Konfigurieren der 802.1X-Port-Authentifizierung auf den Cisco Smart Switches der Serie Sx220

Ziel

In diesem Artikel erfahren Sie, wie Sie die Port-Authentifizierung auf den Smart Switches der Serie Sx220 konfigurieren.

Die 802.1X-Portauthentifizierung ermöglicht die Konfiguration von 802.1X-Parametern für jeden Port Ihres Geräts. Ein Port, der Authentifizierung anfordert, wird als Supplicant bezeichnet. Der Authentifizierer ist ein Switch oder Access Point, der als Netzwerkschutz für Supplicants fungiert. Der Authentifizierer leitet Authentifizierungsmeldungen an den RADIUS-Server weiter, sodass ein Port authentifiziert werden kann und Informationen senden und empfangen kann.

Anwendbare Geräte

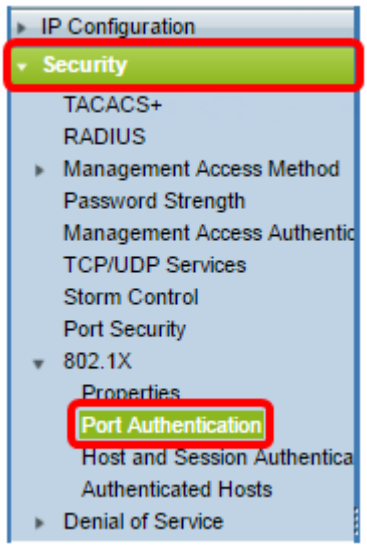
- Serie Sx220

Softwareversion

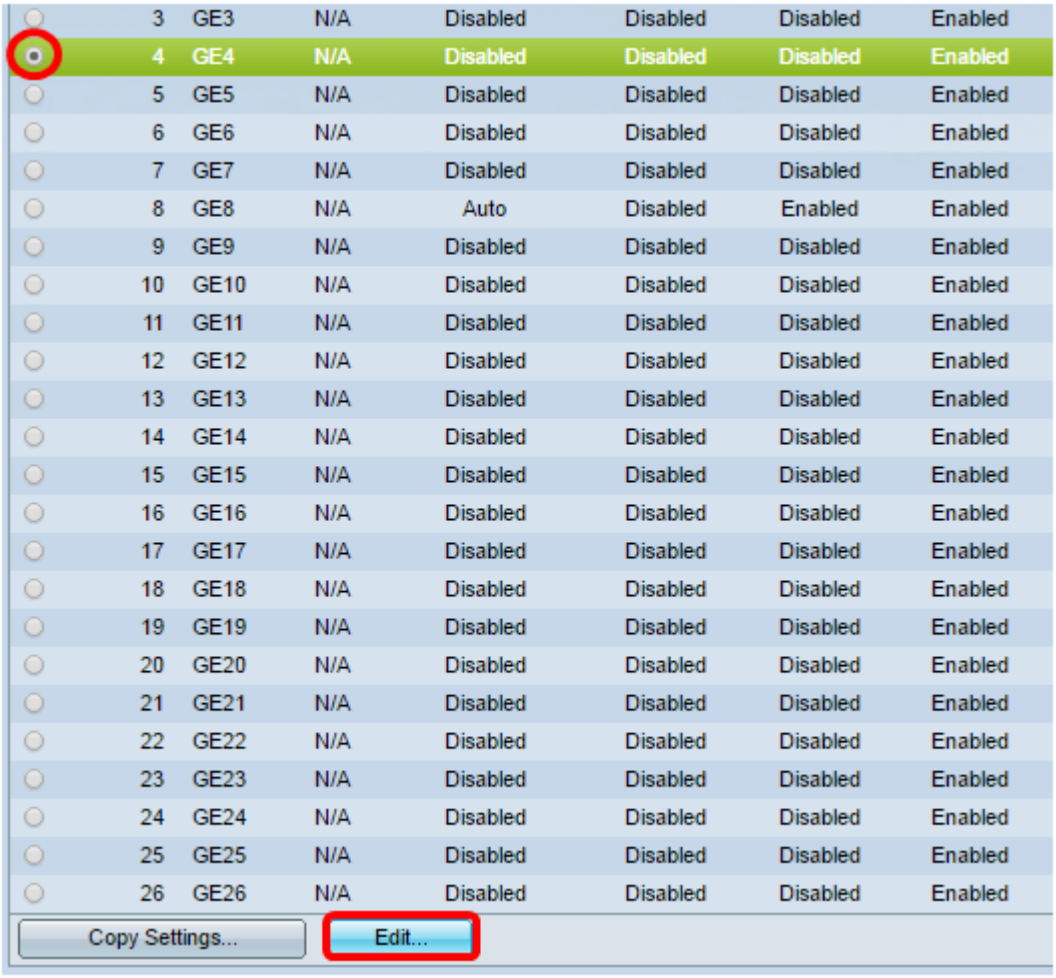
- 1,1 0,14

Port-Authentifizierung konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Switch-Dienstprogramm an, und wählen Sie **Security > 802.1X > Port Authentication aus**.



Schritt 2: Klicken Sie auf das Optionsfeld für den Port, den Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.

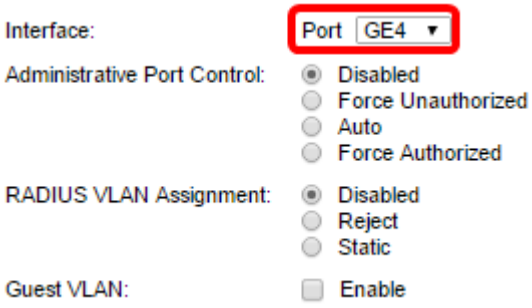


○	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
○	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
○	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
○	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
○	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
○	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
○	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
○	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
○	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
○	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
○	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
○	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
○	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
○	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
