Configure Port Security on Cisco Business 220 Switches

Objective

This article explains your options for port security on your Cisco Business 220 series switch.

Applicable Devices | Firmware Version

- CBS220 series **(DataSheet)** | 2.0.0.17

Introduction

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured. Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port security cannot be enabled on ports on which 802.1X is enabled or on ports that are defined as SPAN destination.

Port Security has two modes:

- **Classic Lock**—All learned MAC addresses on the port are locked, and the port doesn't learn any new MAC addresses. The learned addresses aren't subject to aging or relearning.
- **Limited Dynamic Lock**—The device learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the device doesn't learn additional addresses. In this mode, the addresses are subject to aging and relearning.

When a frame from a new MAC address is detected on a port where it's not authorized (the port is classically locked, and there's a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded.
- Frame is forwarded.
- Frame is discarded and a SYSLOG message is generated.
- Port is shut down.

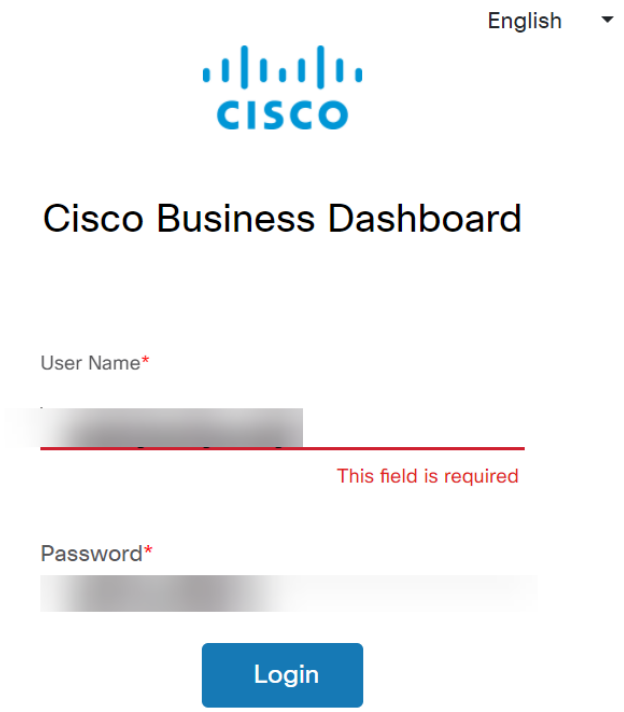
When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address isn't learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

Configure Port Security

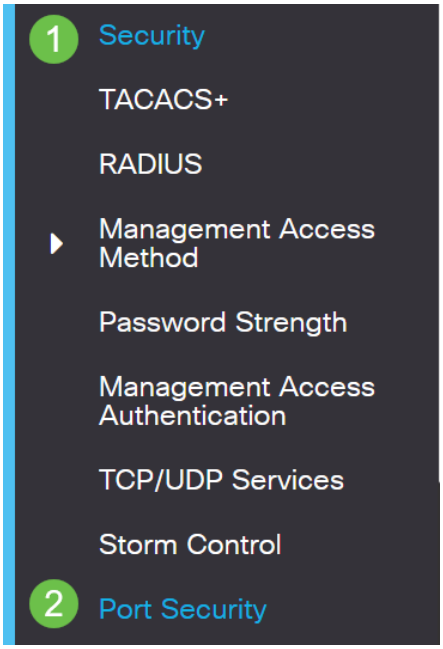
Step 1

Log into the Web User Interface (UI).



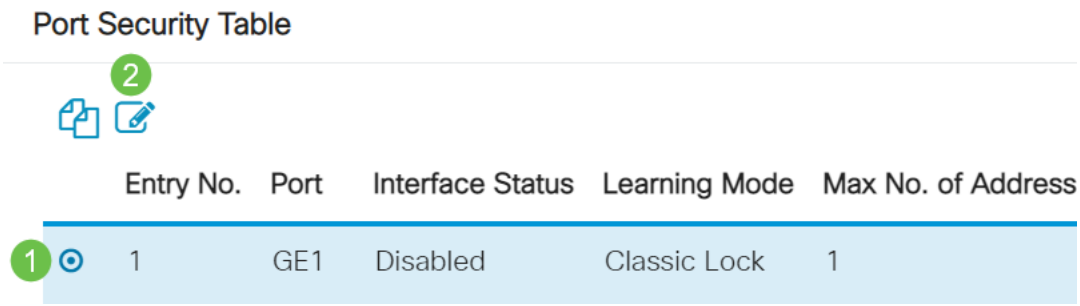
Step 2

From the menu on the left, select **Security > Port Security**.



