

# Port-Sicherheit auf den Cisco Business Switches der Serie 220

## Ziel

In diesem Artikel werden Ihre Optionen für die Port-Sicherheit auf Ihrem Cisco Business Switch der Serie 220 erläutert.

## Unterstützte Geräte | Firmware-Version

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

## Einführung

Die Netzwerksicherheit kann erhöht werden, indem der Zugriff auf einen Port auf Benutzer mit bestimmten MAC-Adressen beschränkt wird. Die MAC-Adressen können entweder dynamisch abgerufen oder statisch konfiguriert werden. Die Portsicherheit überwacht empfangene und erfasste Pakete. Der Zugriff auf gesperrte Ports ist auf Benutzer mit bestimmten MAC-Adressen beschränkt.

Port-Sicherheit kann an Ports, an denen 802.1X aktiviert ist, oder an Ports, die als SPAN-Ziel definiert sind, nicht aktiviert werden.

Die Port-Sicherheit verfügt über zwei Modi:

- **Klassische Sperre** - Alle gelernten MAC-Adressen am Port sind gesperrt, und der Port lernt keine neuen MAC-Adressen mehr. Die erlernten Adressen sind nicht Gegenstand von Altern oder Neulernen.
- **Eingeschränkte dynamische Sperrung** - Das Gerät erfasst MAC-Adressen bis zum konfigurierten Grenzwert zulässiger Adressen. Nach Erreichen des Grenzwerts erhält das Gerät keine weiteren Adressen mehr. In diesem Modus werden die Adressen veraltet und neu gelernt.

Wenn ein Frame aus einer neuen MAC-Adresse an einem Port erkannt wird, an dem er nicht autorisiert ist (der Port ist klassisch gesperrt, eine neue MAC-Adresse vorhanden, oder der Port dynamisch gesperrt, und die maximale Anzahl zulässiger Adressen überschritten wurde), wird der Schutzmechanismus aufgerufen, und eine der folgenden Aktionen kann durchgeführt werden:

- Frame wird verworfen.
- Frame wird weitergeleitet.
- Frame wird verworfen und eine SYSLOG-Nachricht generiert.
- Der Port wird heruntergefahren.

Wenn die sichere MAC-Adresse an einem anderen Port angezeigt wird, wird der Frame weitergeleitet, aber die MAC-Adresse wird an diesem Port nicht erfasst.


Zusätzlich zu einer dieser Aktionen können Sie auch Traps generieren und deren Häufigkeit und Anzahl begrenzen, um eine Überlastung der Geräte zu vermeiden.

## Konfigurieren der Port-Sicherheit

### Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche an.

English ▾



### Cisco Business Dashboard

User Name\*

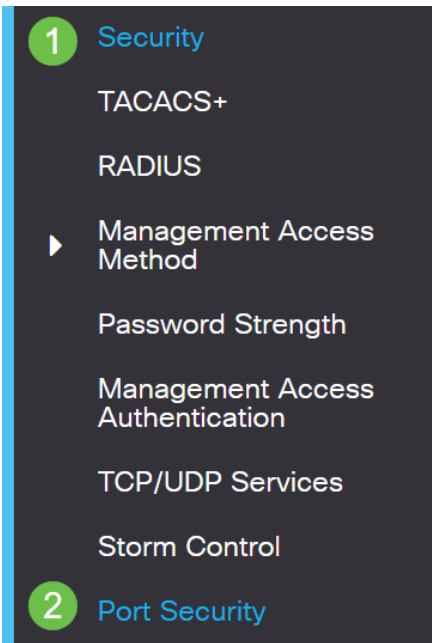
This field is required

Password\*

Login

### Schritt 2

Wählen Sie im Menü auf der linken Seite **Security > Port Security** aus.



### Schritt 3

Wählen Sie eine zu ändernde Schnittstelle aus, und klicken Sie dann auf das Bearbeitungssymbol.

