Konfigurieren der 802.1x-Port-Authentifizierungseinstellung auf einem Switch

Ziel

IEEE 802.1x ist ein Standard, der die Zugriffskontrolle zwischen Client und Server vereinfacht. Bevor einem Client Services über ein Local Area Network (LAN) oder einen Switch bereitgestellt werden können, muss der mit dem Switch-Port verbundene Client vom Authentifizierungsserver authentifiziert werden, der den Remote Authentication Dial-In User Service (RADIUS) ausführt.

Die 802.1x-Authentifizierung hindert nicht autorisierte Clients daran, über öffentlich zugängliche Ports eine Verbindung mit einem LAN herzustellen. Die 802.1x-Authentifizierung ist ein Client-Server-Modell. Bei diesem Modell haben Netzwerkgeräte die folgenden spezifischen Rollen:

Client oder Supplicant (Client oder Supplicant): Ein Client oder Supplicant ist ein Netzwerkgerät, das den Zugriff auf das LAN anfordert. Der Client ist mit einem Authentifizierer verbunden.

Authentifizierer - Ein Authentifizierer ist ein Netzwerkgerät, das Netzwerkdienste bereitstellt und mit dem die Supplicant Ports verbunden sind. Folgende Authentifizierungsmethoden werden unterstützt:

802.1x-basiert - Wird in allen Authentifizierungsmodi unterstützt. Bei der 802.1x-basierten Authentifizierung extrahiert der Authentifizierer die EAP-Nachrichten (Extensible Authentication Protocol) aus den 802.1x-Nachrichten oder EAP over LAN (EAPoL)-Paketen und leitet sie mithilfe des RADIUS-Protokolls an den Authentifizierungsserver weiter.

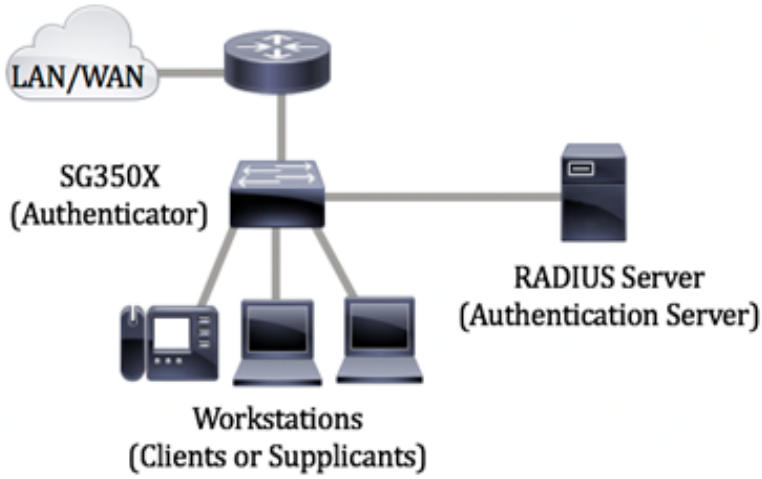
MAC-basiert - Wird in allen Authentifizierungsmodi unterstützt. Bei MAC-basierter (Media Access Control) Ausführung des EAP-Client-Teils der Software durch den Authentifizierer selbst im Auftrag der Clients, die Netzwerkzugriff anfordern.

Webbasiert - Wird nur in Multisitzungsmodi unterstützt. Bei webbasierter Authentifizierung führt der Authentifizierer selbst den EAP-Client-Teil der Software für die Clients aus, die Netzwerkzugriff anfordern.

Authentifizierungsserver - Ein Authentifizierungsserver führt die eigentliche Authentifizierung des Clients durch. Der Authentifizierungsserver für das Gerät ist ein RADIUS-Authentifizierungsserver mit EAP-Erweiterungen.

Hinweis: Ein Netzwerkgerät kann entweder Client oder Komponente, Authentifizierer oder beide pro Port sein.

Das nachfolgende Bild zeigt ein Netzwerk, das die Geräte entsprechend den spezifischen Rollen konfiguriert hat. In diesem Beispiel wird ein SG350X-Switch verwendet.



Richtlinien für die Konfiguration von 802.1x:

Erstellen Sie ein Virtual Access Network (VLAN). Klicken Sie hier, um VLANs mithilfe des webbasierten Dienstprogramms Ihres Switches zu erstellen. CLI-basierte Anweisungen erhalten Sie hier.

Konfigurieren der Port-VLAN-Einstellungen auf dem Switch Klicken Sie hier, um das webbasierte Dienstprogramm zu konfigurieren. Klicken Sie hier, um die CLI zu verwenden.

Konfigurieren Sie 802.1x-Eigenschaften auf dem Switch. 802.1x sollte auf dem Switch global aktiviert sein, um die Port-basierte 802.1x-Authentifizierung zu aktivieren. Anweisungen hierzu erhalten Sie hier.

(Optional) Konfigurieren Sie den Zeitbereich auf dem Switch. Um zu erfahren, wie Sie die Zeitbereichseinstellungen auf Ihrem Switch konfigurieren, klicken Sie hier.

802.1x-Port-Authentifizierung konfigurieren Dieser Artikel enthält Anweisungen zum Konfigurieren der Einstellungen für die 802.1x-Portauthentifizierung auf Ihrem Switch.

Um zu erfahren, wie Sie die MAC-basierte Authentifizierung auf einem Switch konfigurieren, klicken Sie hier.

Anwendbare Geräte

Serie Sx300

Serie Sx350

SG350X-Serie

Serie Sx500

Serie Sx550X

Softwareversion

1.4.7.06 — Sx300, Sx500

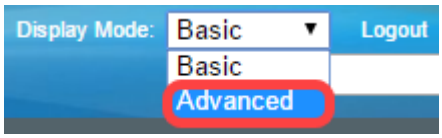
2.2.8.04 - Sx350, SG350X, Sx550X

Konfigurieren der 802.1x-Port-Authentifizierungseinstellungen auf einem Switch

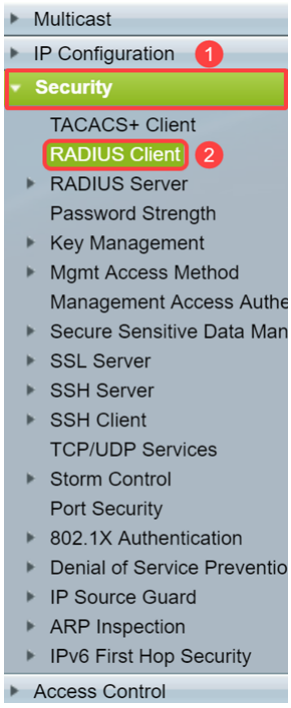
Konfigurieren der RADIUS-Client-Einstellungen

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

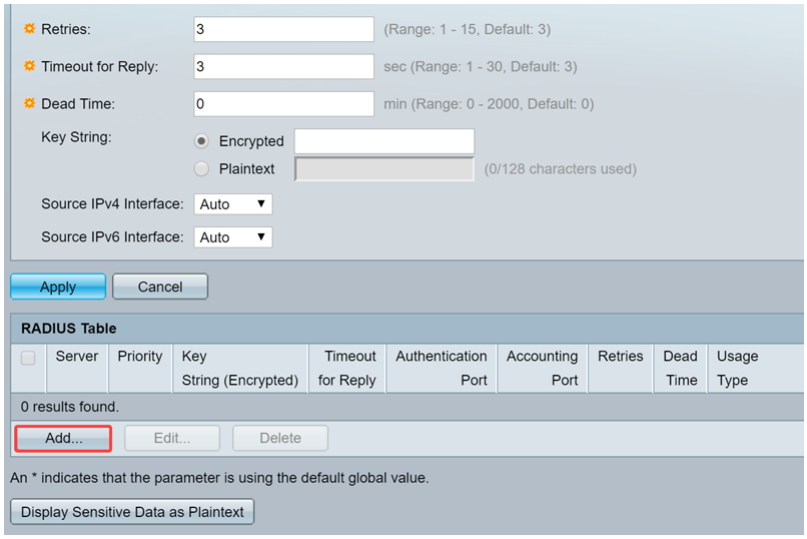
Hinweis: Die verfügbaren Menüoptionen können je nach Gerätemodell variieren. In diesem Beispiel wird SG550X-24 verwendet.



Schritt 2: Navigieren Sie zu **Security > RADIUS Client**.