○	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
○	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
○	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
○	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
○	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
○	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
○	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
○	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
○	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

Hinweis: In diesem Beispiel wird Port GE4 ausgewählt.

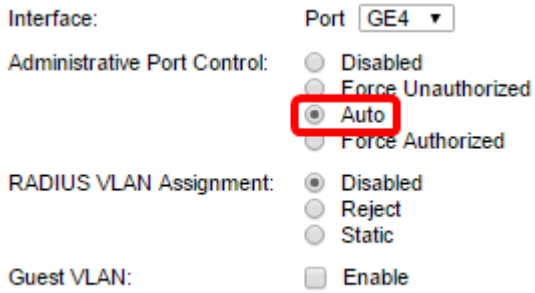
Schritt 3: Daraufhin wird das Fenster "Edit Port Authentication" (Portauthentifizierung bearbeiten) angezeigt. Vergewissern Sie sich in der Dropdown-Liste Interface (Schnittstelle), dass der angegebene Port der in Schritt 2 ausgewählte Port ist. Andernfalls klicken Sie auf den Dropdown-Pfeil, und wählen Sie den richtigen Port aus.



Schritt 4: Wählen Sie eine Optionsschaltfläche für das Administrative Port Control. Dadurch wird der Port-Autorisierungsstatus bestimmt. Folgende Optionen stehen zur Verfügung:

- Disabled (Deaktiviert): Deaktiviert 802.1X. Dies ist der Standardstatus.
- Force Unauthorized (Nicht autorisieren erzwingen) - Verweigert den Schnittstellenzugriff, indem die Schnittstelle in den nicht autorisierten Zustand verschoben wird. Der Switch stellt dem Client über die Schnittstelle keine Authentifizierungsdienste zur Verfügung.
- Auto (Automatisch): Aktiviert die Port-basierte Authentifizierung und Autorisierung auf dem Switch. Die Schnittstelle wechselt zwischen einem autorisierten oder nicht

autorisierten Zustand, der auf dem Authentifizierungs-Austausch zwischen Switch und Client basiert.
- Force Authorized (Autorisiert erzwingen): Autorisiert die Schnittstelle ohne Authentifizierung.

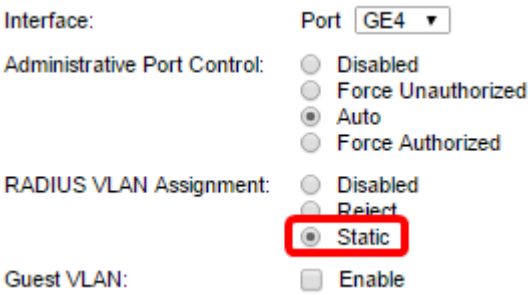


Hinweis: In diesem Beispiel wird Auto ausgewählt.