#### Port Security Table

The screenshot shows the 'Port Security Table' configuration page. At the top left, there is a green circle with the number '2' and two icons: a document and a pencil. Below this is a table with the following columns: Entry No., Port, Interface Status, Learning Mode, and Max No. of Address. The first row of the table is highlighted in light blue and contains the following data: Entry No. 1, Port GE1, Interface Status Disabled, Learning Mode Classic Lock, and Max No. of Address 1. A green circle with the number '1' and a radio button icon is positioned to the left of the first row.

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

### Schritt 4

Geben Sie die Parameter ein.

- **Interface** (Schnittstelle): Wählen Sie den Schnittstellennamen aus.
- **Administrative Status**: Wählen Sie diese Option aus, um den Port zu sperren.
- **Learning Mode (Lernmodus)**: Wählen Sie den Typ der Portsperrung aus. Um dieses Feld zu konfigurieren, muss der Schnittstellenstatus entsperrt werden. Das Feld Lernmodus wird nur aktiviert, wenn das Feld Schnittstellenstatus gesperrt ist. Um den Lernmodus zu ändern, muss die Sperrschnittstelle gelöscht werden. Nachdem der Modus geändert wurde, kann die Sperrschnittstelle wieder eingesetzt werden. Folgende Optionen sind verfügbar:
  - **Klassische Sperre** - Sperrt den Port sofort, unabhängig von der Anzahl der bereits abgefragten Adressen.
  - **Eingeschränkte dynamische Sperrung** - Sperrt den Port, indem die aktuellen dynamischen MAC-Adressen des Ports gelöscht werden. Der Port erfasst bis zu den maximal zulässigen Adressen für den Port. Sowohl das erneute Lernen als auch das Altern von MAC-Adressen sind aktiviert.
- **Max No of Addresses Allowed (Max. Anzahl zulässiger Adressen)**: Geben Sie die

maximale Anzahl von MAC-Adressen ein, die auf dem Port gelernt werden können, wenn der Lernmodus "Eingeschränkte dynamische Sperrung" ausgewählt wurde. Die Zahl 0 gibt an, dass auf der Schnittstelle nur statische Adressen unterstützt werden.

- **Aktion bei Verletzung** - Wählen Sie eine Aktion aus, die auf Pakete angewendet werden soll, die an einem gesperrten Port eintreffen. Folgende Optionen sind verfügbar:
  - **Discard** - Verwirft Pakete von einer beliebigen unbekanntenen Quelle
  - **Forward (Weiterleiten)**: Weiterleitet Pakete von einer unbekanntenen Quelle weiter, ohne die MAC-Adresse zu kennen
  - **Discard and Log (Verwerfen und Protokollieren)**: Verwirft Pakete von einer beliebigen unbekanntenen Quelle, beendet die Schnittstelle, protokolliert die Ereignisse und sendet Traps an die angegebenen Trap-Empfänger Shutdown (Herunterfahren von Paketen von einer beliebigen unbekanntenen Quelle). Anschließend wird der Port heruntergefahren. Der Port bleibt so lange geschlossen, bis er wieder aktiviert wird oder bis das Gerät neu gestartet wird.
  - **Trap Frequency (Trap-Frequenz)** - Geben Sie die minimale Zeit (in Sekunden) ein, die zwischen Traps vergeht.

Klicken Sie auf **Apply** (Anwenden).

## Edit Port Settings



Interface: **1**  Port GE1 ▾

Administrative Status: **2**  Enable

Learning Mode: **3**  Classic Lock  
 Limited Dynamic Lock

✦ Max No. of Address Allowed: **4**  (Range: 1 - 256, Default: 1)

Action on Violation: **5**  Discard  
 Forward  
 Discard and Log  
 Shutdown

✦ Trap Frequency (sec): **6**  (Range: 1 - 1000000, Default: 10)

---

**7**

Wenn Sie ein Beispiel für das Standardverhalten der Port-Sicherheit auf Ihrem CBS220 sehen möchten, überprüfen Sie das [Portsicherheitsverhalten](#).

Fazit

So einfach ist das. Profitieren Sie von Ihrem sicheren Netzwerk!

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

Weitere Artikel finden Sie auf der [Cisco Business Switch Support-Seite](#).