Authentifizierer damit kommunizieren kann.

In diesem Dokument wird die Einrichtung von 802.1X für Switches der Serie SG300 erläutert.

Anwendbare Geräte

·Switches der Serie SG300

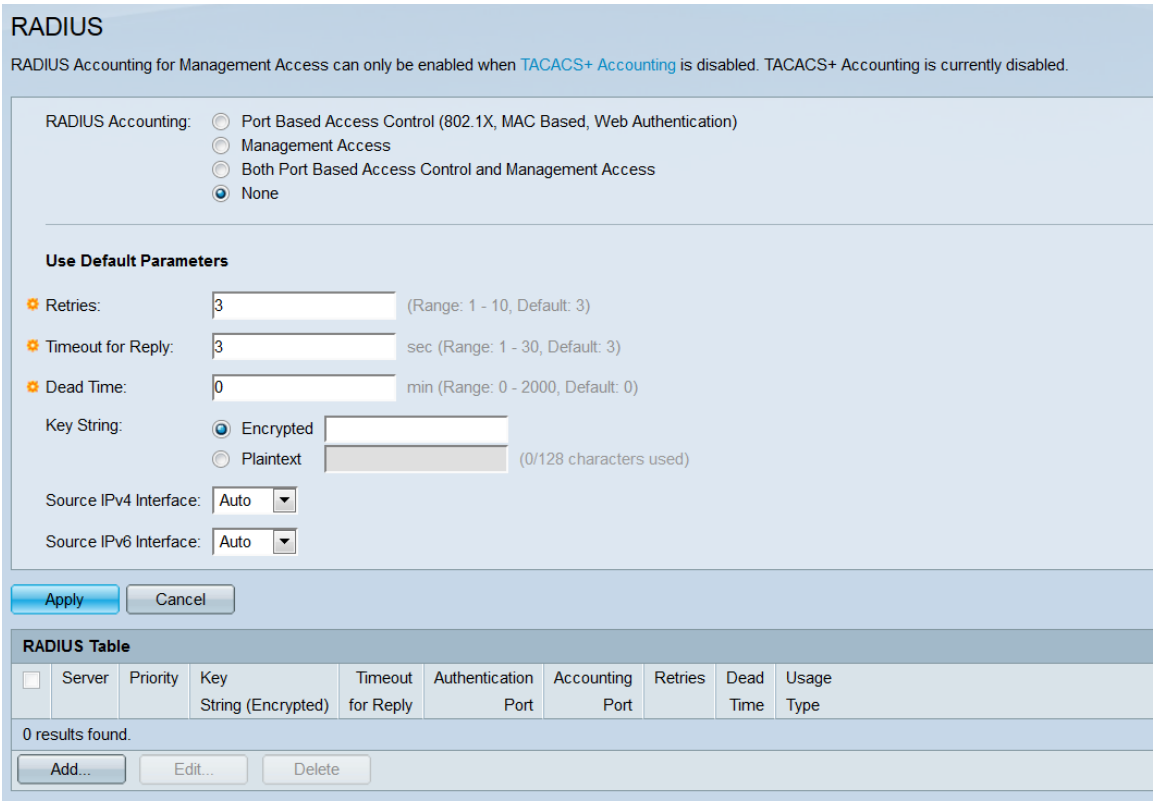
Softwareversion

·v1.4.1.3

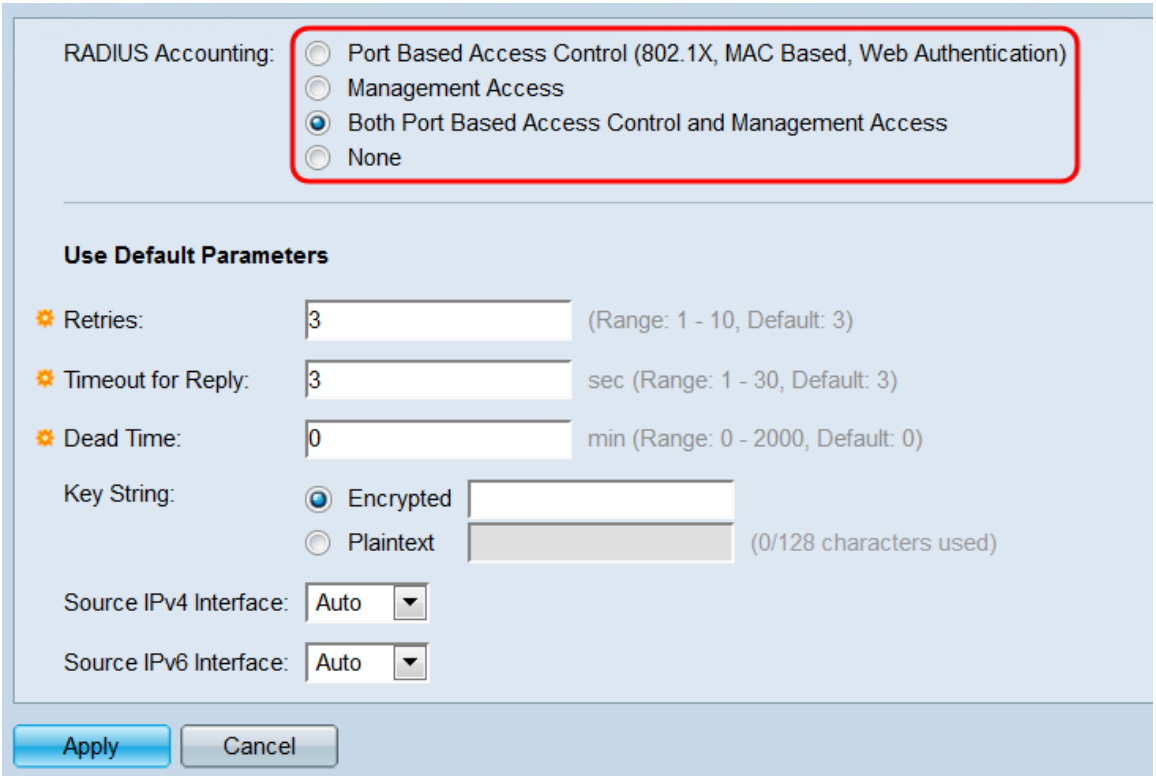
Einrichten der 802.1X-Authentifizierung

Hinzufügen eines RADIUS-Servers

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



Schritt 2: Wählen Sie im Feld *RADIUS Accounting* (RADIUS-*Accounting*) ein Optionsfeld aus, um auszuwählen, welche Accounting-Informationen dem RADIUS-Server zugewiesen werden sollen. Ein RADIUS-Server kann Accounting-Informationen erhalten, die die Sitzungszeit, die verwendeten Ressourcen und andere Dinge eines Benutzers überwachen. Die hier ausgewählte Option hat keine Auswirkungen auf die Leistung von 802.1X.



Folgende Optionen stehen zur Verfügung:

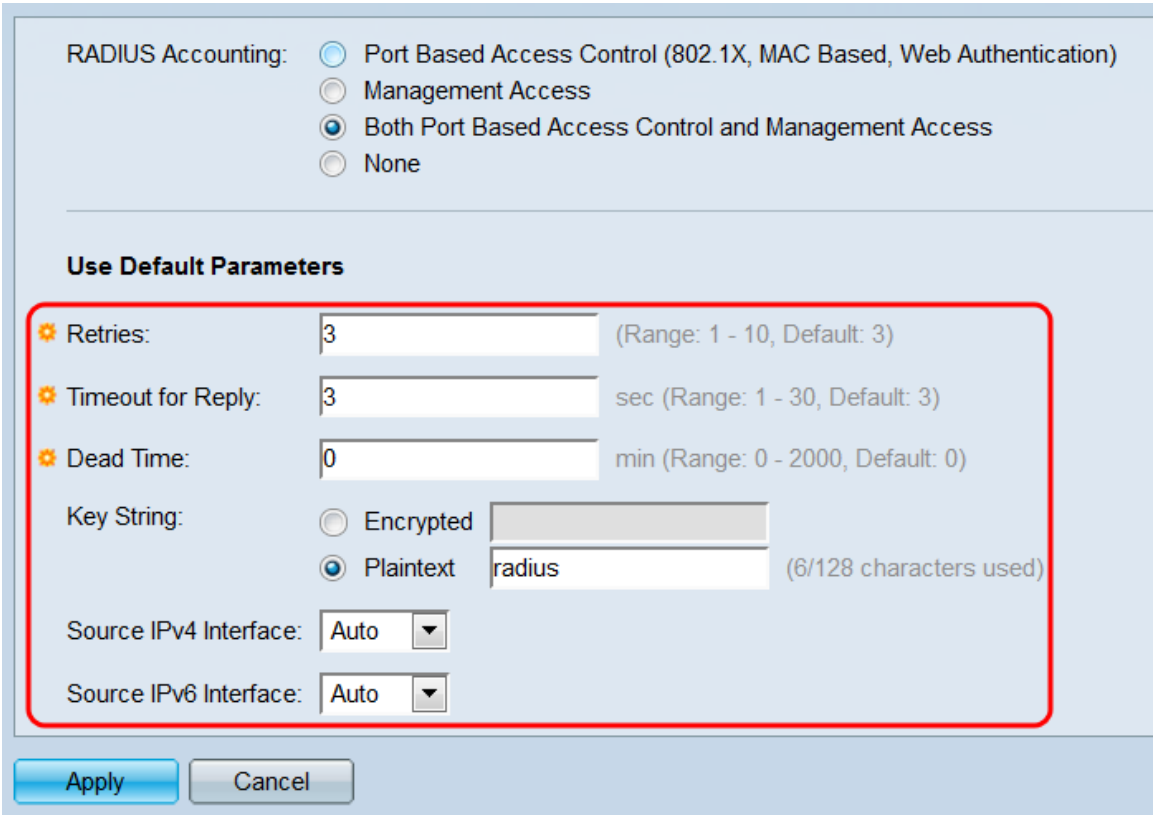
·Portbasierte Zugriffskontrolle - Diese Option sendet Accounting-Informationen über Port-basierte authentifizierte Sitzungen an den RADIUS-Server.

·Managementzugriff - Diese Option sendet Accounting-Informationen über die Managementsitzungen des Switches an den RADIUS-Server.

·Port-basierte Zugriffskontrolle und Verwaltungszugriff: Diese Option sendet beide Arten von Accounting-Informationen an den RADIUS-Server.

·Keine - Senden Sie keine Accounting-Informationen an den RADIUS-Server.

Schritt 3: Konfigurieren Sie im Bereich *Standardparameter verwenden* die standardmäßig verwendeten Einstellungen, es sei denn, ein hinzugefügter RADIUS-Server wird mit eigenen spezifischen Einstellungen konfiguriert. Jeder einzelne Servereintrag, den Sie dem Switch hinzufügen, kann entweder die Standardeinstellungen oder einzelne eindeutige Einstellungen verwenden. In diesem Artikel werden die in diesem Abschnitt definierten Standardeinstellungen verwendet.