Schritt 5: (Optional) Wählen Sie eine Optionsschaltfläche für die RADIUS VLAN-Zuweisung. Dadurch wird die dynamische VLAN-Zuweisung für den angegebenen Port aktiviert. Folgende Optionen stehen zur Verfügung:

- Disabled (Deaktiviert): Ignoriert das VLAN-Autorisierungsergebnis und behält das ursprüngliche VLAN des Hosts bei. Dies ist die Standardaktion.
- Ablehnen: Wenn der angegebene Port autorisierte VLAN-Informationen empfängt, verwendet er diese Informationen. Wenn jedoch keine VLAN-autorisierten Informationen vorhanden sind, werden diese vom Host abgelehnt und nicht autorisiert.
- Statisch - Wenn der angegebene Port autorisierte VLAN-Informationen empfängt, verwendet er diese Informationen. Wenn jedoch keine VLAN-autorisierten Informationen vorhanden sind, wird das ursprüngliche VLAN des Hosts beibehalten.

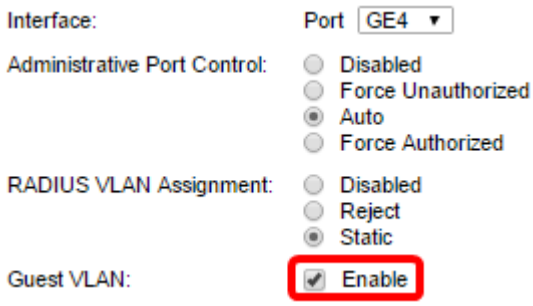
Hinweis: Wenn ein VLAN autorisierte Informationen von RADIUS enthält, das VLAN jedoch nicht administrativ für Device Under Test (DUT) erstellt wurde, wird das VLAN automatisch erstellt. In diesem Beispiel wird "Statisch" ausgewählt.



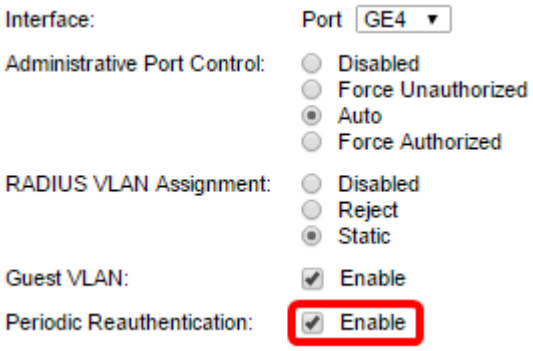
Schneller Tipp: Damit die Funktion für die dynamische VLAN-Zuweisung funktioniert, müssen die folgenden VLAN-Attribute vom RADIUS-Server gesendet werden:

- [64] Tunnel-Type = VLAN (Typ 13)
- [65] Tunnel-Medium-Type = 802 (Typ 6)
- [81] Tunnel-Private-Group-ID = VLAN-ID

Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren**, damit das Gast-VLAN ein Gast-VLAN für nicht autorisierte Ports verwendet.

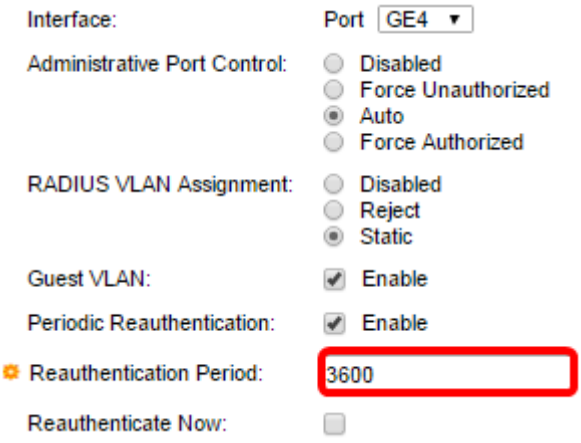


Schritt 7: Aktivieren Sie das Kontrollkästchen **Aktivieren** für die regelmäßige erneute Authentifizierung. Dadurch werden nach dem angegebenen Authentifizierungszeitraum Port-Re-Authentifizierungsversuche aktiviert.



Hinweis: Diese Funktion ist standardmäßig aktiviert.