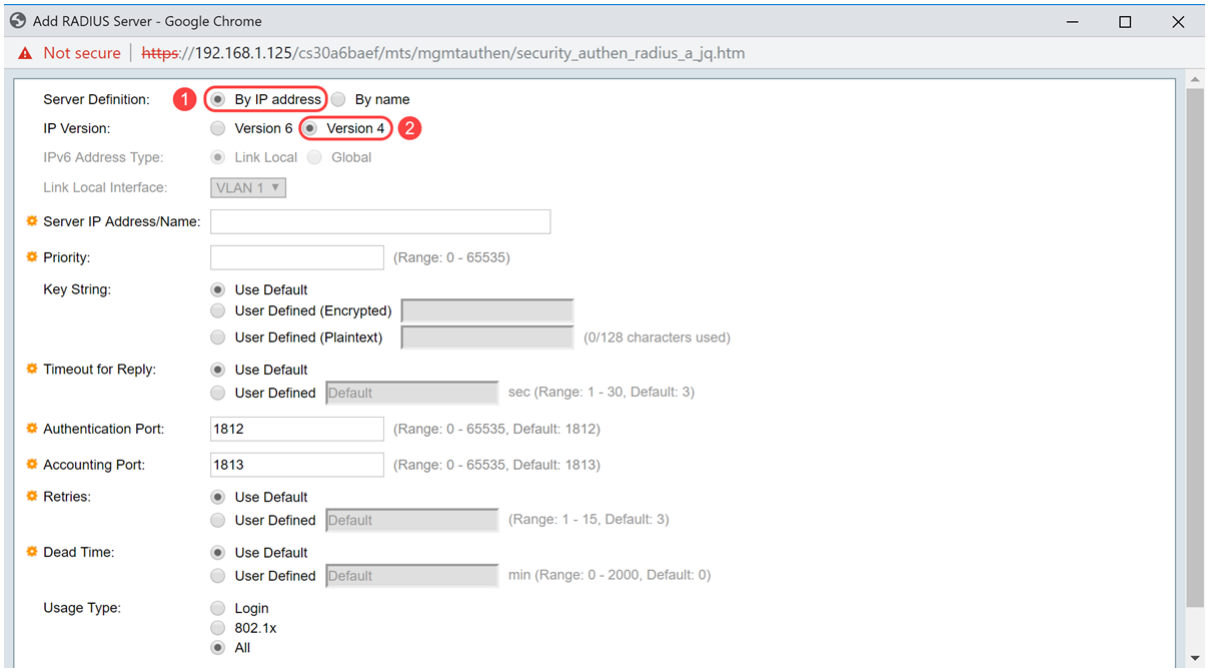


Schritt 3: Blättern Sie nach unten zum Abschnitt *RADIUS Table*, und klicken Sie auf **...**, um einen RADIUS-Server hinzuzufügen.



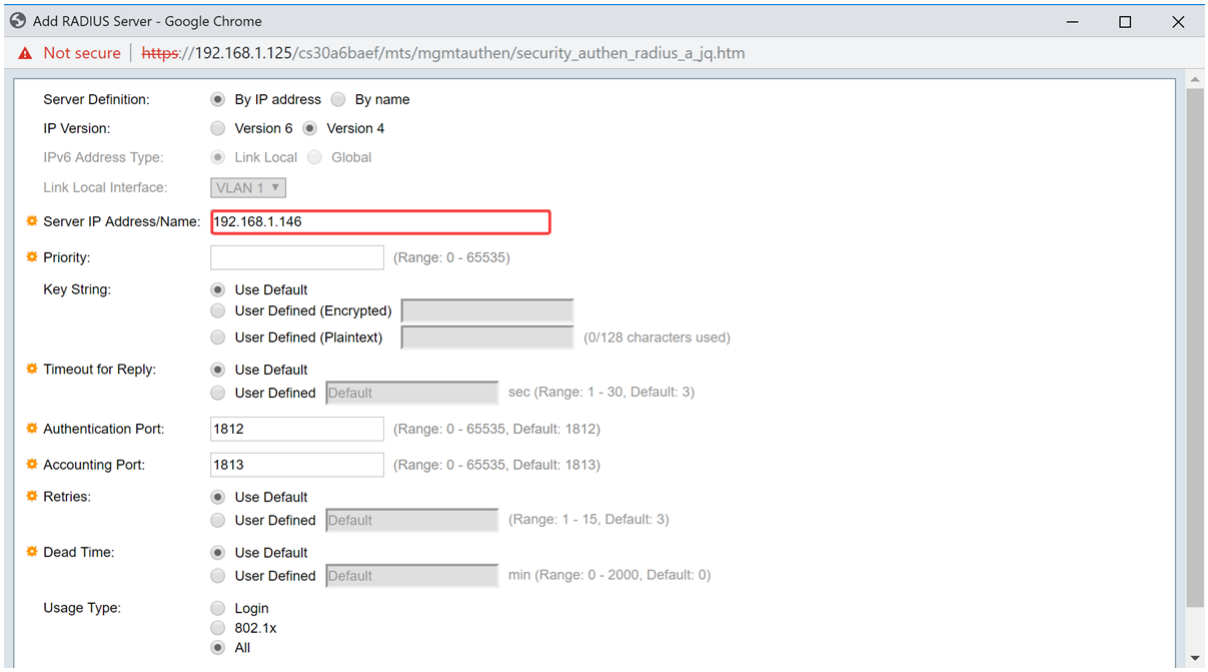
Schritt 4: Wählen Sie im Feld *Serverdefinition* aus, ob der RADIUS-Server nach IP-Adresse oder Name angegeben werden soll. Wählen Sie im Feld *IP-Version* die Version der IP-Adresse des RADIUS-Servers aus.

Hinweis: In diesem Beispiel werden die **By IP-Adresse** und **Version 4** verwendet.

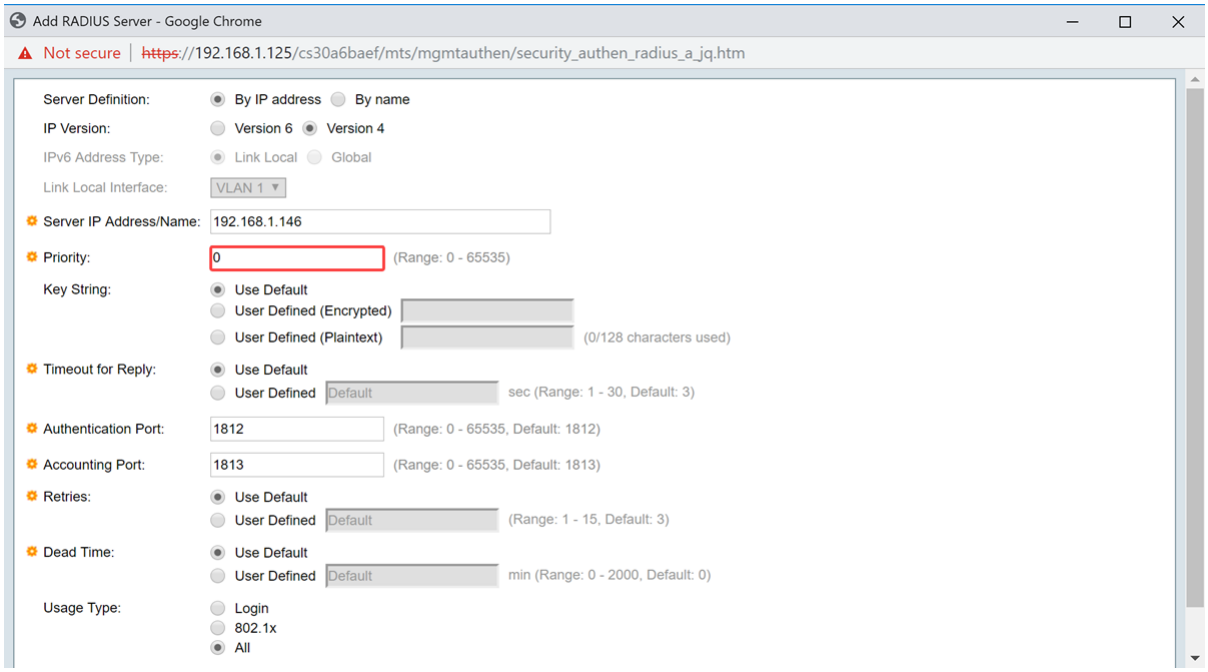


Schritt 5: Geben Sie im RADIUS-Server die IP-Adresse oder den Namen ein.

Hinweis: Wir geben die IP-Adresse **192.168.1.146** in das Feld *IP-Adresse/Name* des *Servers ein*.