Konfigurieren Sie die folgenden Einstellungen:

·Wiederholungen: Geben Sie ein, wie oft der Switch versucht, einen RADIUS-Server zu kontaktieren, bevor er zum nächsten Server wechselt. Der Standardwert ist 3.

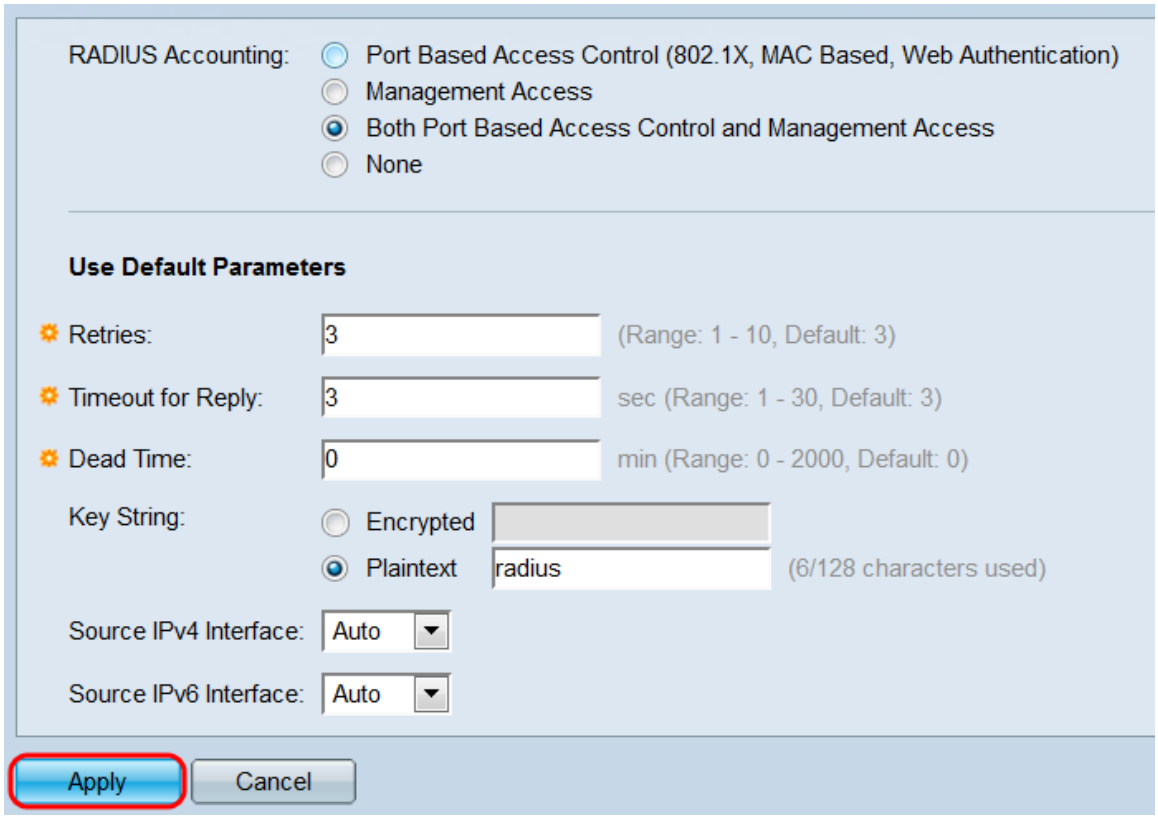
·Timeout for Reply (Zeitüberschreitung für Antwort): Geben Sie die Anzahl der Sekunden ein, die der Switch auf eine Antwort vom RADIUS-Server wartet, bevor er weitere Maßnahmen ergreift (Wiederholen oder Aufgeben). Der Standardwert ist 3.

·Dead Time (Ausfallzeit): Geben Sie die Anzahl der Minuten ein, die vergehen, bevor ein nicht reagierender RADIUS-Server für Serviceanfragen übergeben wird. Der Standardwert ist 0. Dieser Wert bedeutet, dass der Server nicht umgangen wird.

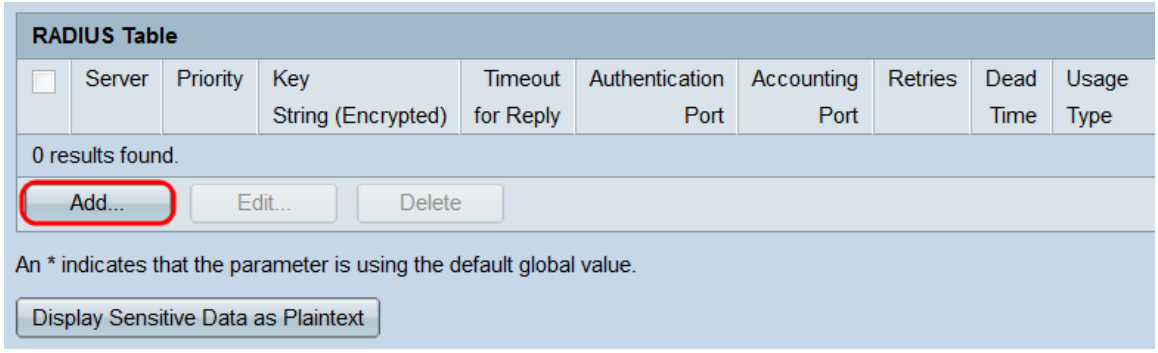
·Key String - Geben Sie den geheimen Schlüssel für die Authentifizierung zwischen dem Switch und dem RADIUS-Server ein. Wenn Sie über einen verschlüsselten Schlüssel verfügen, geben Sie ihn mit dem Optionsfeld **Verschlüsselt** ein. Geben Sie andernfalls die Klartext-Taste mit dem Optionsfeld **Plaintext** ein.

·IPv4/IPv6-Quellschnittstelle - Wählen Sie mithilfe dieser Dropdown-Listen aus, welche IPv4/IPv6-Quellschnittstelle bei der Kommunikation mit dem RADIUS-Server verwendet wird. Der Standardwert ist "Auto" (Automatisch). Dabei wird die standardmäßige Quell-IP-Adresse verwendet, die auf der ausgehenden Schnittstelle definiert ist.

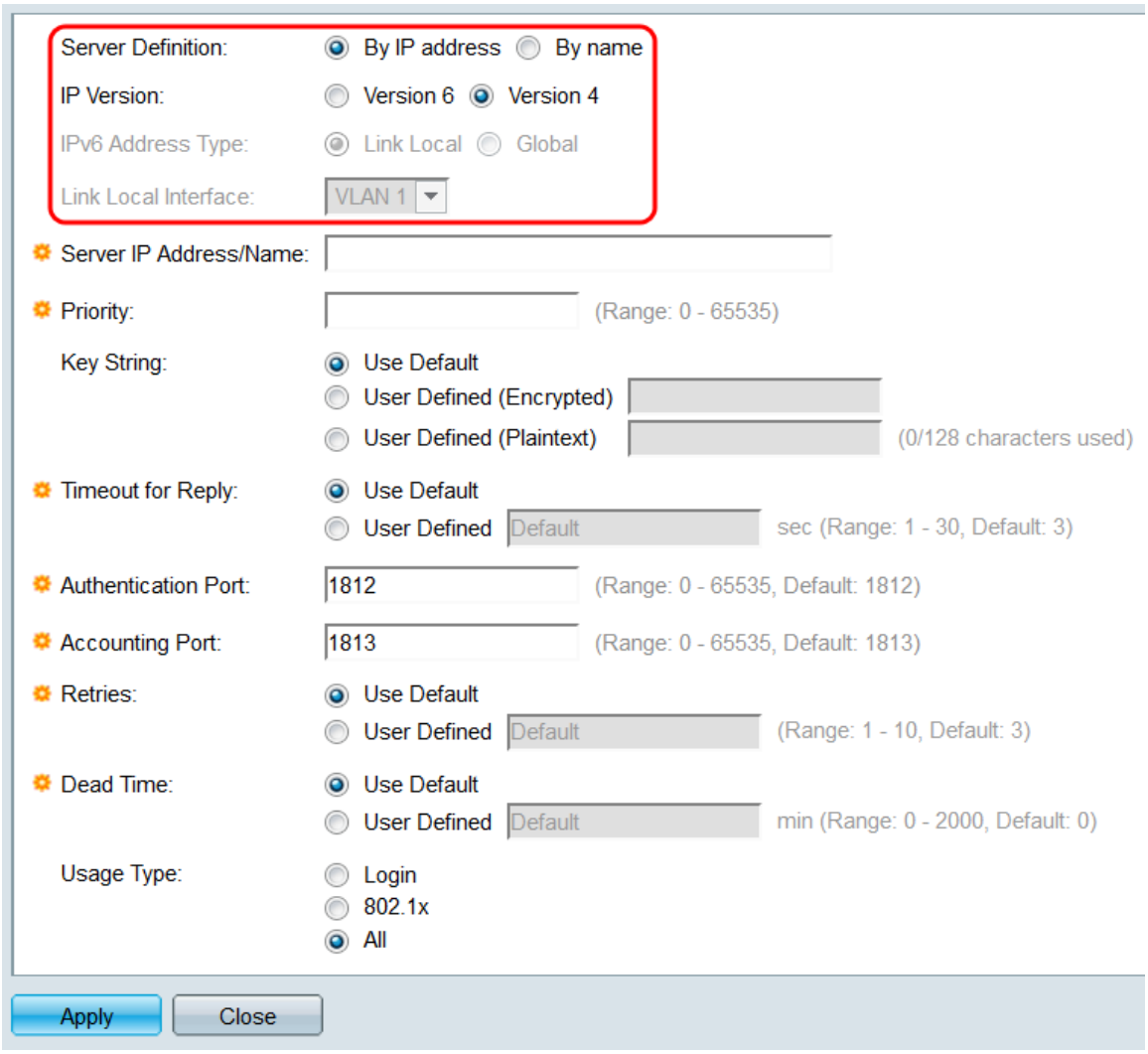
Schritt 4: Klicken Sie auf **Übernehmen**. Die Standardeinstellungen werden übernommen.