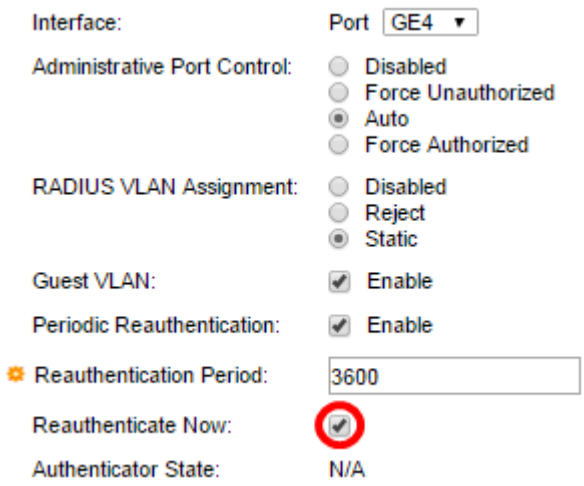
Schritt 8: Geben Sie im Feld *Reauthentication Period* einen Wert ein. Dies ist die Zeit in Sekunden, um den Port erneut zu authentifizieren.



Hinweis: In diesem Beispiel wird der Standardwert 3600 verwendet.

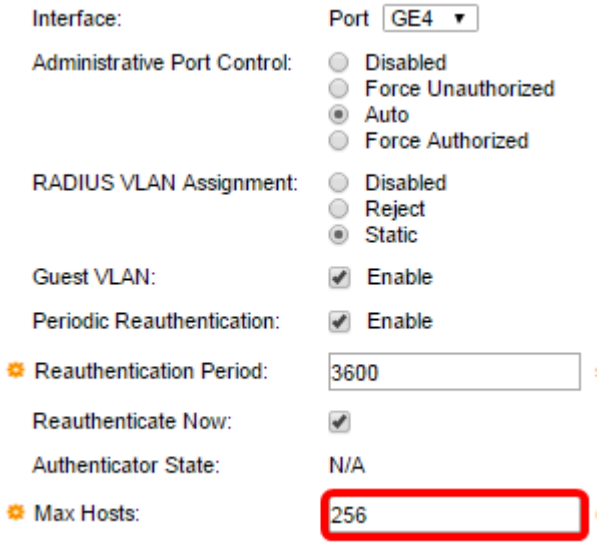
Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen **Reauthentication Now**, um die sofortige Port-Reauthentifizierung zu aktivieren.

Hinweis: Das Feld Authentifizierer-Status zeigt den aktuellen Authentifizierungsstatus an.



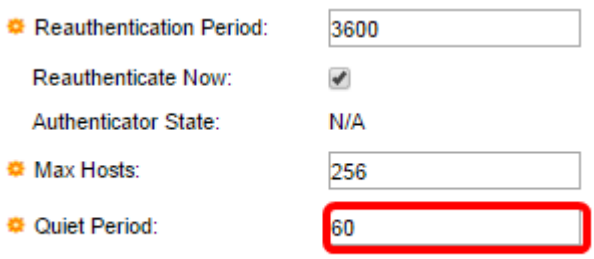
Hinweis: Wenn der Port nicht in Force Authorized (Autorisiert) oder Force Unauthorized (Nicht autorisiert erzwingen) ist, befindet er sich im Auto-Modus, und der Authentifizierer zeigt den Status der ausgeführten Authentifizierung an. Nachdem der Port authentifiziert wurde, wird der Status als Authenticated (Authentifiziert) angezeigt.

Schritt 10: Geben Sie im Feld *Max Hosts* die maximal zulässige Anzahl an authentifizierten Hosts für den jeweiligen Port ein. Dieser Wert wird nur im Multisitzungsmodus aktiviert.



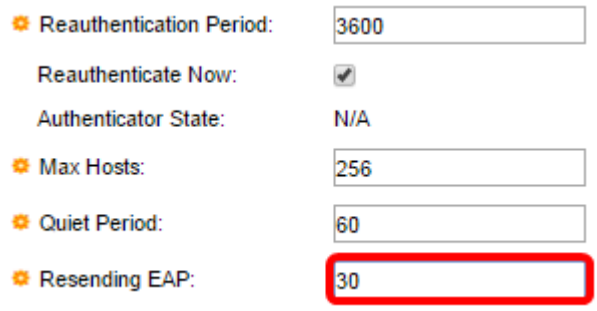
Hinweis: In diesem Beispiel wird der Standardwert 256 verwendet.