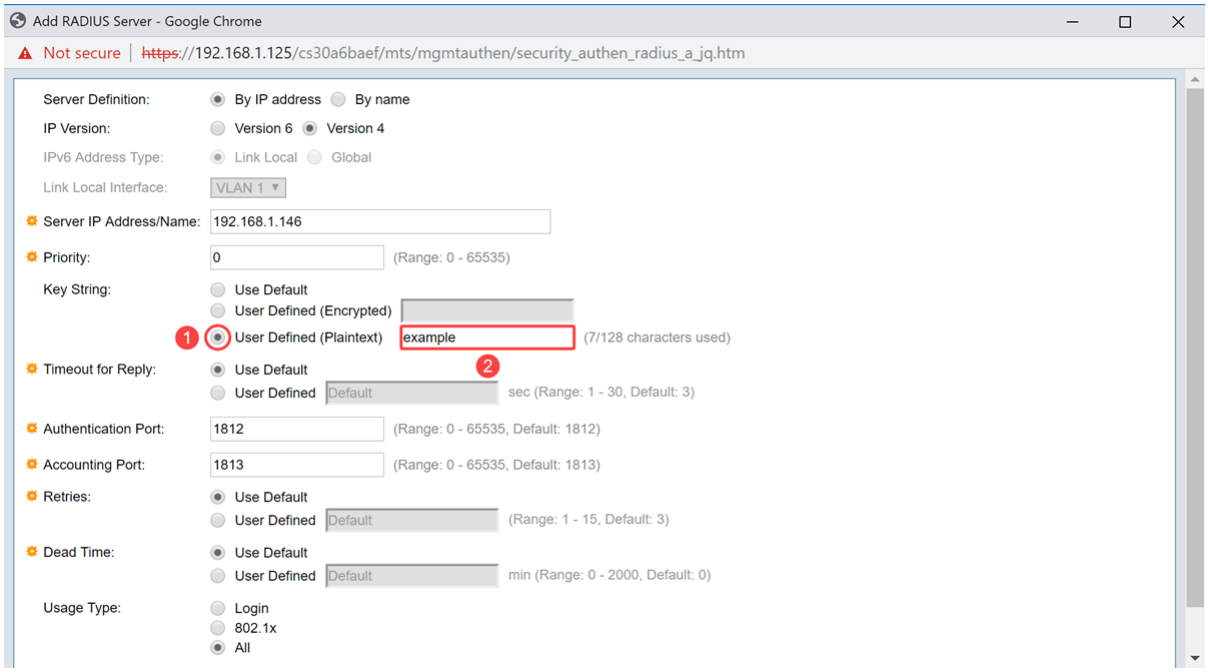
Schritt 6: Geben Sie die Priorität des Servers ein. Die Priorität legt die Reihenfolge fest, in der das Gerät versucht, die Server zu kontaktieren, um einen Benutzer zu authentifizieren. Das Gerät beginnt zuerst mit dem RADIUS-Server mit der höchsten Priorität. 0 hat höchste Priorität.



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.

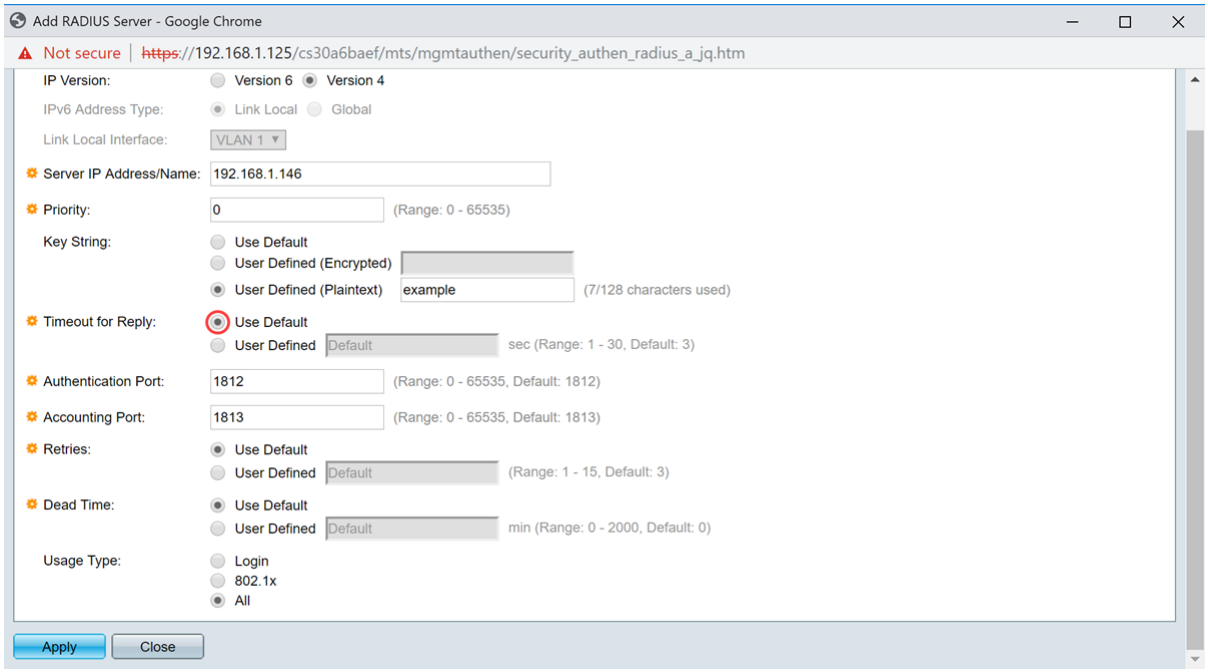
Hinweis: Wir verwenden den **User Defined (Plaintext)** und geben das Schlüsselbeispiel **ein**.

Um zu erfahren, wie Sie die RADIUS-Servereinstellungen auf Ihrem Switch konfigurieren, klicken Sie hier.



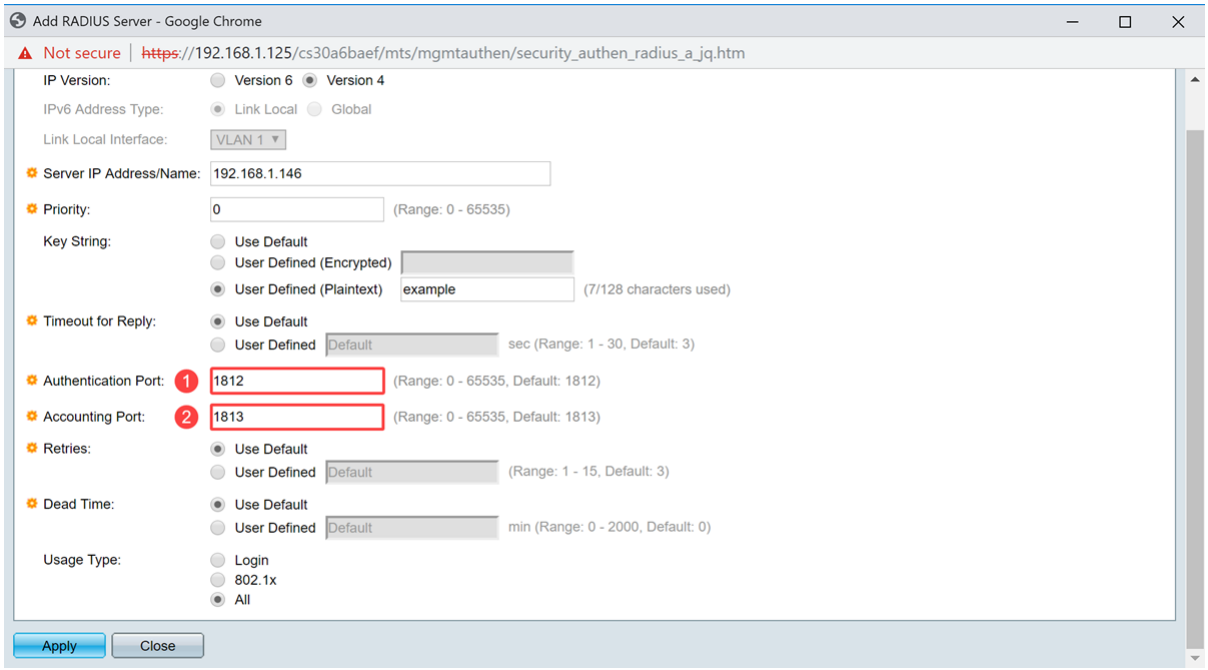
Schritt 8: Wählen Sie im Feld *Timeout für Antwort* entweder **Standard** oder **Benutzerdefiniert** aus. Wenn **User Defined** (Benutzerdefiniert) ausgewählt wurde, geben Sie die Anzahl der Sekunden ein, die das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor die Abfrage erneut versucht wird, oder wechseln Sie zum nächsten Server, wenn die maximale Anzahl von Wiederholungen vorgenommen wurde. Wenn **Standard verwenden** ausgewählt ist, verwendet das Gerät den Standard-Timeoutwert.

Hinweis: In diesem Beispiel wurde **Use Default (Standard verwenden)** ausgewählt.



Schritt 9: Geben Sie die UDP-Portnummer des RADIUS-Server-Ports für die Authentifizierungsanfrage im Feld *Authentifizierungsport ein*. Geben Sie die UDP-Portnummer des RADIUS-Server-Ports für Buchhaltungsanfragen im Feld *Buchhaltungsport ein*.