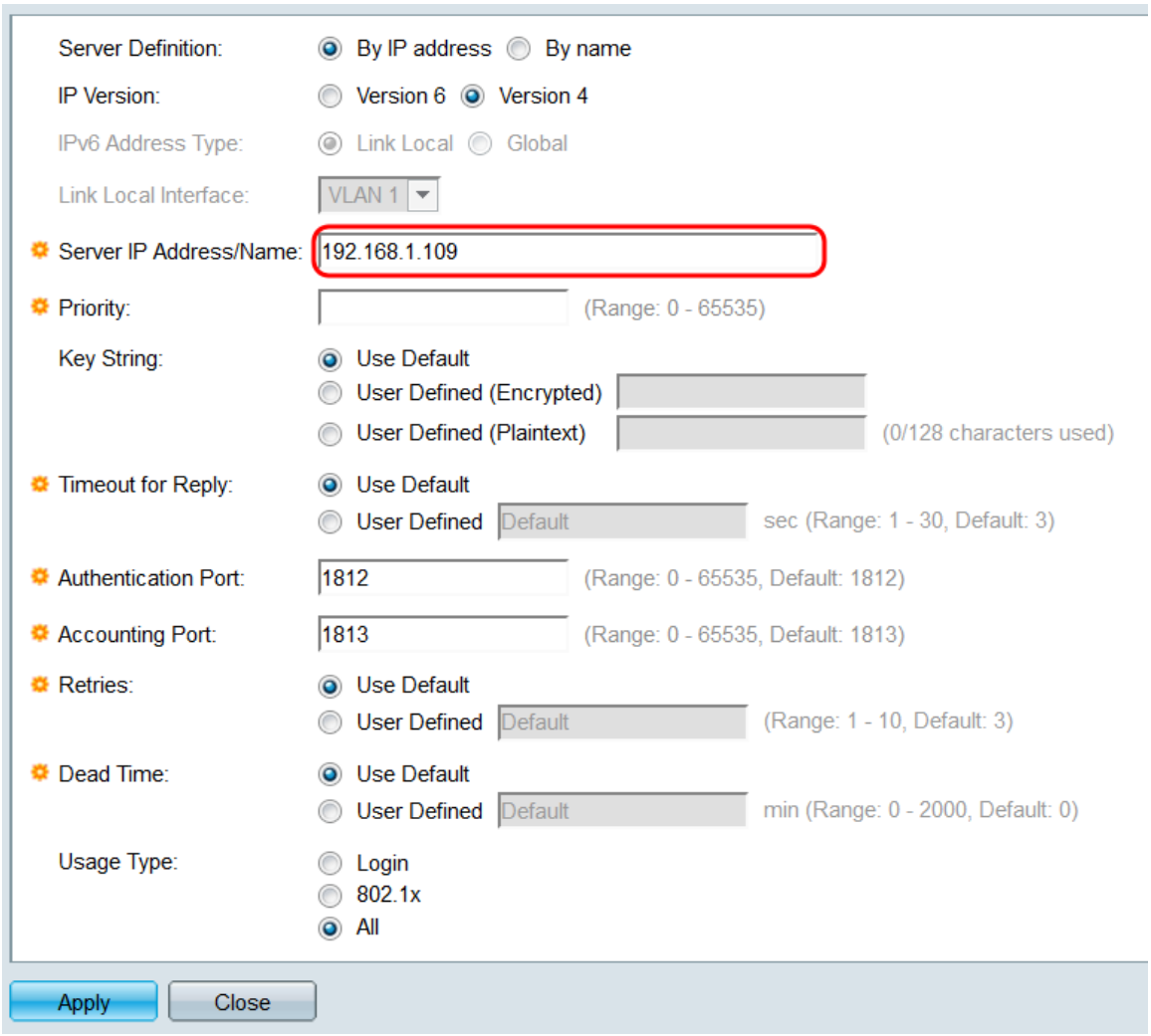
Schritt 5: Die *RADIUS-Tabelle* zeigt die aktuell auf dem Switch konfigurierten RADIUS-Servereinträge. Um einen neuen Eintrag hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen...**. Das Fenster *RADIUS-Server hinzufügen* wird geöffnet.



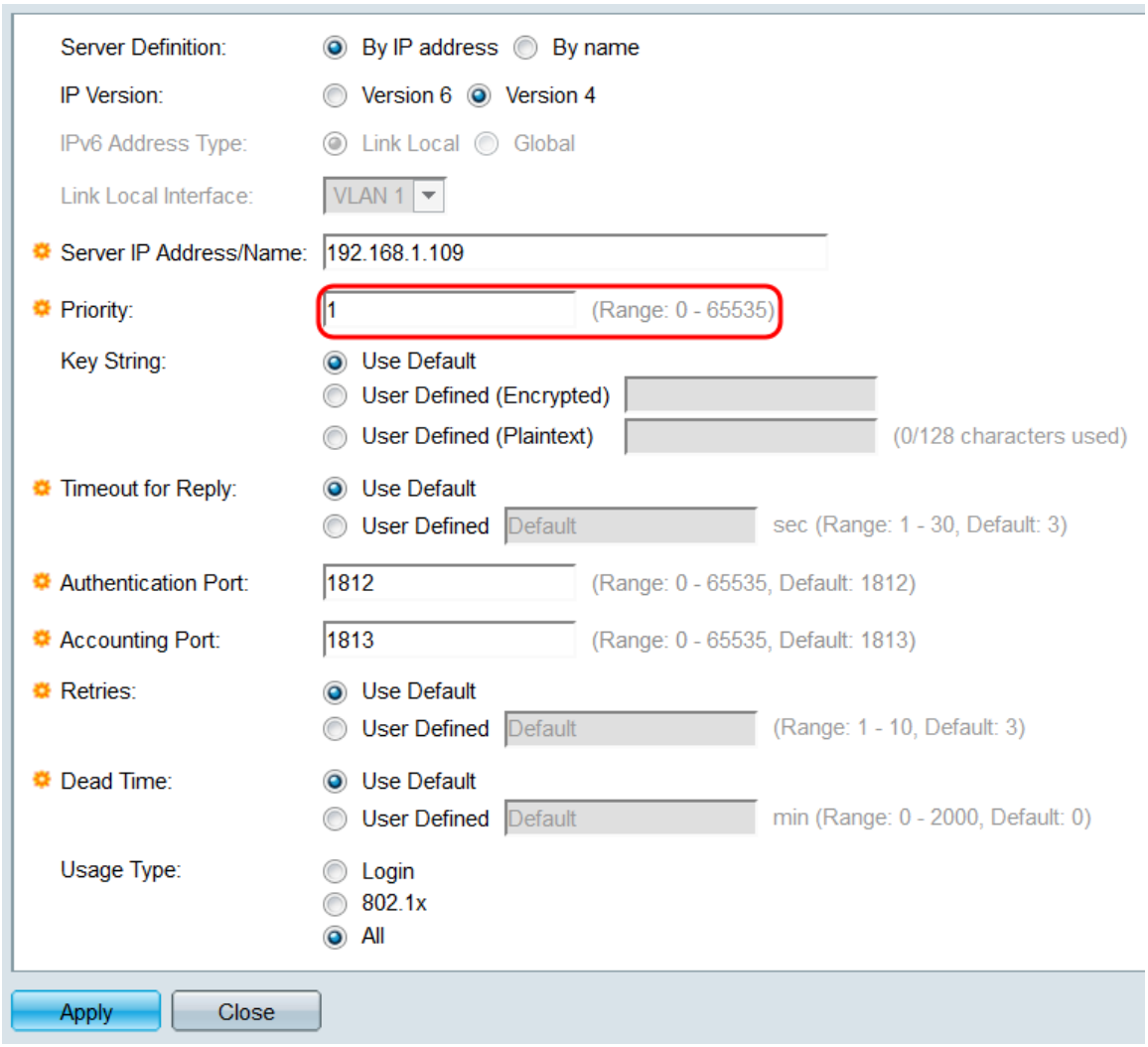
Schritt 6: Wählen Sie im Feld *"Serverdefinition"* aus, ob Sie den RADIUS-Server **nach IP-Adresse** oder **nach Name** (Hostname) kontaktieren möchten. Wenn Sie **Nach IP-Adresse** ausgewählt haben, wählen Sie entweder IPv6 (**Version 6**) oder IPv4 (**Version 4**) aus. Wenn Sie **Version 6** ausgewählt haben, geben Sie mithilfe des *IPv6-Adresstyps* und der *Link Local Interface* die verwendete IPv6-Adresse an.



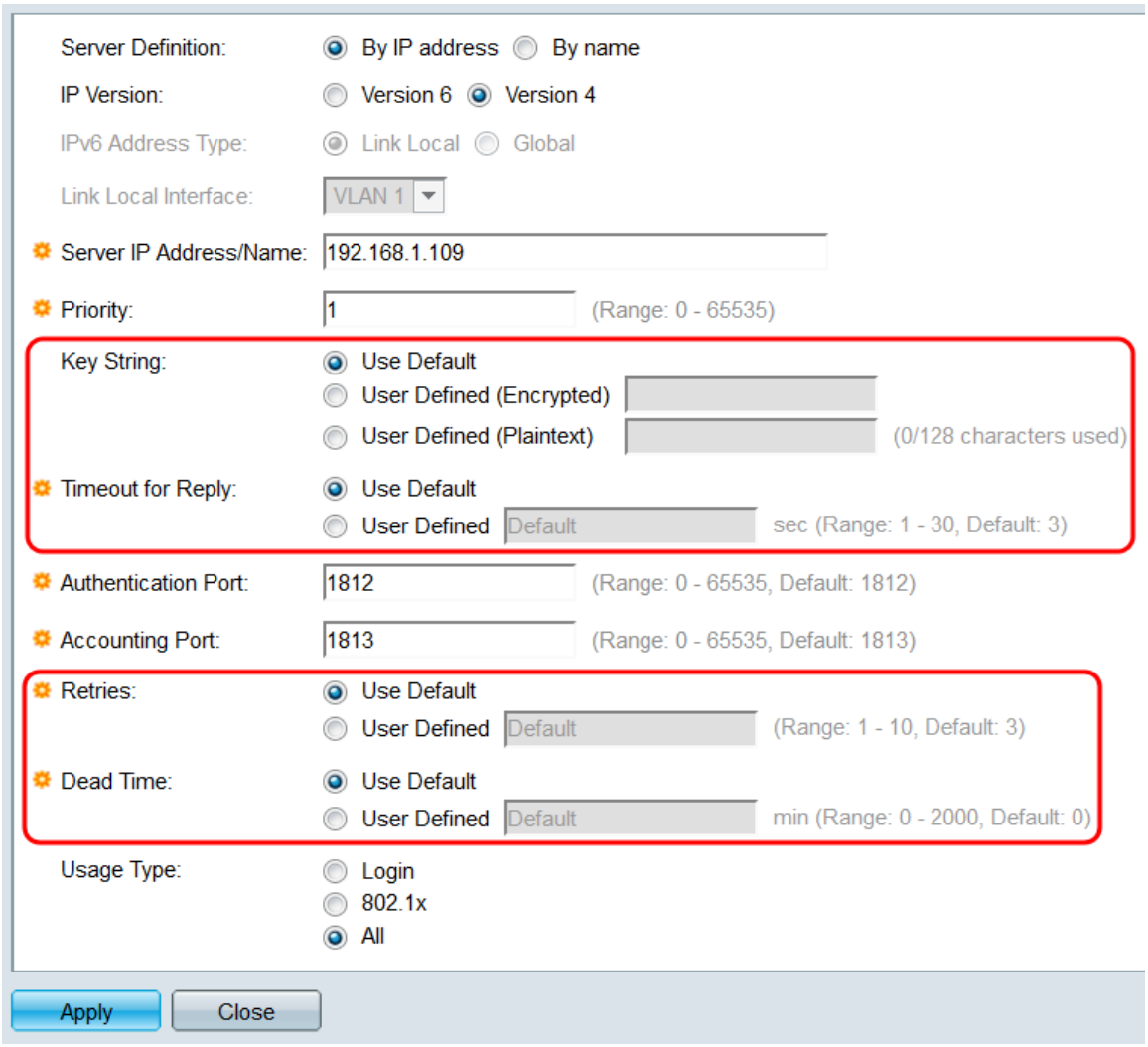
Schritt 7: Geben Sie im Feld *Server IP Address/Name (IP-Adresse/Name des Servers)* die IP-Adresse oder den Hostnamen des RADIUS-Servers ein.



