

# Konfigurieren der 802.1x-Authentifizierung auf Cisco Business Switches der Serie 220

## Ziel

In diesem Artikel erfahren Sie, wie Sie die 802.1x-Authentifizierung für die Cisco Business Smart Switches der Serie 220 konfigurieren.

## Unterstützte Geräte | Firmware-Version

- Serie CBS 220 ([Datenblatt](#)) | 2,0 0,17

## Einführung

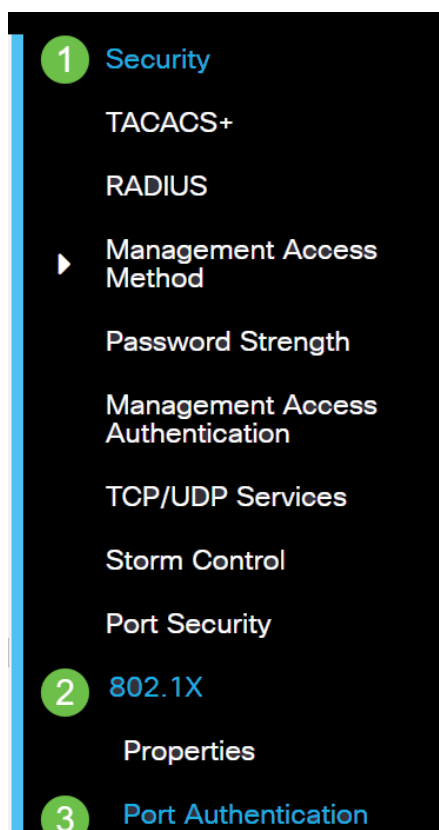
Die Portauthentifizierung ermöglicht die Konfiguration von Parametern für jeden Port. Da einige Konfigurationsänderungen nur möglich sind, wenn sich der Port im Force Authorized-Status befindet (z. B. Host-Authentifizierung), wird empfohlen, das Port-Steuerelement vor Änderungen in Force Authorized (Autorisiert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

Ein Port mit 802.1x-Definition kann kein Mitglied einer LAG werden. 802.1x und Port Security können nicht gleichzeitig auf demselben Port aktiviert werden. Wenn Sie die Port-Sicherheit auf einer Schnittstelle aktivieren, kann die Administrative Port Control nicht in den Auto-Modus geändert werden.

## Port-Authentifizierung konfigurieren

### Schritt 1

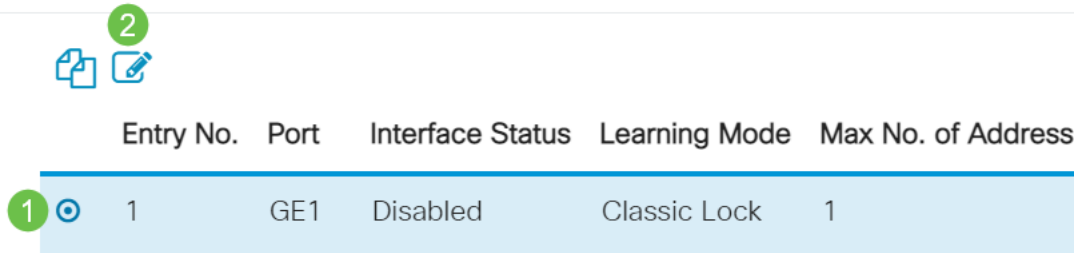
Melden Sie sich bei der Webbenutzeroberfläche des Switches an, und wählen Sie **Security > 802.1x > Port Authentication** aus.



## Schritt 2

Klicken Sie auf das Optionsfeld für den Port, den Sie konfigurieren möchten, und klicken Sie dann auf das **Bearbeitungssymbol**.

### Port Security Table



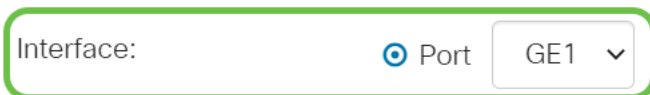
The screenshot shows a 'Port Security Table' with a table containing one entry. A green circle with the number '2' is positioned above a copy and edit icon. A green circle with the number '1' is positioned to the left of the first row of the table.

Entry No.	Port	Interface	Status	Learning Mode	Max No. of Address
1	GE1	Disabled	Classic Lock	1	

## Schritt 3

Das Fenster *Edit Port Authentication* (Portauthentifizierung bearbeiten) wird 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.

### Edit Port Authentication

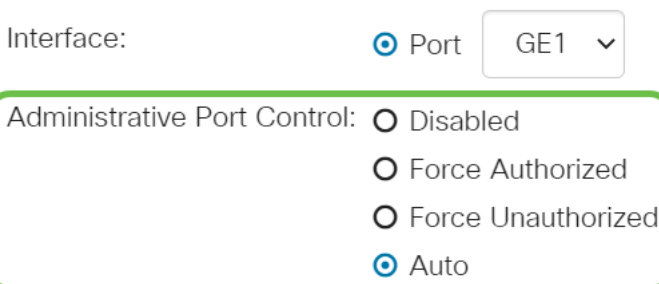


Interface:  Port GE1 ▾

## Schritt 4

Wählen Sie eine Optionsschaltfläche für das Administrative Port Control. Dadurch wird der Port-Autorisierungsstatus bestimmt. Folgende Optionen sind verfügbar:

- **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**: 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.



Interface:  Port GE1 ▾

Administrative Port Control:  Disabled  
 Force Authorized  
 Force Unauthorized  
 Auto

## 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 sind verfügbar:

- **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.

Wenn von RADIUS autorisierte VLAN-Informationen vorliegen, das VLAN jedoch nicht administrativ auf Device Under Test (DUT) erstellt wird, wird das VLAN automatisch erstellt.

RADIUS VLAN Assignment:  Disabled  
 Reject  
 Static

**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.

Guest VLAN:  Enable

### Schritt 7

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

Periodic Reauthentication:  Enable

### Schritt 8

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

Reauthentication Period: 3600

### Schritt 9 (optional)

Aktivieren Sie das Kontrollkästchen **Reauthentication Now**, um die sofortige Port-erneute Authentifizierung zu aktivieren.

Das Feld Authentifizierer-Status zeigt den aktuellen Authentifizierungsstatus an.

Reauthenticate Now:  Enable

Authenticator State: Initialize

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 Multi-Session-Modus aktiviert.

Max Hosts: 256 (Range: 1 - 256, Default: 256)

### Schritt 11

Geben Sie im Feld *Stille Periode* die Anzahl der Sekunden ein, die der Switch nach einem fehlgeschlagenen Authentifizierungs-Austausch im Ruhezustand verbleibt. Befindet sich der Switch in einem ruhigen Zustand, bedeutet dies, dass der Switch keine neuen Authentifizierungsanforderungen vom Client mehr hört.

Quiet Period: 60 sec (Range: 0 - 65535)

### 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.

Resending EAP: 30 (Range: 1 - 65535, Default: 30)

### 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.

Max EAP Requests: 2 (Range: 1 - 10, Default: 2)

### Schritt 14

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

Supplicant Timeout: 30 sec (Range: 1 - 65535, Default: 30)

## 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.

 Server Timeout:	30	sec (Range: 1 - 65535, Default:
---	----	---------------------------------

## Schritt 16

Klicken Sie auf Apply (Anwenden).

<input type="button" value="Apply"/>	<input type="button" value="Close"/>
--------------------------------------	--------------------------------------

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

Weitere Konfigurationen finden Sie im [Cisco Business Switches der Serie 220](#).

Weitere Artikel finden Sie auf der [Support-Seite für Cisco Business Switches der Serie 220](#).