

# Sécurité des ports sur les commutateurs Cisco Business 220

## Objectif

Cet article explique les options de sécurité des ports de votre commutateur Cisco Business 220.

## Périphériques pertinents | Version du micrologiciel

- Série CBS220 ([fiche technique](#)) | 2.0.0.17

## Introduction

La sécurité du réseau peut être améliorée en limitant l'accès sur un port aux utilisateurs possédant des adresses MAC spécifiques. Les adresses MAC peuvent être apprises dynamiquement ou configurées de manière statique. La sécurité des ports surveille les paquets reçus et appris. L'accès aux ports verrouillés est limité aux utilisateurs possédant des adresses MAC spécifiques.

La sécurité des ports ne peut pas être activée sur les ports sur lesquels 802.1X est activé ou sur les ports définis comme destination SPAN.

La sécurité des ports comporte deux modes :

- **Verrouillage classique** : toutes les adresses MAC apprises sur le port sont verrouillées et le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne sont pas sujettes au vieillissement ou au réapprentissage.
- **Limited Dynamic Lock** : le périphérique apprend les adresses MAC jusqu'à la limite configurée des adresses autorisées. Une fois la limite atteinte, le périphérique n'apprend pas d'adresses supplémentaires. Dans ce mode, les adresses sont sujettes au vieillissement et au réapprentissage.

Lorsqu'une trame d'une nouvelle adresse MAC est détectée sur un port où elle n'est pas autorisée (le port est verrouillé de façon classique et il y a une nouvelle adresse MAC, ou le port est verrouillé de façon dynamique et le nombre maximal d'adresses autorisées a été dépassé), le mécanisme de protection est appelé et l'une des actions suivantes peut avoir lieu :

- La trame est ignorée.
- La trame est transférée.
- La trame est ignorée et un message SYSLOG est généré.
- Le port est arrêté.

Lorsque l'adresse MAC sécurisée est vue sur un autre port, la trame est transférée, mais l'adresse MAC n'est pas apprise sur ce port.


Outre l'une de ces actions, vous pouvez également générer des interruptions et limiter leur fréquence et leur nombre pour éviter de surcharger les périphériques.

## Configurer la sécurité des ports

### Étape 1

Connectez-vous à l'interface utilisateur Web.

English ▾



### Cisco Business Dashboard

User Name\*

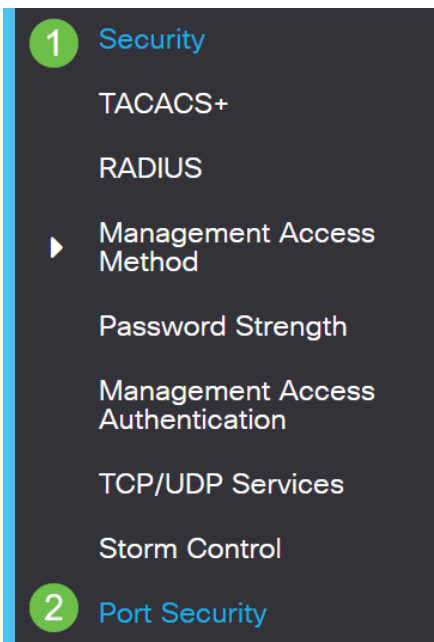
This field is required

Password\*

Login

### Étape 2

Dans le menu de gauche, sélectionnez **Security > Port Security**.



### Étape 3

Sélectionnez une interface à modifier, puis cliquez sur l'**icône de modification**.

#### Port Security Table

The screenshot shows the 'Port Security Table' with a green circle containing the number '2' and a modification icon (a document with a pencil) highlighted. Below the table title, there are two icons: a document and a pencil. The table has the following columns: Entry No., Port, Interface Status, Learning Mode, and Max No. of Address. The first row is highlighted in light blue and has a green circle with the number '1' and a selection icon (a circle with a dot) next to the 'Entry No.' value of 1.

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

### Étape 4

Saisissez les paramètres.

- **Interface** : sélectionnez le nom de l'interface.
- **Administrative Status** : sélectionnez cette option pour verrouiller le port.
- **Learning Mode** : sélectionnez le type de verrouillage de port. Pour configurer ce champ, l'état de l'interface doit être déverrouillé. Le champ Learning Mode n'est activé que si le champ Interface Status est verrouillé. Pour modifier le mode d'apprentissage, l'interface de verrouillage doit être désactivée. Une fois le mode modifié, l'interface de verrouillage peut être rétablie. Les options sont les suivantes :
  - **Classic Lock** : verrouille le port immédiatement, quel que soit le nombre d'adresses déjà acquises.
  - **Limited Dynamic Lock** : verrouille le port en supprimant les adresses MAC dynamiques actuelles associées au port. Le port apprend jusqu'aux adresses maximales autorisées sur le port. Le réapprentissage et le vieillissement des adresses MAC sont activés.
- **Max No. of Addresses Allowed** : saisissez le nombre maximal d'adresses MAC pouvant être apprises sur le port si le mode d'apprentissage Limited Dynamic Lock est sélectionné. Le nombre 0 indique que seules les adresses statiques sont prises en

charge sur l'interface.

- **Action on Violation** : sélectionnez une action à appliquer aux paquets arrivant sur un port verrouillé. Les options sont les suivantes :
  - **Discard** : rejette les paquets de toute source non apprise.
  - **Forward** : transfère les paquets d'une source inconnue sans apprendre l'adresse MAC.
  - **Discard and Log** : ignore les paquets de n'importe quelle source non apprise, arrête l'interface, consigne les événements et envoie des interruptions aux récepteurs de déroulement spécifiés
  - **Shutdown** : rejette les paquets de n'importe quelle source non apprise et arrête le port. Le port reste arrêté jusqu'à ce qu'il soit réactivé ou jusqu'au redémarrage du périphérique.
  - **Fréquence de déroulement** : saisissez le temps minimum (en secondes) qui s'écoule entre les déroulements.

Cliquez sur Apply.

## 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**

Si vous souhaitez voir un exemple de comportement par défaut pour la sécurité des ports sur votre CBS220, consultez [Comportement de sécurité des ports](#).

### Conclusion

C'est aussi simple que ça. Profitez de votre réseau sécurisé !

Pour plus de configurations, reportez-vous au [Guide d'administration des commutateurs de la gamme Cisco Business 220](#).

Si vous souhaitez consulter d'autres articles, consultez la [page d'assistance des](#)

[commutateurs Cisco Business 220.](#)