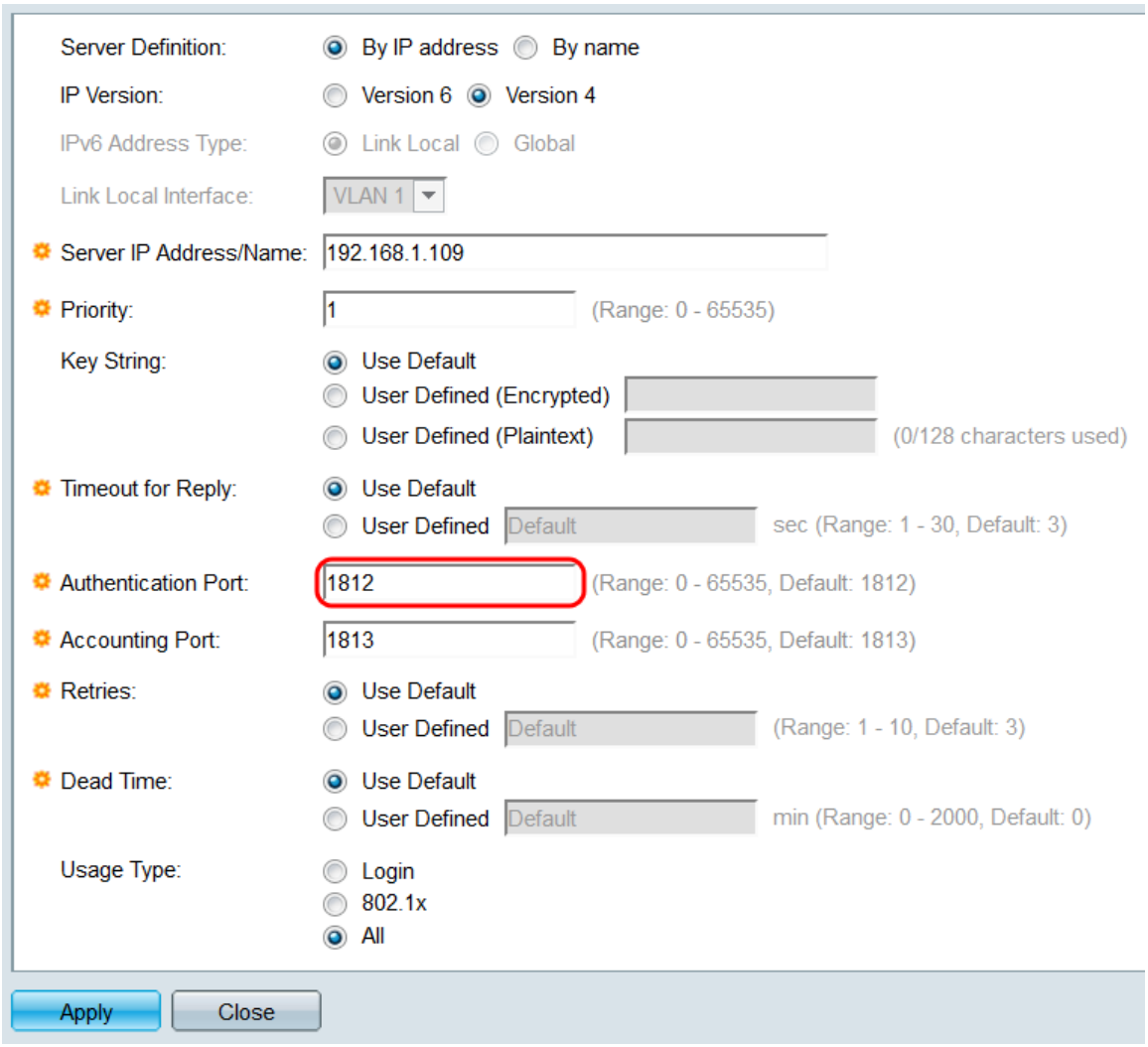
Schritt 8: Geben Sie im Feld *Priorität* die Priorität ein, die Sie diesem Server zuweisen möchten. Der Switch versucht, den Server mit der höchsten Priorität zu kontaktieren und setzt die Liste so lange fort, bis ein reaktionsschneller Server gefunden wird. Der Bereich liegt zwischen 0 und 65.535, wobei 0 die höchste Priorität darstellt.



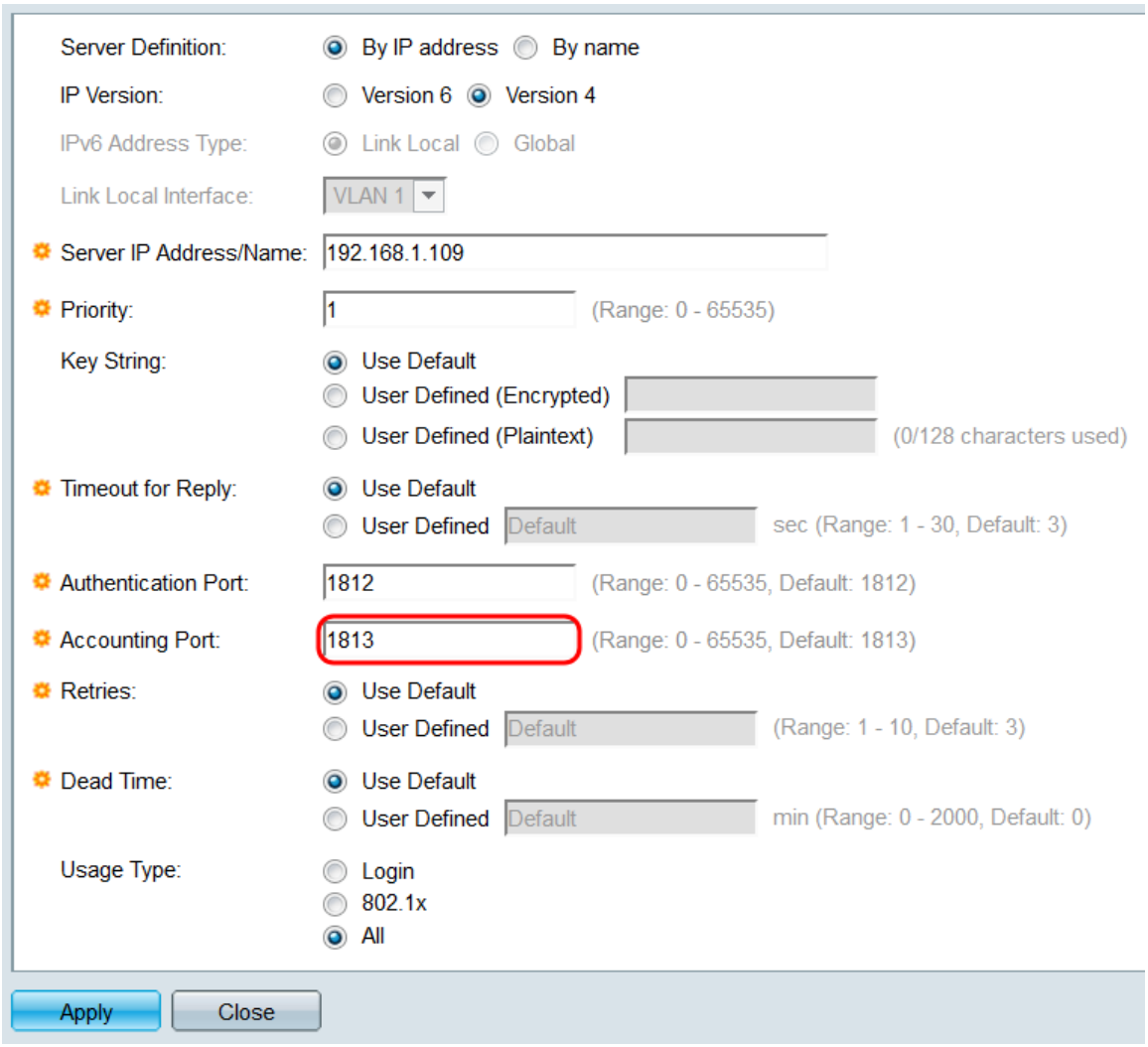
Schritt 9: Wählen Sie das Optionsfeld **Standard verwenden** in den *Feldern Schlüsselzeichenfolge*, *Zeitüberschreitung für Antworten*, *Wiederholungen* und *Verlustzeit, um die zuvor auf der RADIUS-Seite konfigurierten Einstellungen zu verwenden.* Sie können auch die Optionsfelder **Benutzerdefiniert** auswählen, um Einstellungen zu konfigurieren, die sich von den Standardeinstellungen unterscheiden. In diesem Fall werden diese Einstellungen nur für diesen spezifischen RADIUS-Server verwendet.