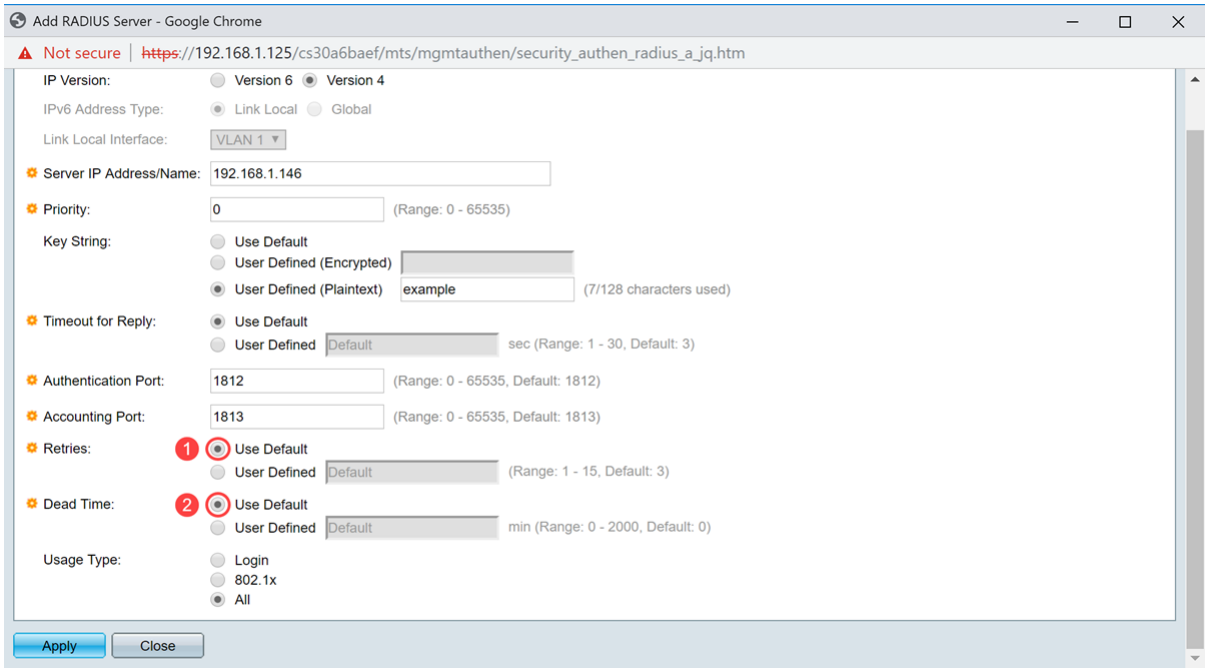
Hinweis: In diesem Beispiel wird der Standardwert sowohl für den Authentifizierungsport als auch für den Accounting-Port verwendet.



Schritt 10: Wenn **User Defined (Benutzerdefiniert)** für das Feld *Retries (Wiederholungen)* ausgewählt ist, geben Sie die Anzahl der Anforderungen ein, die an den RADIUS-Server gesendet werden, bevor ein Fehler als aufgetreten angesehen wird. Wenn **Standard verwenden** ausgewählt wurde, verwendet das Gerät den Standardwert für die Anzahl der Wiederholungen.

Wenn **User Defined (Benutzerdefiniert)** für *Dead Time (Ausfallzeit)* ausgewählt ist, geben Sie die Anzahl der Minuten ein, die überschritten werden müssen, bevor ein nicht reagierender RADIUS-Server für Serviceanfragen umgangen wird. Wenn **Standard verwenden** ausgewählt wurde, verwendet das Gerät den Standardwert für die Ausfallzeit. Wenn Sie 0 Minuten eingegeben haben, gibt es keine Ausfallzeit.

Hinweis: In diesem Beispiel wählen Sie **Standard** für beide Felder **verwenden**.

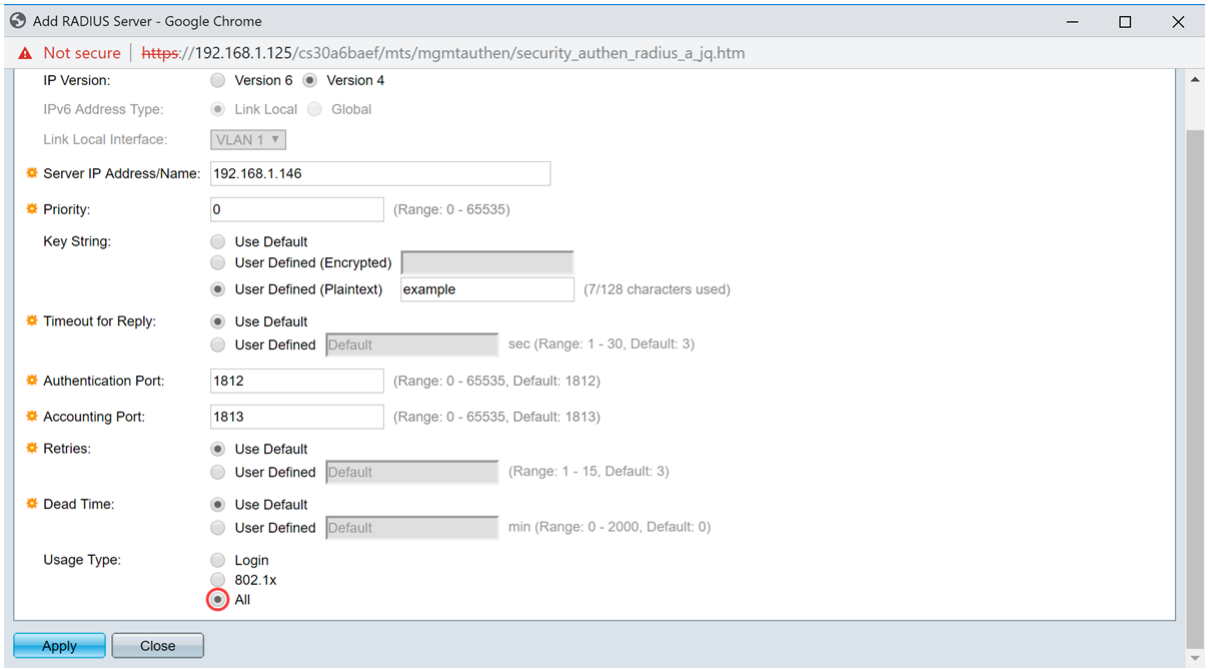


Schritt 11: Geben Sie im Feld *Usage Type* (*Nutzungstyp*) den Authentifizierungstyp des RADIUS-Servers ein. Folgende Optionen stehen zur Verfügung:

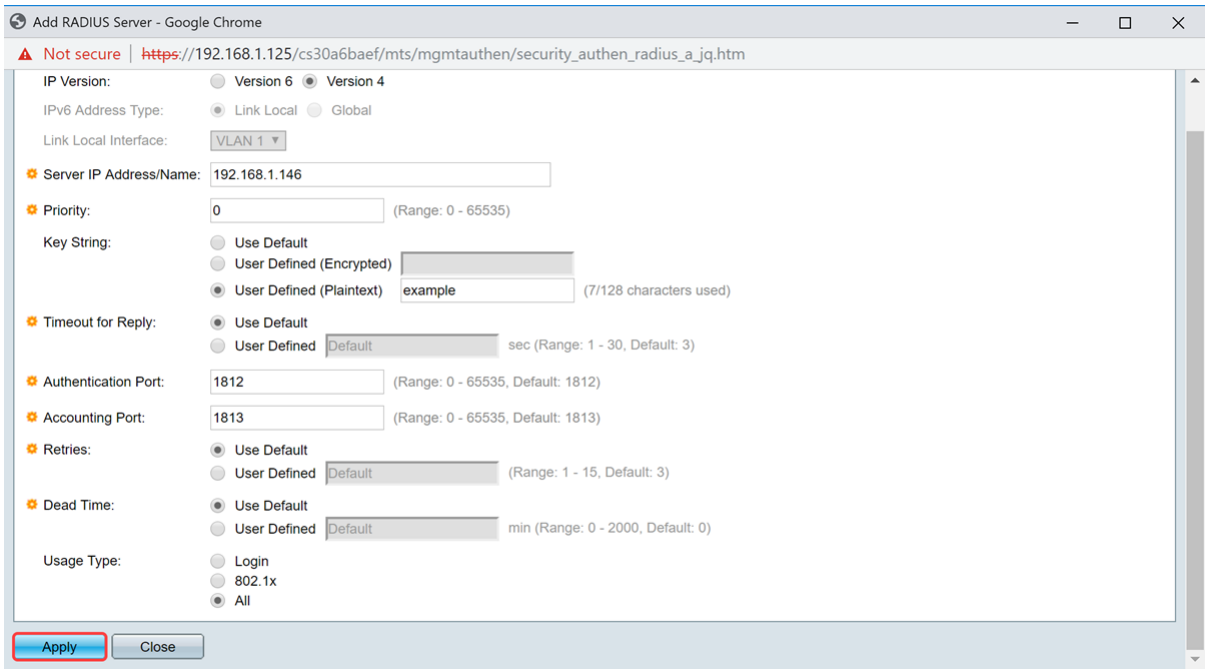
Anmeldung - Der RADIUS-Server wird zur Authentifizierung von Benutzern verwendet, die das Gerät verwalten möchten.