Step 3

Select an interface to be modified and then click on the **edit icon**.



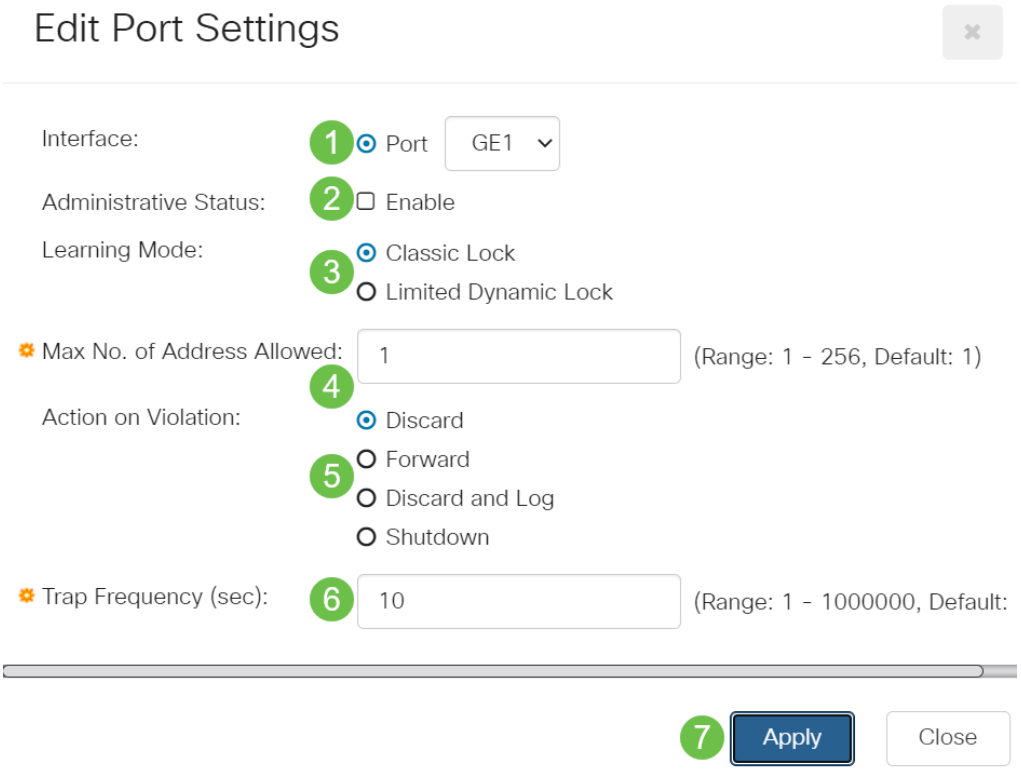
Step 4

Enter the parameters.

- **Interface**—Select the interface name.
- **Administrative Status**—Select to lock the port.
- **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the Interface Status field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
    - **Classic Lock**—Locks the port immediately, regardless of the number of addresses that have already been learned.
    - **Limited Dynamic Lock**—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging of MAC addresses are enabled.

- **Max No. of Addresses Allowed**—Enter the maximum number of MAC addresses that can be learned on the port if Limited Dynamic Lock learning mode is selected. The number 0 indicates that only static addresses are supported on the interface.
- **Action on Violation**—Select an action to be applied to packets arriving on a locked port. The options are:
    - **Discard**—Discards packets from any unlearned source •
    - **Forward**—Forwards packets from an unknown source without learning the MAC address
    - **Discard and Log**—Discards packets from any unlearned source, shuts down the interface, logs the events, and sends traps to the specified trap receivers Shutdown—Discards packets from any unlearned source, and shuts down the port. The port remains shut down until reactivated, or until the device is rebooted.
    - **Trap Frequency**—Enter minimum time (in seconds) that elapses between traps

Click **Apply**.



If you would like to see an example of the default behavior for port security on your CBS220, check out **Port Security Behavior**.

Conclusion

It is as simple as that. Enjoy your secure network!

For more configurations, refer to the **Cisco Business 220 Series Switches Administration Guide**.

If you would like to view other articles, check out the **Cisco Business 220 Series Switch Support Page**.