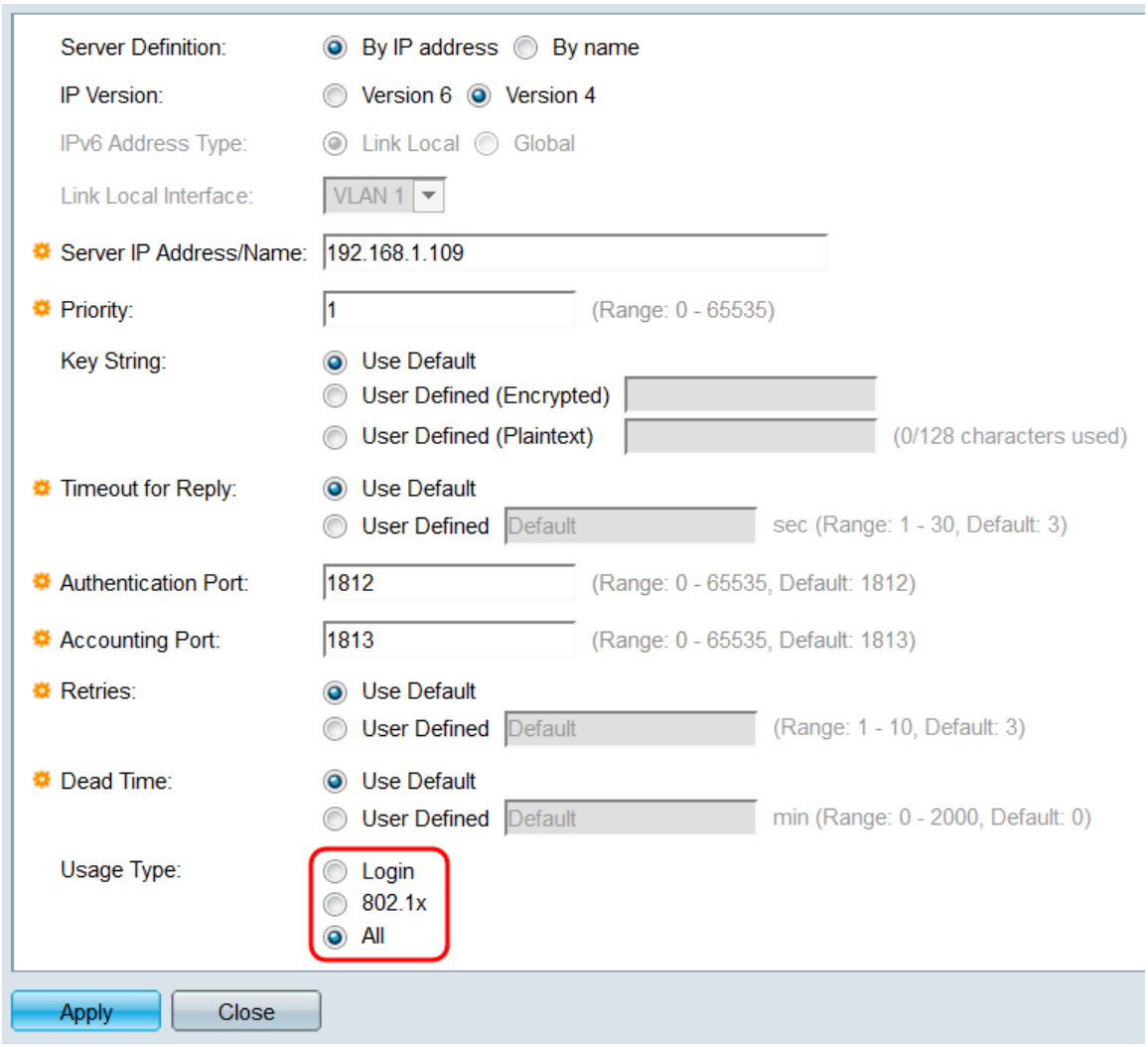
Schritt 10: Geben Sie im Feld *Authentication Port* (Authentifizierungsport) den Port an, der für die Authentifizierungskommunikation mit dem RADIUS-Server verwendet wird. Es wird empfohlen, dass dies auf dem Standardport 1812 belassen wird.



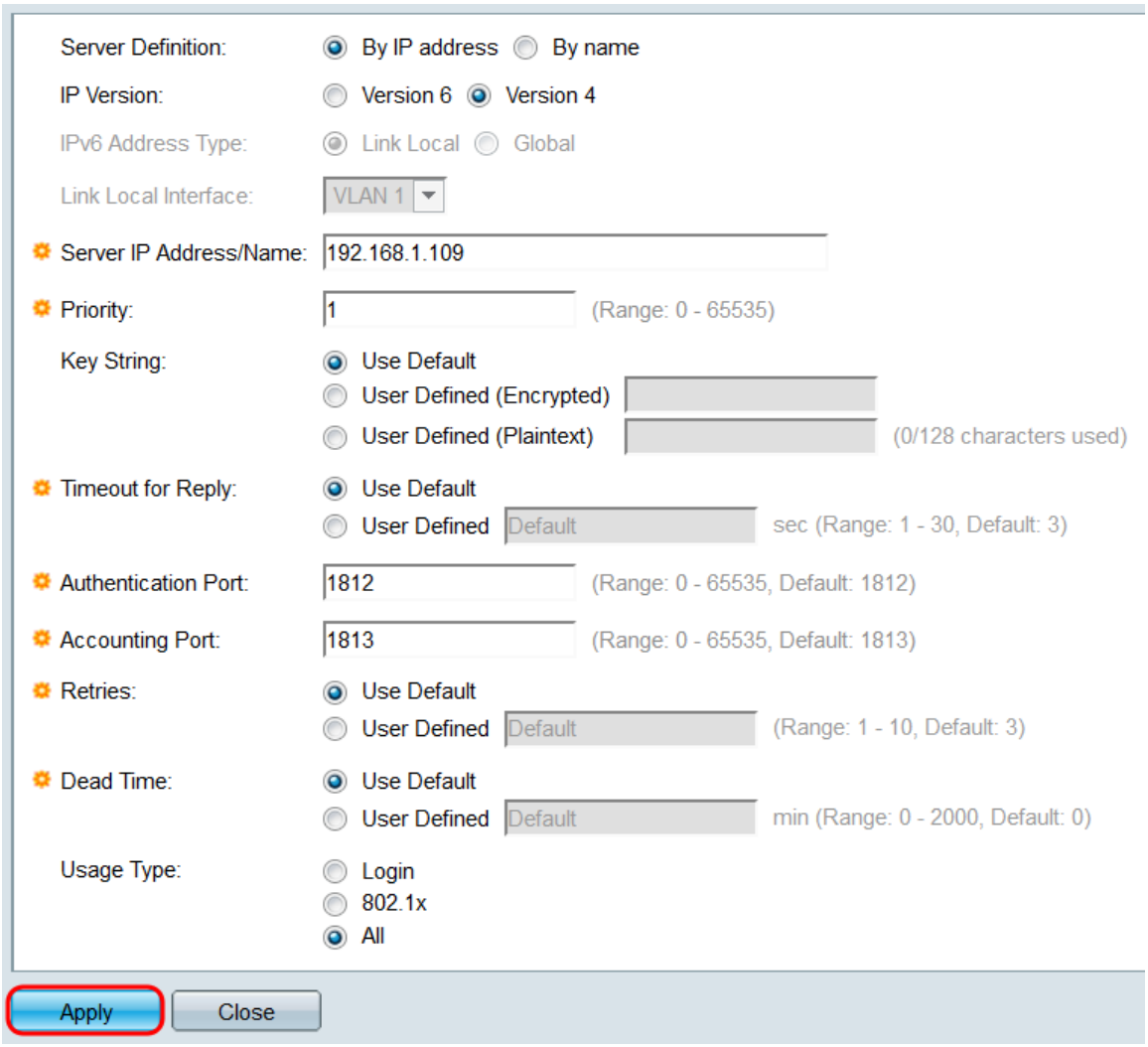
Schritt 11: Geben Sie im Feld *Buchhaltungsport* den Port an, der für die Accounting-Kommunikation mit dem RADIUS-Server verwendet wird. Es wird empfohlen, dass dieser auf dem Standardport 1813 belassen wird.



Schritt 12: Wählen Sie im Feld *Usage Type* (Nutzungstyp) aus, für welchen der RADIUS-Server verwendet werden soll. Wählen Sie bei der Konfiguration von 802.1X entweder die Optionsschaltflächen **802.1x** oder **All** aus, um den RADIUS-Server für die 802.1X-Portauthentifizierung zu verwenden.

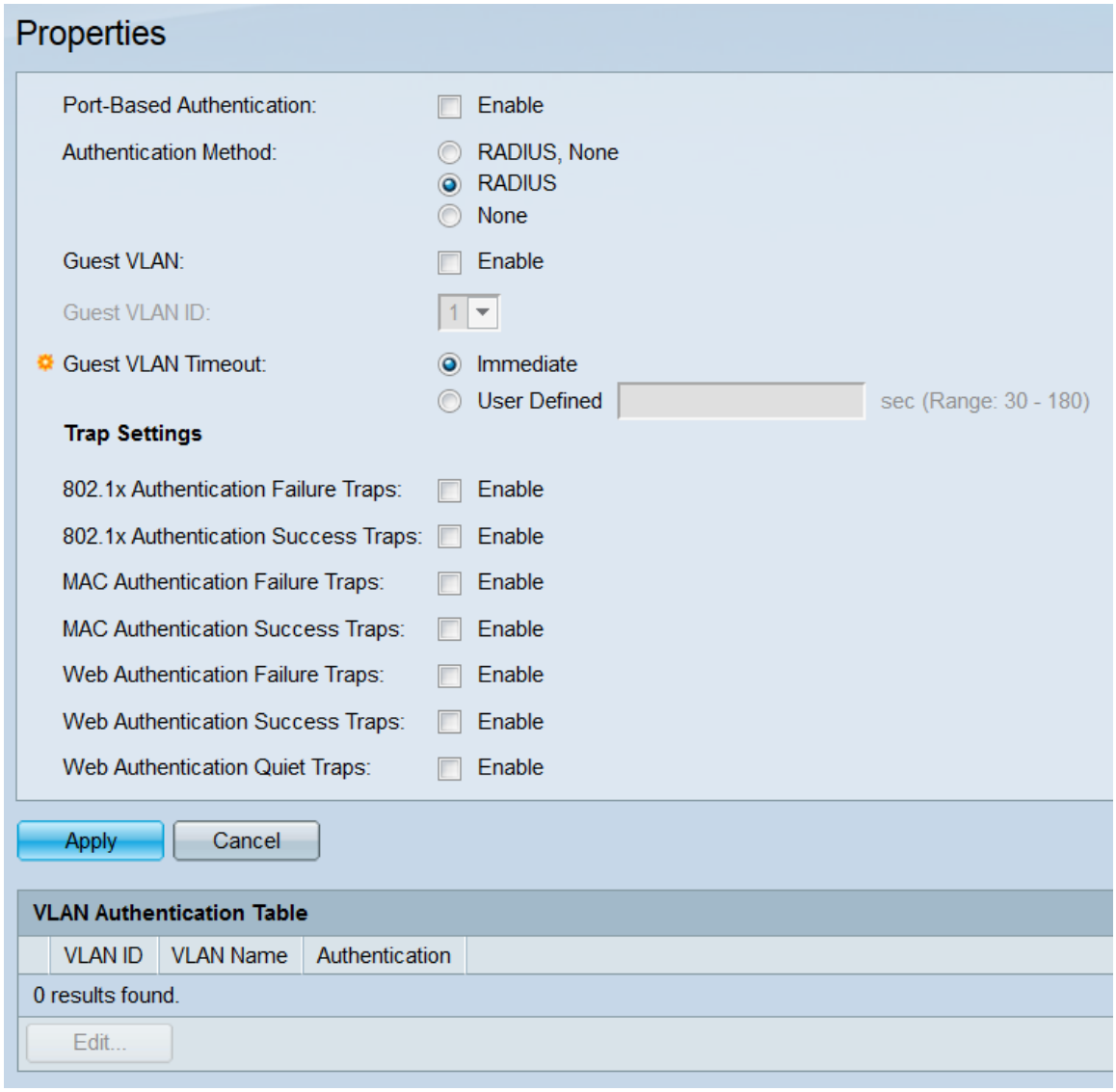


Schritt 13: Klicken Sie auf **Übernehmen**. Der Server wird der *RADIUS-Tabelle* hinzugefügt. Fahren Sie zum Aktivieren der portbasierten 802.1X-Authentifizierung mit dem nächsten Abschnitt fort.