802.1x - Der RADIUS-Server wird für die 802.1x-Authentifizierung verwendet.

Alle - Der RADIUS-Server dient zur Authentifizierung von Benutzern, die das Gerät verwalten möchten, und zur 802.1x-Authentifizierung.



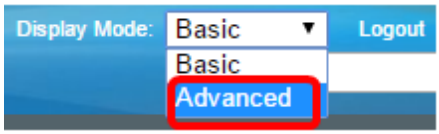
Schritt 12: Klicken Sie auf **Übernehmen**.



Konfigurieren der Einstellungen für die 802.1x-Portauthentifizierung

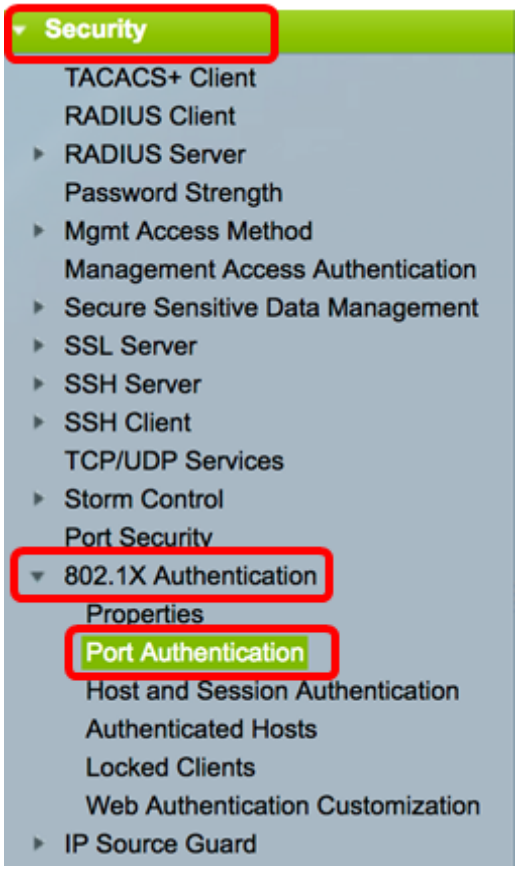
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an, und wählen Sie dann in der Dropdown-Liste Anzeigemodus die Option **Erweitert** aus.

Hinweis: Die verfügbaren Menüoptionen können je nach Gerätemodell variieren. In diesem Beispiel wird SG350X-48MP verwendet.



Hinweis: Wenn Sie einen Switch der Serie Sx300 oder Sx500 haben, fahren Sie mit Schritt 2 fort.

Schritt 2: Wählen Sie **Security > 802.1X Authentication > Port Authentication aus**.

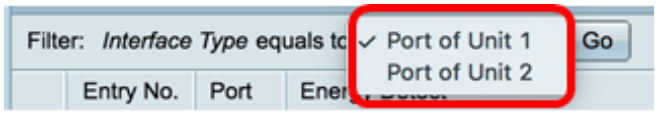


Schritt 3: Wählen Sie in der Dropdown-Liste *Schnittstellentyp* eine Schnittstelle aus.

Port - Wählen Sie in der Dropdown-Liste *Interface Type (Schnittstellentyp)* die Option **Port** aus, wenn nur ein Port ausgewählt werden muss.

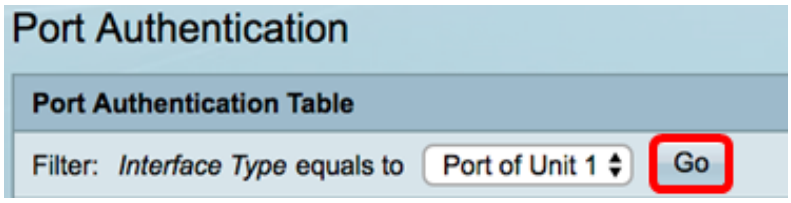
LAG: Wählen Sie in der Dropdown-Liste *Interface Type (Schnittstellentyp*) die zu konfigurierende LAG aus. Dies betrifft die in der LAG-Konfiguration definierte Portgruppe.

Hinweis: In diesem Beispiel wird Port von Einheit 1 ausgewählt.

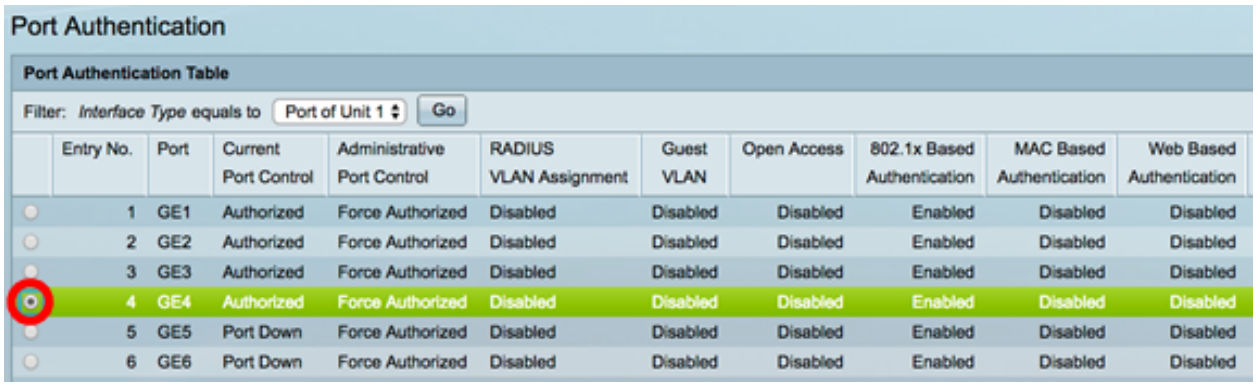


Hinweis: Wenn Sie über einen nicht stapelbaren Switch wie einen Switch der Serie Sx300 verfügen, fahren Sie mit Schritt 5 fort.

Schritt 4: Klicken Sie auf **Go**, um eine Liste der Ports oder LAGs auf der Schnittstelle anzuzeigen.



Schritt 5: Klicken Sie auf den Port, den Sie konfigurieren möchten.



Hinweis: In diesem Beispiel wird GE4 ausgewählt.

Schritt 6: Blättern Sie auf der Seite nach unten, und klicken Sie dann auf **Bearbeiten**.

Schritt 7: (Optional) Wenn Sie eine andere Schnittstelle bearbeiten möchten, wählen Sie eine der Dropdown-Listen Einheit und Port aus.

Hinweis: In diesem Beispiel wird Port GE4 von Einheit 1 ausgewählt.

Schritt 8: Klicken Sie auf das Optionsfeld für das gewünschte Port-Steuerelement im Bereich Administrative Port Control. Folgende Optionen stehen zur Verfügung:

Force Unauthorized (Nicht autorisieren erzwingen) - Verweigert den Schnittstellenzugriff, indem der Port in den nicht autorisierten Zustand verschoben wird. Der Port verwirft Datenverkehr.

Auto (Automatisch): Der Port wechselt je nach Authentifizierung der Komponente zwischen einem autorisierten oder einem nicht autorisierten Status.

Force Authorized (Autorisiert erzwingen) - Autorisiert den Port ohne Authentifizierung. Der Port leitet den Datenverkehr weiter.

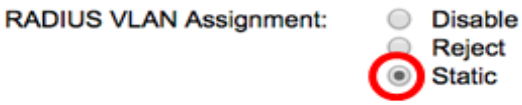
Hinweis: In diesem Beispiel wird Auto ausgewählt.

Schritt 9: Klicken Sie auf das Optionsfeld RADIUS VLAN Assignment (RADIUS-VLAN-Zuweisung), um die dynamische VLAN-Zuweisung für den ausgewählten Port zu konfigurieren. Folgende Optionen stehen zur Verfügung:

Disable (Deaktivieren) - Feature ist nicht aktiviert.

Ablehnen - Wenn der RADIUS-Server die Komponente autorisiert hat, aber kein Supplicant VLAN bereitgestellt hat, wird die Komponente abgelehnt.

Static (Statisch): Wenn der RADIUS-Server die Komponente autorisiert hat, aber kein Supplicant VLAN bereitgestellt hat, wird die Komponente akzeptiert.



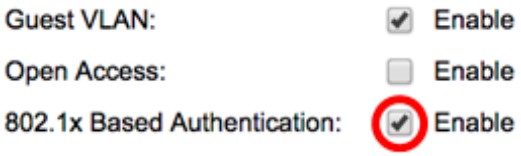
Hinweis: In diesem Beispiel wird "Statisch" ausgewählt.