Schritt 11: Geben Sie im Feld *Stille Periode* die Anzahl der Sekunden ein, die der Switch nach einem fehlgeschlagenen Authentifizierungs-Austausch im Ruhezustand verbleibt. Wenn sich der Switch im Ruhezustand befindet, bedeutet dies, dass der Switch keine neuen Authentifizierungsanforderungen vom Client überwacht.



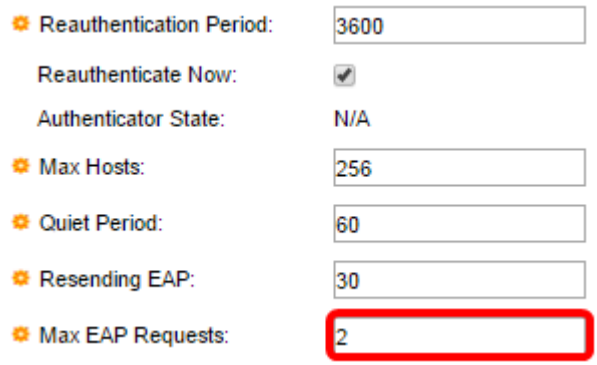
Hinweis: In diesem Beispiel wird der Standardwert 60 verwendet.

Schritt 12: Geben Sie im Feld *Resending EAP* (*EAP erneut senden*) die Anzahl der Sekunden ein, die der Switch auf eine Antwort auf eine EAP-Anforderung (Extensible Authentication Protocol) oder einen Identitäts-Frame vom Supplicant (Client) wartet, bevor die Anforderung erneut gesendet wird.



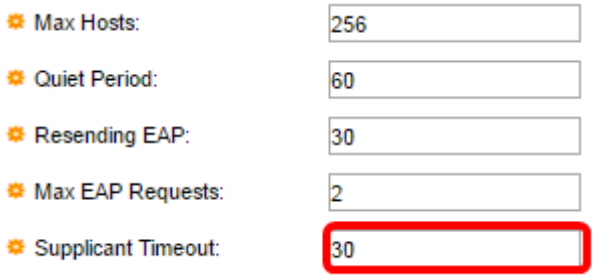
Hinweis: In diesem Beispiel wird der Standardwert 30 verwendet.

Schritt 13: Geben Sie im Feld *Max EAP Requests* (Max. EAP-Anforderungen*)* die maximale Anzahl der EAP-Anfragen ein, die gesendet werden können. Wenn nach dem festgelegten Zeitraum (Supplicant Timeout) keine Antwort empfangen wird, wird der Authentifizierungsprozess neu gestartet.



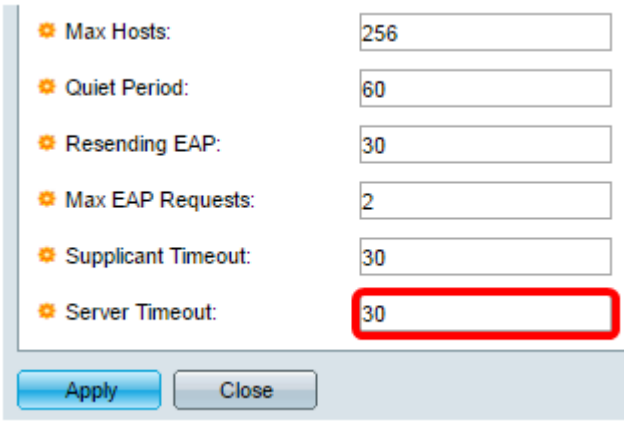
Hinweis: In diesem Beispiel wird der Standardwert 2 verwendet.

Schritt 14: Geben Sie im Feld *Supplicant Timeout (Supplicant Timeout*) die Anzahl der Sekunden ein, die vergeht, bevor EAP-Anforderungen an die Komponente gesendet werden.



Hinweis: In diesem Beispiel wird der Standardwert 30 verwendet.

Schritt 15: Geben Sie im Feld *Server Timeout* (Serverzeitüberschreitung) die Anzahl der Sekunden ein, die vergeht, bevor der Switch eine Anforderung an den Authentifizierungsserver erneut sendet.



Hinweis: In diesem Beispiel wird der Standardwert 30 verwendet.

Schritt 16: Klicken Sie auf **Übernehmen**.

Sie sollten jetzt die Port-Authentifizierung auf Ihrem Switch erfolgreich konfiguriert haben.