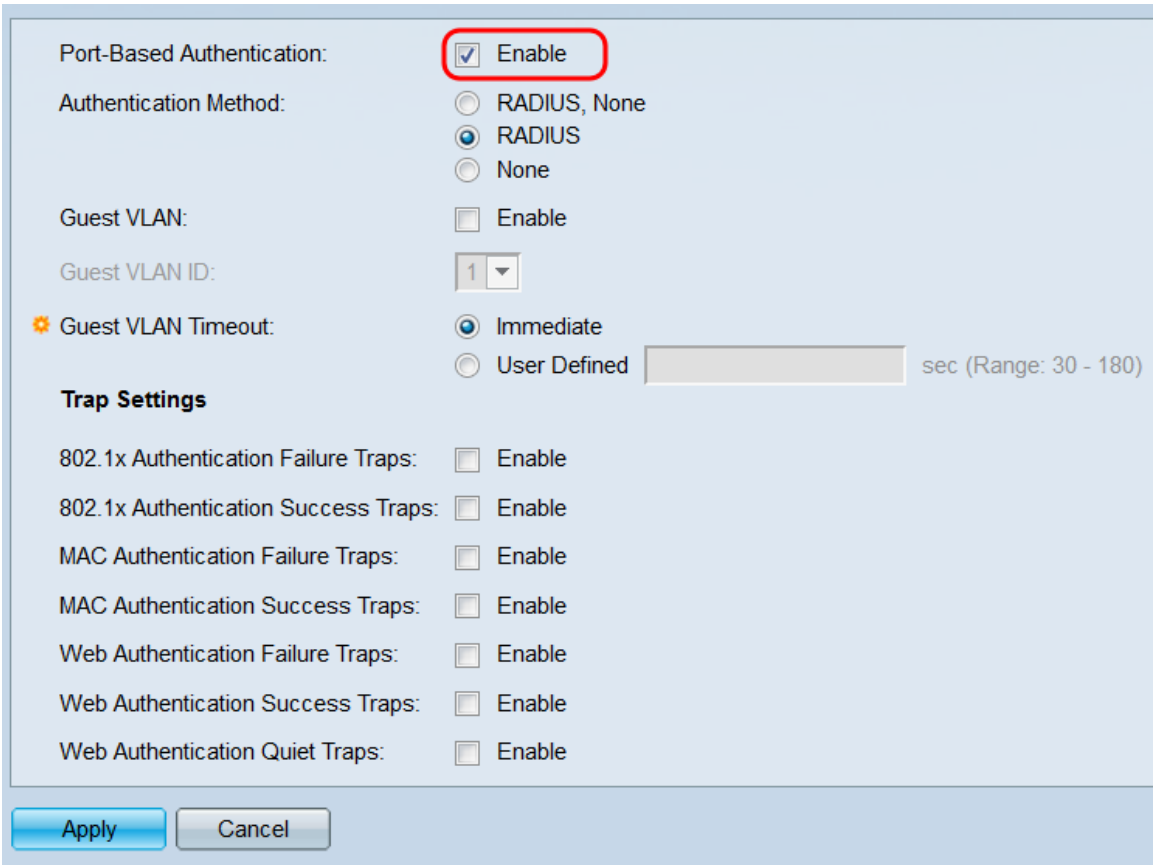


Aktivieren der Port-basierten Authentifizierung

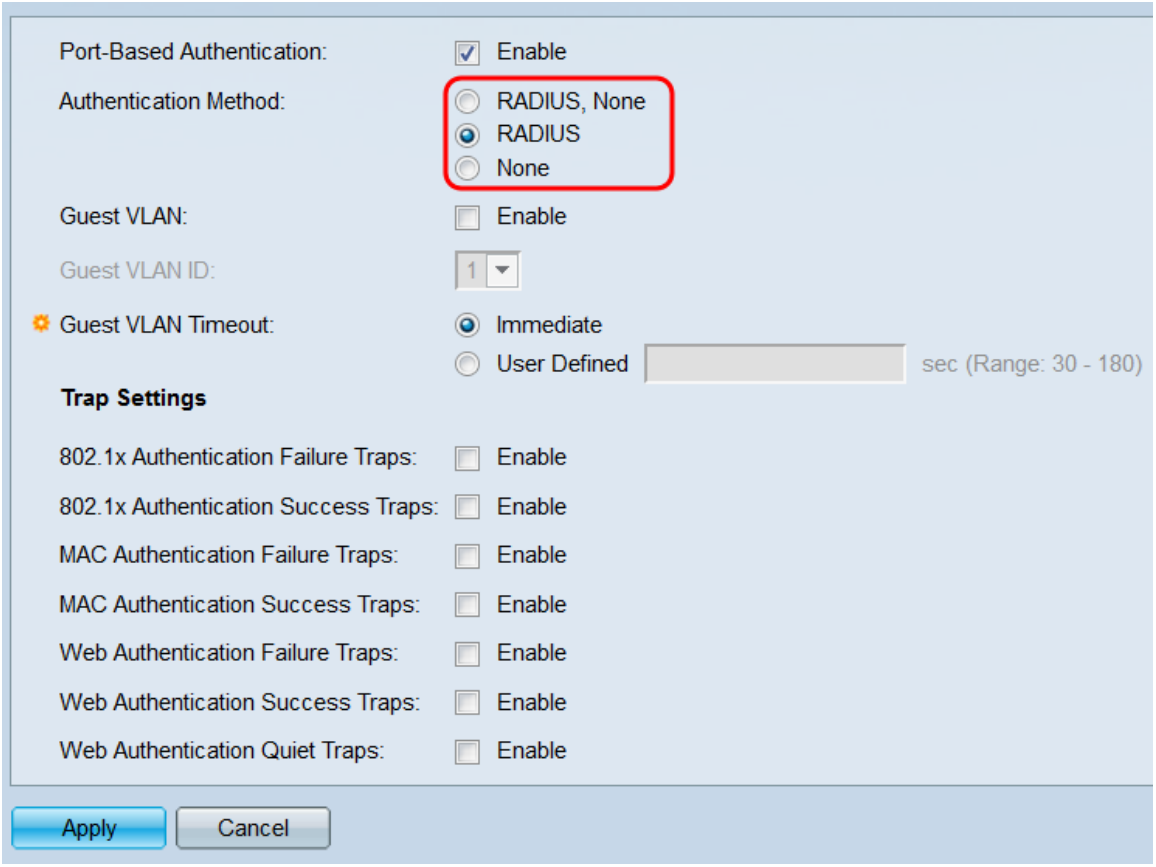
Schritt 1: Gehen Sie im Webkonfigurationsprogramm zu **Security > 802.1X/MAC/Web Authentication > Properties**. Die Seite *Eigenschaften* wird geöffnet.



Schritt 2: Aktivieren Sie im Feld *Port-Based Authentication* das **Kontrollkästchen Enable (Aktivieren)**, um die Port-basierte Authentifizierung zu aktivieren. Dies ist standardmäßig aktiviert.



Schritt 3: Wählen Sie im Feld *Authentication Method* (Authentifizierungsmethode) ein Optionsfeld aus, um festzulegen, wie die Port-basierte Authentifizierung funktioniert.



Folgende Optionen stehen zur Verfügung:

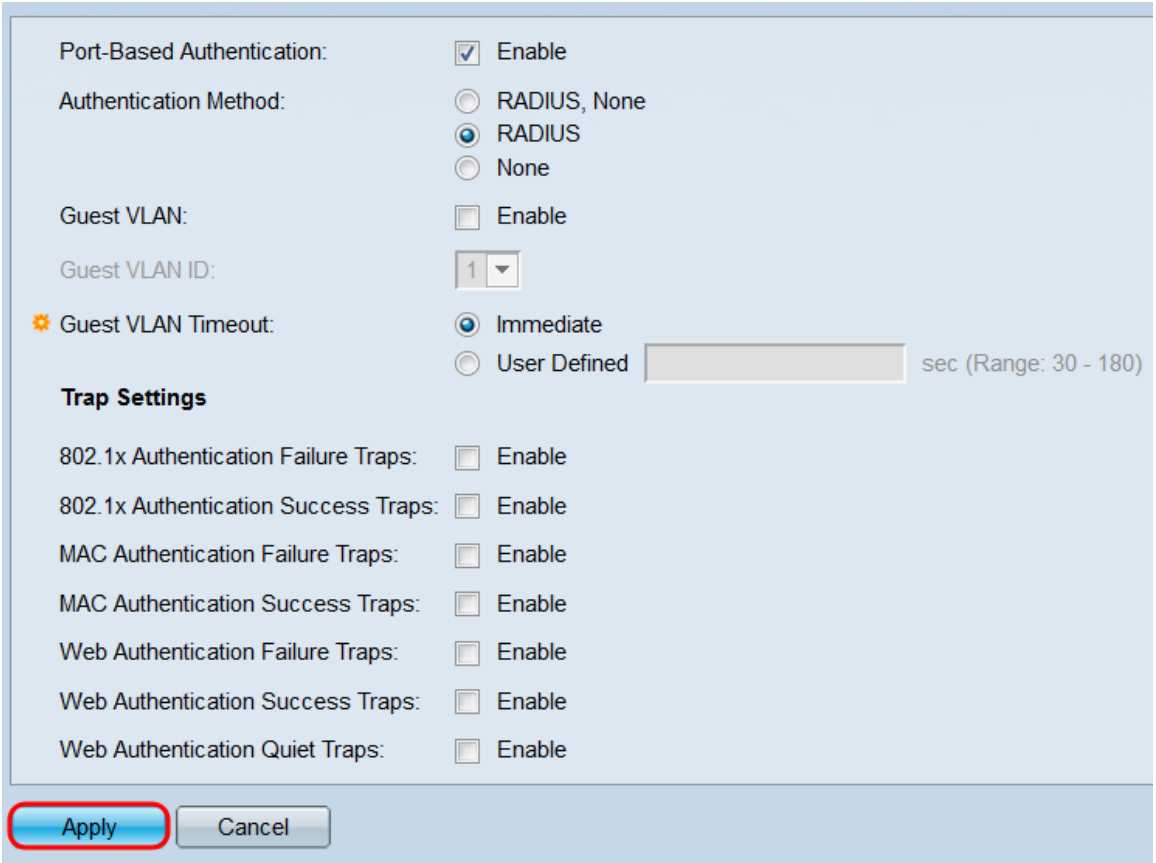
·RADIUS, None (RADIUS, Keine): Der Switch versucht, mit den auf der *RADIUS*-Seite definierten RADIUS-Servern Kontakt aufzunehmen. Wenn von den Servern keine Antwort

empfangen wird, wird keine Authentifizierung durchgeführt, und die Sitzung ist zulässig. Wenn der Server reagiert und die Anmeldeinformationen falsch sind, wird die Sitzung abgelehnt.