Schritt 10: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Gast-VLAN, um das Gast-VLAN für nicht autorisierte Ports zu aktivieren. Das Gast-VLAN fügt den nicht autorisierten Port automatisch dem im Gast-VLAN-ID-Bereich der 802.1-Eigenschaften ausgewählten VLAN hinzu.

Schritt 11: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Open Access (Offenen Zugriff aktivieren), um den freien Zugriff zu aktivieren. Open Access hilft Ihnen, die Konfigurationsprobleme von Hosts zu verstehen, die mit dem Netzwerk verbunden sind, überwacht schlechte Situationen und ermöglicht die Behebung dieser Probleme.

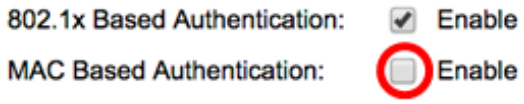
Hinweis: Wenn Open Access auf einer Schnittstelle aktiviert ist, behandelt der Switch alle Fehler, die von einem RADIUS-Server empfangen wurden, als erfolgreich und ermöglicht den Zugriff auf das Netzwerk für mit Schnittstellen verbundene Stationen, unabhängig von den Authentifizierungsergebnissen. In diesem Beispiel ist Open Access deaktiviert.

Schritt 12: Aktivieren Sie das Kontrollkästchen **802.1x-basierte Authentifizierung aktivieren**, um die 802.1X-Authentifizierung auf dem Port zu aktivieren.



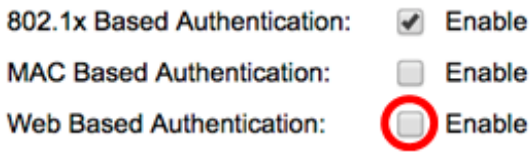
Schritt 13: Aktivieren Sie das Kontrollkästchen **MAC-basierte Authentifizierung aktivieren**, um die Portauthentifizierung auf der Grundlage der zugehörigen MAC-Adresse zu aktivieren. Auf dem Port können nur acht MAC-basierte Authentifizierungen verwendet werden.

Hinweis: Damit die MAC-Authentifizierung erfolgreich ist, müssen der Benutzername und das Kennwort der RADIUS-Serverkomponente die entsprechende MAC-Adresse sein. Die MAC-Adresse muss in Kleinbuchstaben eingegeben und ohne die eingegeben werden. oder - Trennzeichen (z. B. 0020aa00bcc).



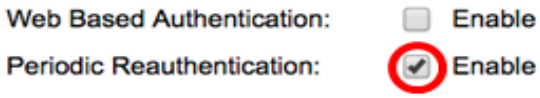
Hinweis: In diesem Beispiel ist die MAC-basierte Authentifizierung deaktiviert.

Schritt 14: Aktivieren Sie das Kontrollkästchen Webbasierte Authentifizierung **aktivieren**, um die webbasierte Authentifizierung auf dem Switch zu aktivieren. In diesem Beispiel ist die webbasierte Authentifizierung deaktiviert.



Hinweis: In diesem Beispiel ist die webbasierte Authentifizierung deaktiviert.

Schritt 15: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Periodic Reauthentication (** Periodische Reauthentifizierung **aktivieren**), um die erneute Authentifizierung des Ports nach einer bestimmten Zeit zu erzwingen. Diese Zeit wird im Feld *Reauthentication Period* definiert.

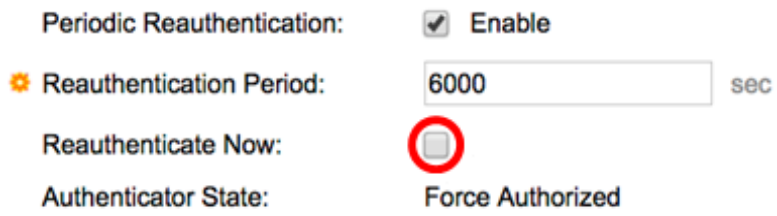


Hinweis: In diesem Beispiel ist die Periodenneuauthentifizierung aktiviert.

Schritt 16: (Optional) Geben Sie im Feld *Reauthentication Period* einen Wert ein. Dieser Wert stellt die Anzahl der Sekunden dar, bis die Schnittstelle den Port erneut authentifiziert. Der Standardwert ist 3600 Sekunden und der Bereich liegt zwischen 300 und 4294967295 Sekunden.

Hinweis: In diesem Beispiel werden 6000 Sekunden konfiguriert.

Schritt 17: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Reauthentication Now (Jetzt erneut authentifizieren aktivieren), um eine sofortige Port-erneute Authentifizierung zu erzwingen. In diesem Beispiel ist die sofortige erneute Authentifizierung deaktiviert.



Im Bereich "Authenticator State" (Authentifizierungsstatus) wird der Autorisierungsstatus des Ports angezeigt.

Schritt 18: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Time Range (Zeitbereich aktivieren), um eine Beschränkung für die Dauer der Port-Autorisierung zu aktivieren.

Hinweis: In diesem Beispiel ist Time Range aktiviert. Wenn Sie diese Funktion überspringen möchten, fahren Sie mit Schritt 20 fort.

Schritt 19: (Optional) Wählen Sie aus der Dropdown-Liste "Time Range Name" (Zeitbereichsname) einen zu verwendenden Zeitraum aus.

Hinweis: In diesem Beispiel wird Dayshift gewählt.

Schritt 20: Klicken Sie im Bereich Maximum WBA Login Attempts (Maximale WBA-Anmeldeversuche) entweder auf Infinite (Unbegrenzt), um keine Beschränkung zu erhalten, oder auf User Defined (Benutzerdefiniert), um eine Beschränkung festzulegen. Wenn User Defined (Benutzerdefiniert) ausgewählt ist, geben Sie die maximal zulässige Anzahl von Anmeldeversuchen für die webbasierte Authentifizierung ein.

Hinweis: In diesem Beispiel wird Infinite ausgewählt.

Schritt 21: Klicken Sie im Bereich Maximum WBA Silence Period (Maximale WBA-Pausenzeit) entweder auf Infinite (Unbegrenzt), um keine Grenze zu überschreiten, oder auf User Defined (Benutzerdefiniert), um eine Obergrenze festzulegen. Wenn User Defined (Benutzerdefiniert) ausgewählt ist, geben Sie die auf der Schnittstelle zulässige maximale Dauer für die unbeaufsichtigte Authentifizierung für die webbasierte Authentifizierung ein.

Hinweis: In diesem Beispiel wird Infinite ausgewählt.

Schritt 22: Klicken Sie im Bereich Max Hosts (Max-Hosts) entweder auf Infinite (Unbegrenzt), um keine Grenze zu überschreiten, oder auf User Defined (Benutzerdefiniert),

um einen Grenzwert festzulegen. Wenn User Defined (Benutzerdefiniert) ausgewählt ist, geben Sie die maximal zulässige Anzahl an autorisierten Hosts für die Schnittstelle ein.

Hinweis: Legen Sie diesen Wert auf 1 fest, um den Einzelhost-Modus für die webbasierte Authentifizierung im Multi-Session-Modus zu simulieren. In diesem Beispiel wird Infinite ausgewählt.

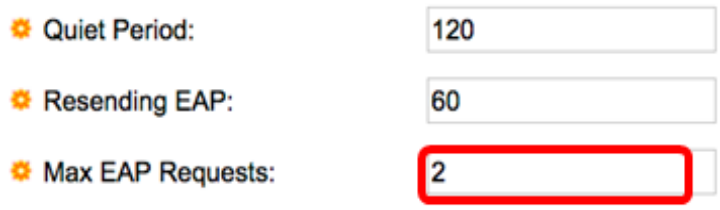
Schritt 23: Geben Sie im Feld *Stille Periode* (Stille Periode) ein, wann der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhezustand bleibt. Wenn sich der Switch im Ruhezustand befindet, bedeutet dies, dass der Switch keine neuen Authentifizierungsanforderungen vom Client überwacht. Der Standardwert ist 60 Sekunden, der Bereich liegt zwischen 1 und 65535 Sekunden.

Hinweis: In diesem Beispiel wird die Zeitdauer für die Stille auf 120 Sekunden festgelegt.

Schritt 24: Geben Sie im Feld *Resending EAP* (EAP erneut senden) ein, wann der Switch auf eine Antwortnachricht vom Supplicant wartet, bevor eine Anfrage erneut gesendet wird. Der Standardwert ist 30 Sekunden, und der Bereich liegt zwischen 1 und 65.535 Sekunden.

Hinweis: In diesem Beispiel ist das erneute Aussenden des EAP auf 60 Sekunden festgelegt.