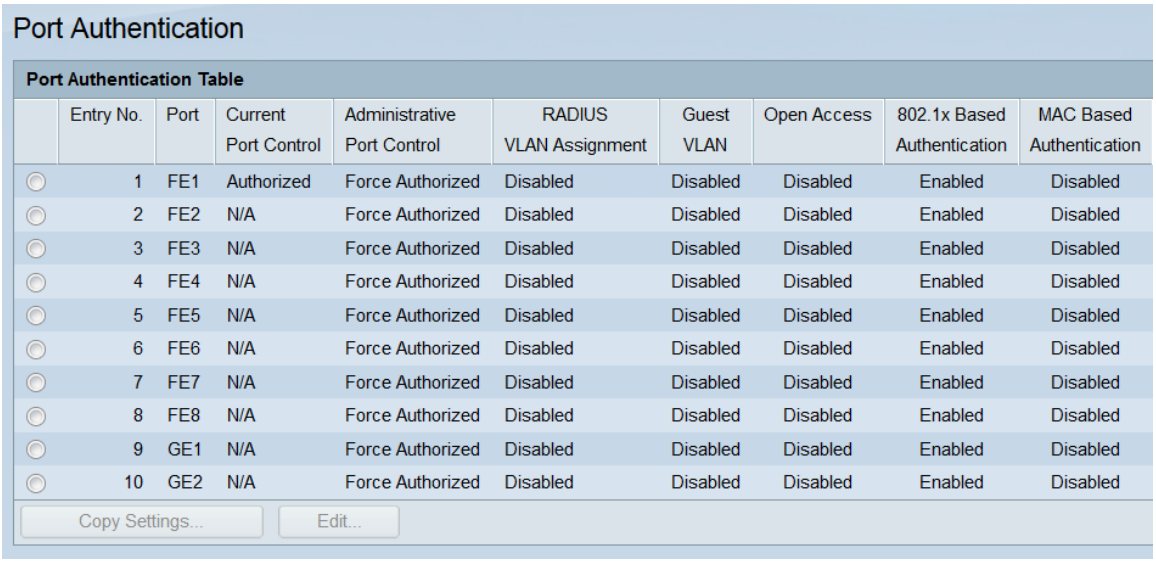
·RADIUS: Der Switch versucht, mit den auf der *RADIUS*-Seite definierten RADIUS-Servern Kontakt aufzunehmen. Wenn keine Antwort von den Servern eingeht, wird die Sitzung abgelehnt. Für die sicherste 802.1X-Implementierung wird diese Option empfohlen.

·Keine: Es wird keine Authentifizierung durchgeführt. Alle Sitzungen sind zulässig. 802.1X wird durch diese Option nicht implementiert.

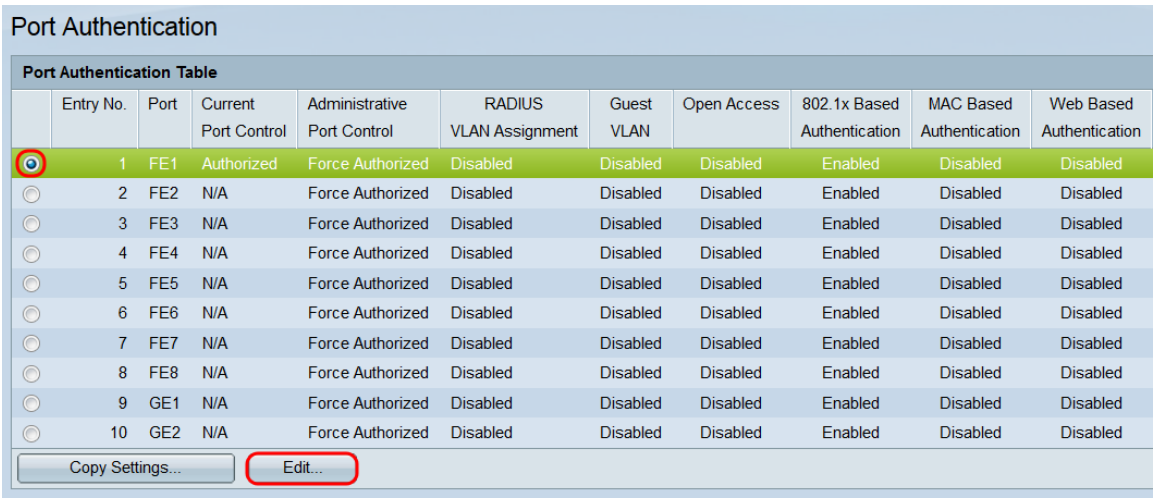
Schritt 4: Klicken Sie auf **Übernehmen**.



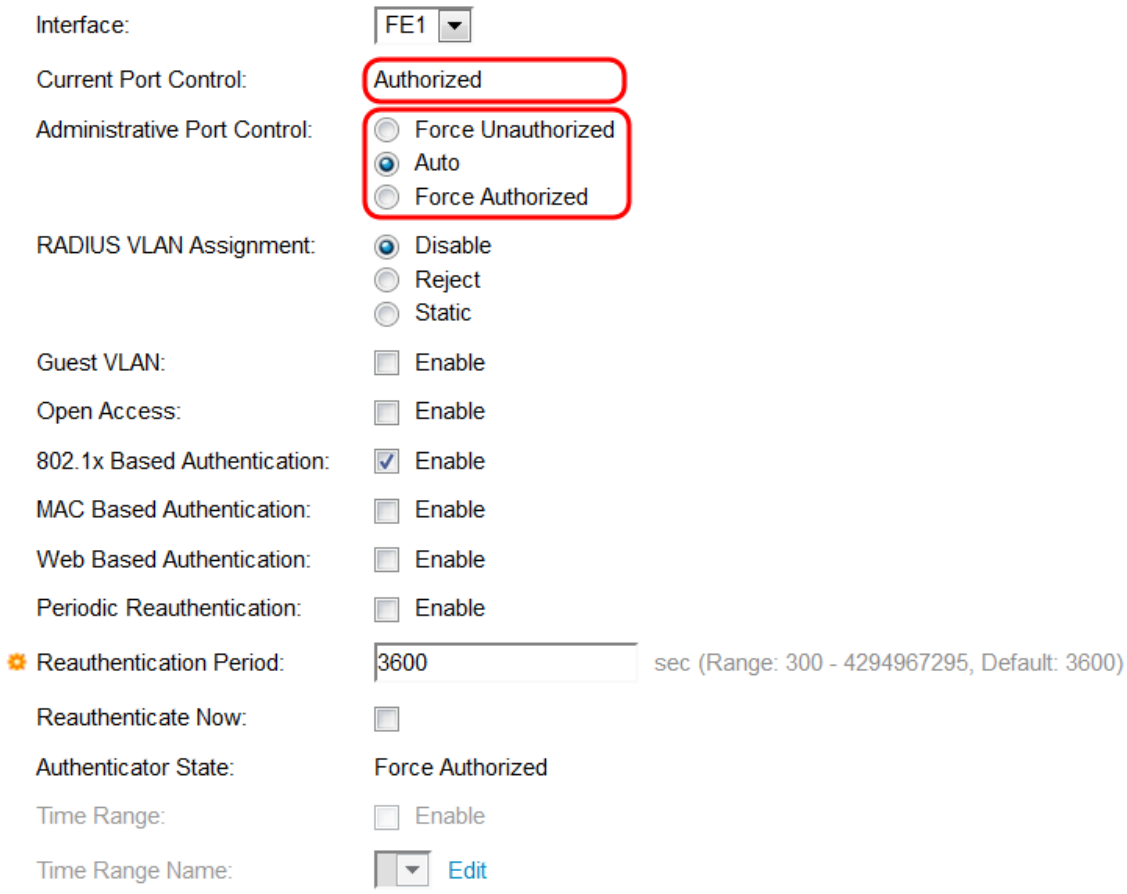
Schritt 5: Navigieren Sie zu **Sicherheit > 802.1X/MAC/Web Authentication > Port Authentication**. Die Seite *"Port Authentication*" wird geöffnet.



Schritt 6: Wählen Sie den zu konfigurierenden Port aus, indem Sie dessen Optionsfeld in der *Port Authentication Table* (*Port-Authentifizierungstabelle)* auswählen und auf die Schaltfläche **Edit..** klicken. Das Fenster *Edit Port Authentication* (Portauthentifizierung bearbeiten) wird geöffnet.



Schritt 7: Wählen Sie im Feld *Administrative Port Control* (*Administrative Port Control*) ein Optionsfeld aus, um festzulegen, wie der Port Sitzungen autorisieren soll. Das Feld *Aktuelle Portsteuerung* zeigt den aktuellen Autorisierungsstatus des ausgewählten Ports an.



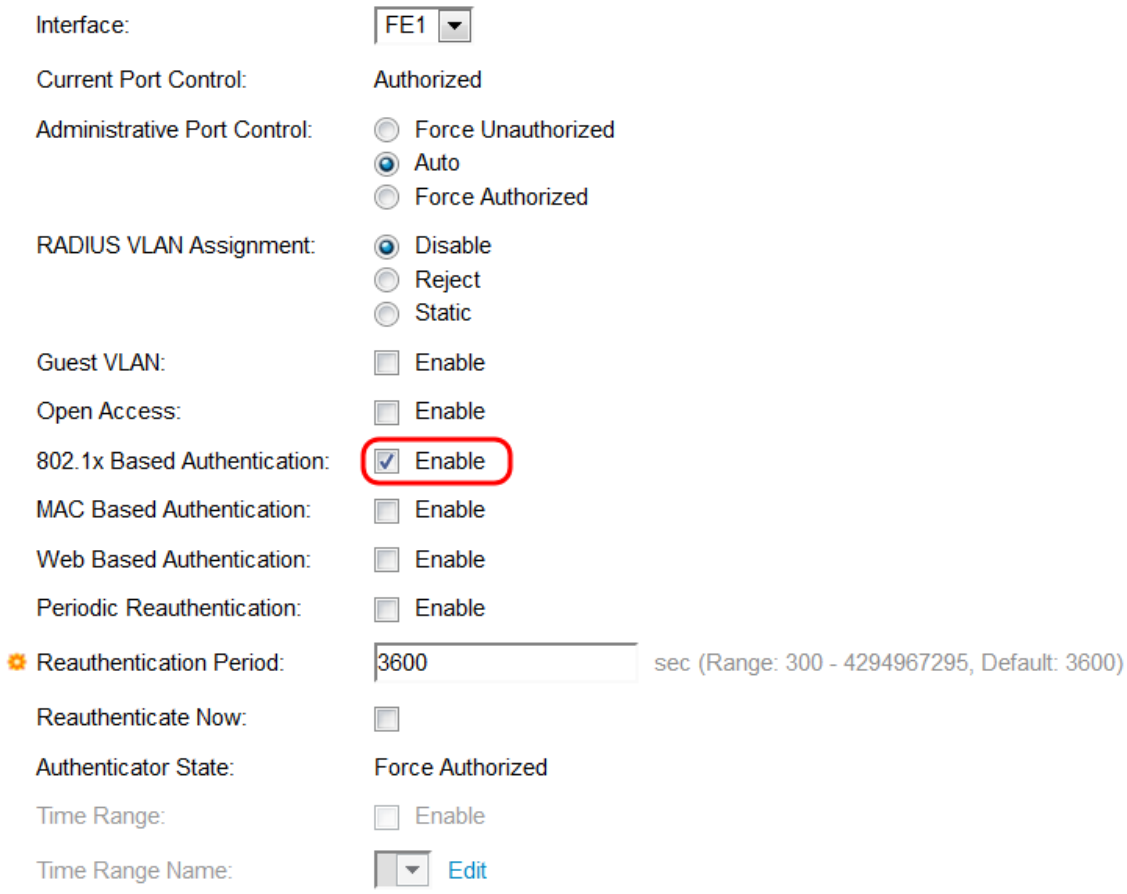
Folgende Optionen stehen zur Verfügung:

·Unauthorized erzwingen - Verschiebt die Schnittstelle in einen nicht autorisierten Zustand. Das Gerät stellt keine Authentifizierung für Clients bereit, die mit diesem Port verbunden sind, und verweigert den Zugriff.

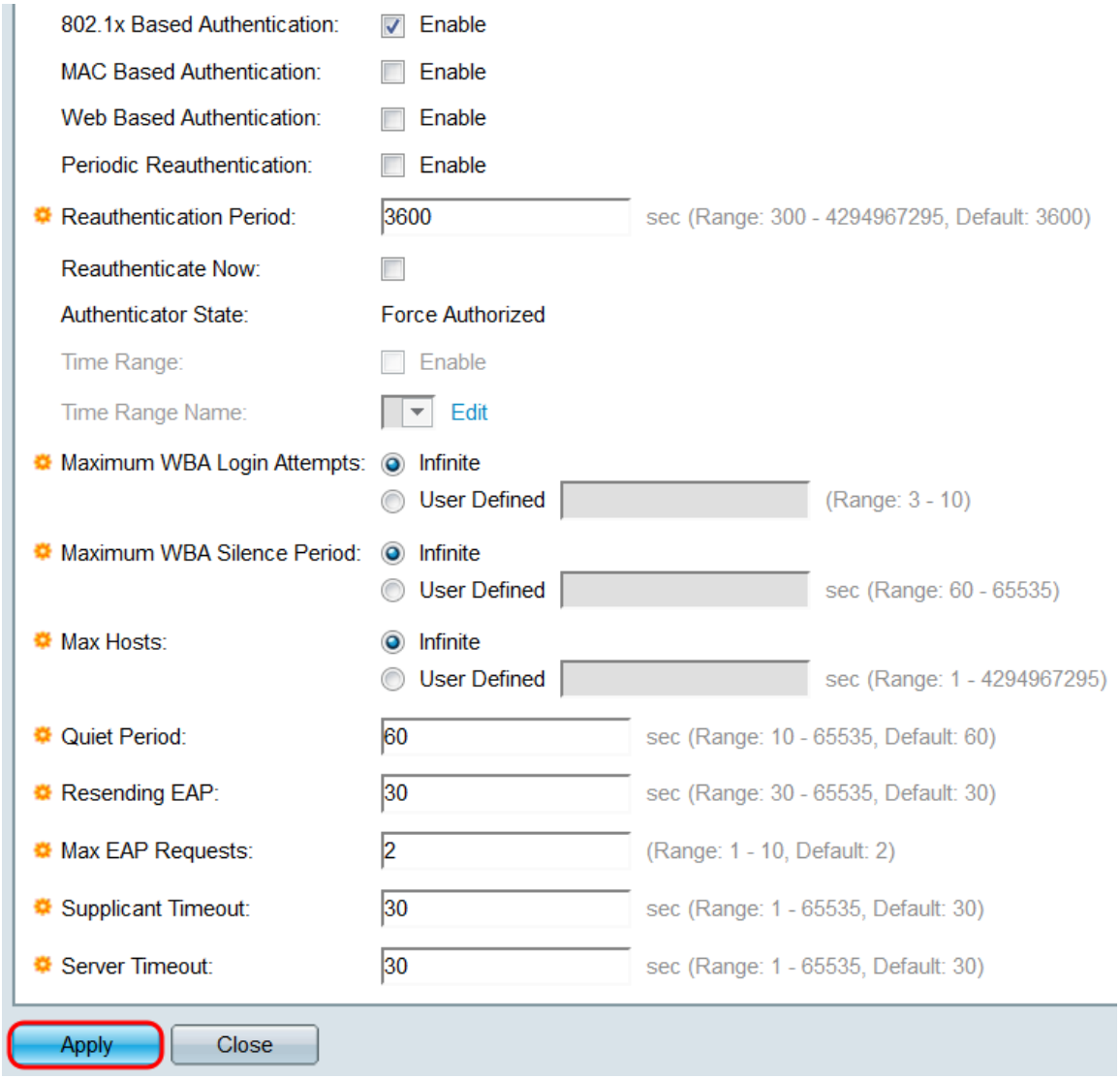
·Auto (Automatisch): Aktiviert die Port-basierte Authentifizierung für den ausgewählten Port. Verschiebt die Schnittstelle zwischen autorisiert und nicht autorisiert, abhängig vom Ergebnis des Authentifizierungsverfahrens. Wählen Sie diese Option aus, um 802.1X zu implementieren.

·Force Authorized (Autorisiert erzwingen) - Verschiebt die Schnittstelle in einen autorisierten Zustand. Das Gerät ermöglicht den Zugriff auf jeden Client, der ohne Authentifizierung mit diesem Port verbunden ist.

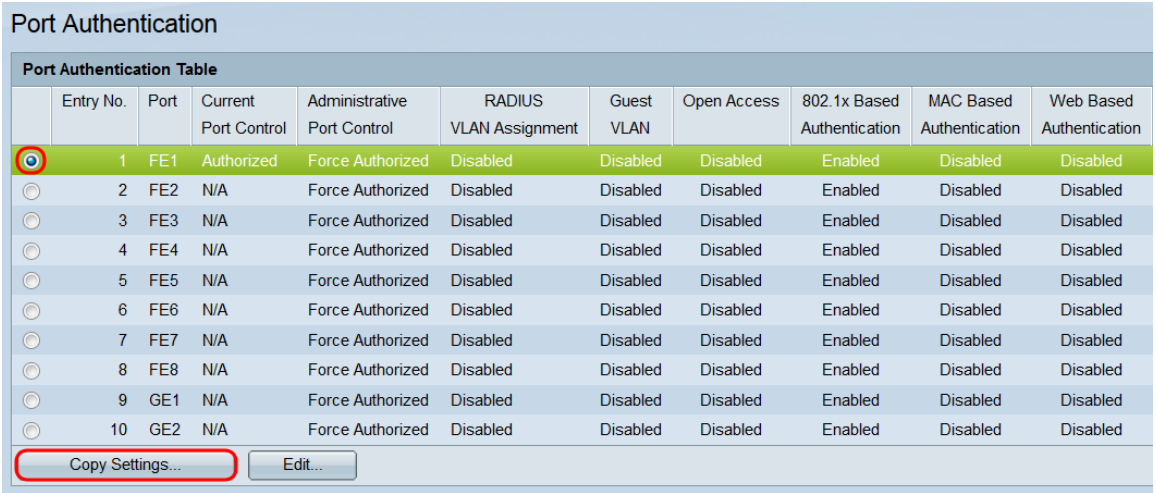
Schritt 8: Aktivieren Sie das **Kontrollkästchen Aktivieren** im Feld *802.1X Based Authentication*, um die 802.1X-Authentifizierung für den ausgewählten Port zu aktivieren.



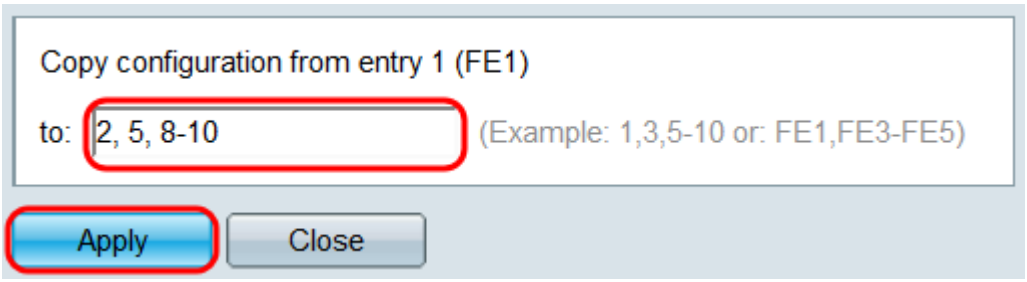
Schritt 9: Klicken Sie auf **Übernehmen**. Der Port sollte nun vollständig für die Port-basierte 802.1X-Authentifizierung konfiguriert sein und ist bereit, die Authentifizierung aller Clients zu starten, die mit ihm verbunden sind. Wählen Sie im Feld *Schnittstelle* einen anderen zu konfigurierenden Port aus, ohne zur Seite *Portauthentifizierung* zurückzukehren.



Schritt 10: Wenn Sie die Einstellungen eines Ports schnell in einen anderen Port oder Port-Bereich kopieren möchten, klicken Sie in der *Port Authentication Table* auf das Optionsfeld des Ports, den Sie kopieren möchten, und klicken Sie auf die Schaltfläche **Copy Settings...**. Das Fenster *Kopiereinstellungen* wird geöffnet.



Schritt 11: Geben Sie im Textfeld den Port oder die Ports (getrennt durch Kommas) ein, in die Sie die Einstellungen kopieren möchten. Sie können auch einen Port-Bereich angeben. Klicken Sie anschließend auf **Apply**, um die Einstellungen zu kopieren.



Sehen Sie sich ein Video zu diesem Artikel an..

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