Schritt 25: Geben Sie im Feld *Max EAP Requests* (Max. EAP-Anforderungen*)* die maximale Anzahl der EAP-Anfragen ein, die gesendet werden können. EAP ist eine Authentifizierungsmethode, die in 802.1X verwendet wird und den Austausch von Authentifizierungsinformationen zwischen Switch und Client ermöglicht. In diesem Fall werden EAP-Anforderungen zur Authentifizierung an den Client gesendet. Der Client muss dann antworten und die Authentifizierungsinformationen abgleichen. Wenn der Client nicht antwortet, wird eine weitere EAP-Anforderung basierend auf dem EAP-Wert "Resending" (Wiedergeben) festgelegt, und der Authentifizierungsprozess wird neu gestartet. Der Standardwert ist 2 und der Bereich liegt zwischen 1 und 10.

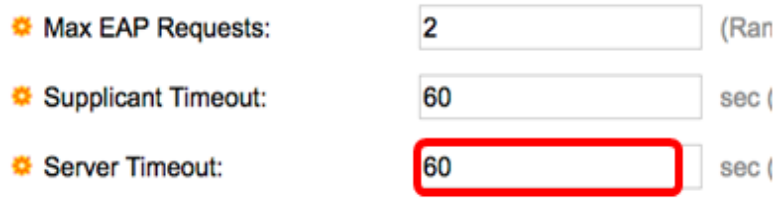


Hinweis: In diesem Beispiel wird der Standardwert 2 verwendet.

Schritt 26: Geben Sie im Feld *Supplicant Timeout* (Supplikant-Zeitüberschreitung*)* die Zeit ein, bevor EAP-Anforderungen an die Komponente gesendet werden. Der Standardwert ist 30 Sekunden, und der Bereich liegt zwischen 1 und 65.535 Sekunden.

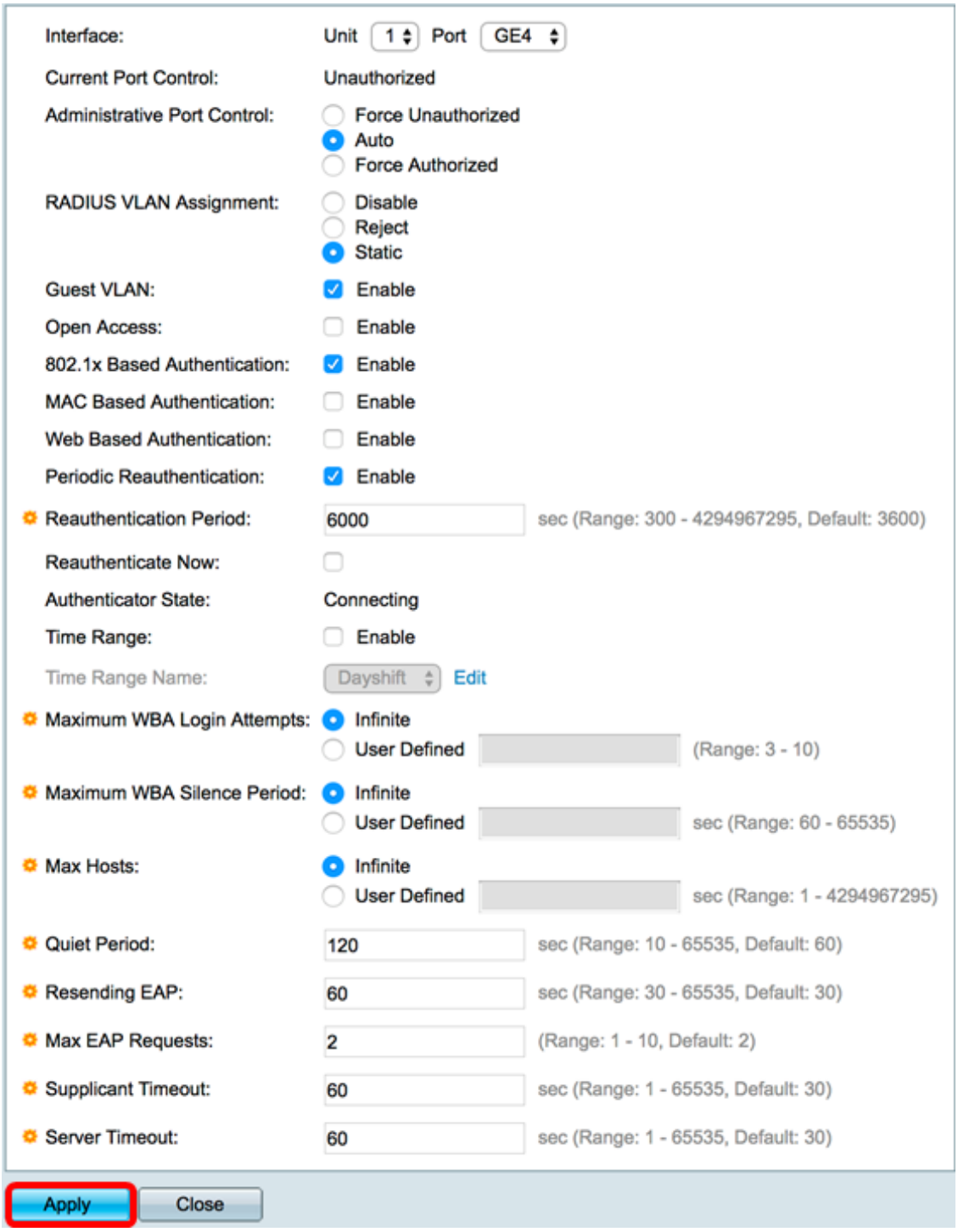
Hinweis: In diesem Beispiel ist das Supplicant Timeout auf 60 Sekunden festgelegt.

Schritt 27: Geben Sie im Feld *Server Timeout* (Serverzeitüberschreitung) die Zeit ein, die vergeht, bevor der Switch eine Anforderung erneut an den RADIUS-Server sendet. Der Standardwert ist 30 Sekunden, und der Bereich liegt zwischen 1 und 65.535 Sekunden.

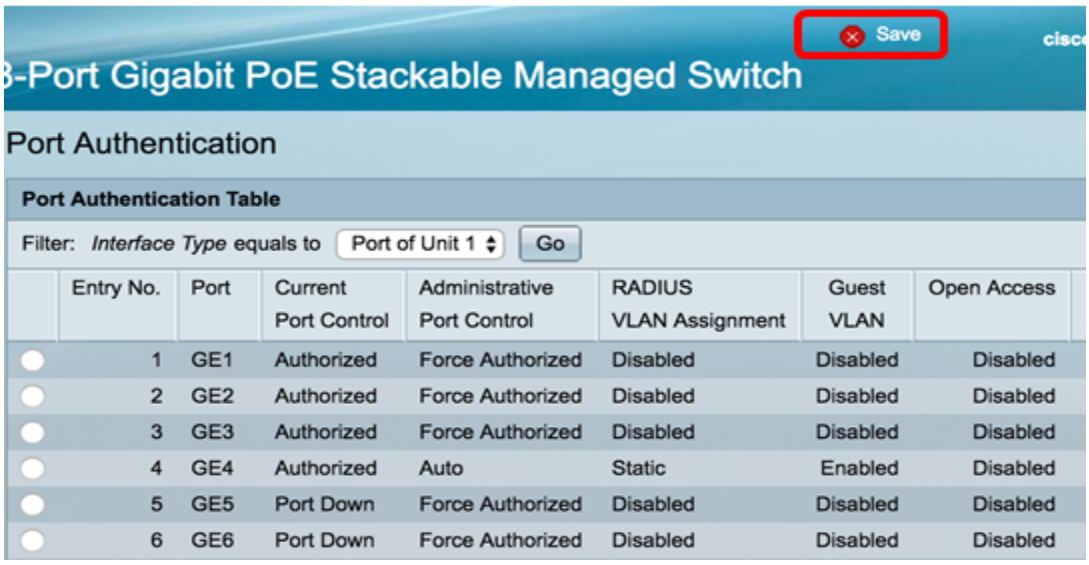


Hinweis: In diesem Beispiel ist der Servertimeout auf 60 Sekunden festgelegt.

Schritt 28: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.



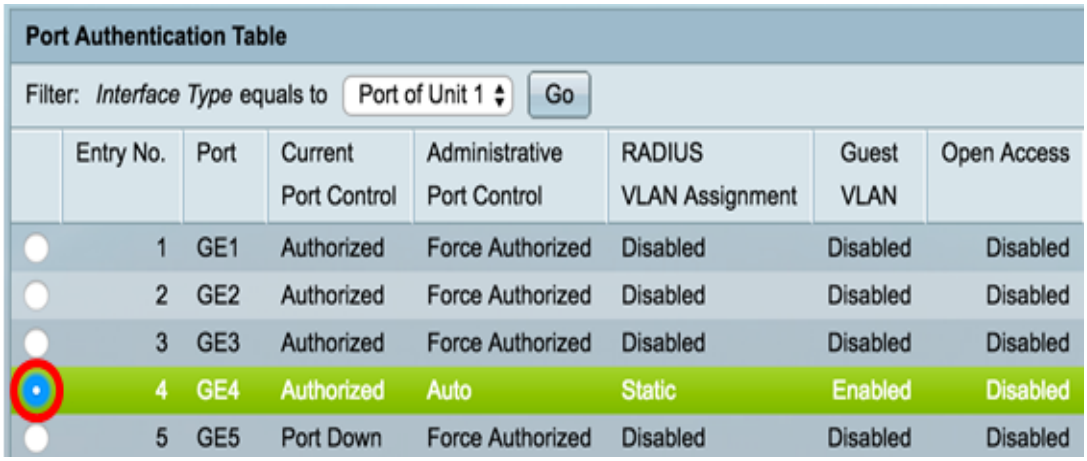
Schritt 29: (Optional) Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.



Sie sollten jetzt die 802.1x-Port-Authentifizierungseinstellungen auf Ihrem Switch erfolgreich konfiguriert haben.

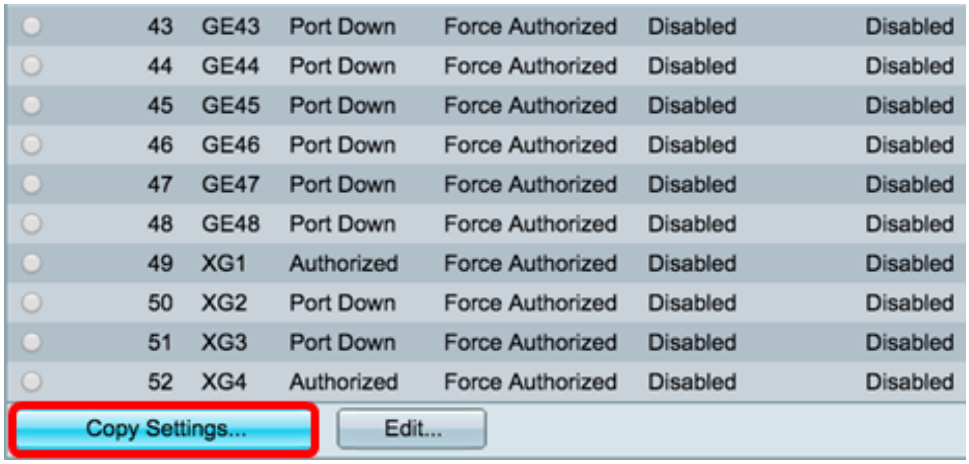
Anwenden von Schnittstellenkonfigurationseinstellungen auf mehrere Schnittstellen

Schritt 1: Klicken Sie auf das Optionsfeld der Schnittstelle, die Sie die Authentifizierungskonfiguration auf mehrere Schnittstellen anwenden möchten.



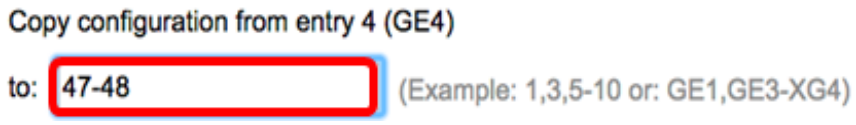
Hinweis: In diesem Beispiel wird GE4 ausgewählt.

Schritt 2: Blättern Sie nach unten, und klicken Sie dann auf **Copy Settings**.



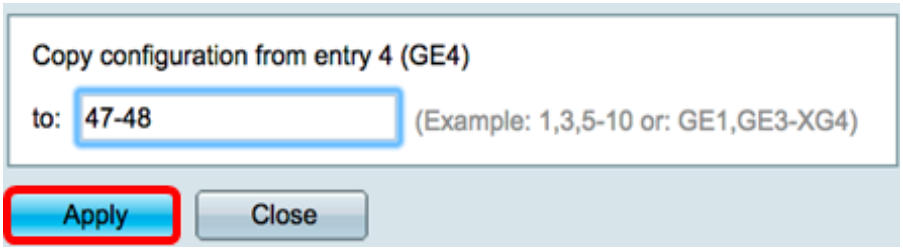
Schritt 3: Geben Sie im Feld *to* den Bereich der Schnittstellen ein, auf die Sie die

Konfiguration der ausgewählten Schnittstelle anwenden möchten. Sie können die Schnittstellennummern oder den Namen der Schnittstellen als Eingabe verwenden. Sie können jede Schnittstelle durch ein Komma getrennt eingeben (z. B. 1, 3, 5 oder GE1, GE3, GE5) oder einen Schnittstellenbereich eingeben (z. B. 1-5 oder GE1-GE5).

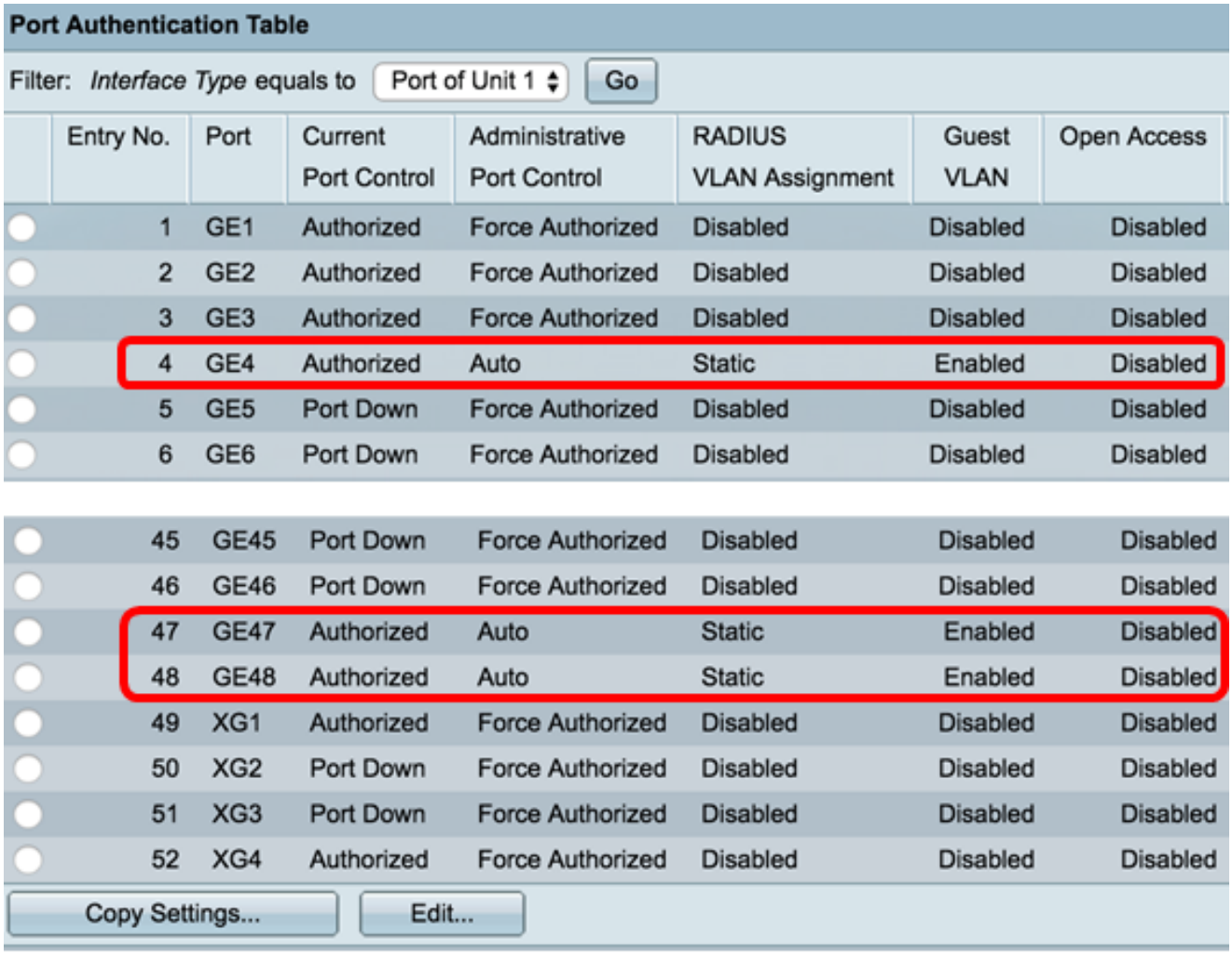


Hinweis: In diesem Beispiel werden die Konfigurationseinstellungen auf die Ports 47 bis 48 angewendet.

Schritt 4: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.



Das folgende Bild zeigt die Änderungen nach der Konfiguration.



Sie sollten jetzt die 802.1x-Authentifizierungseinstellungen eines Ports erfolgreich kopiert und auf andere Ports am Switch angewendet haben.