Port Security Behavior for CBS 250 and 350 Series Switches with Firmware 3.1

Objective

This article provides a demonstration to show changes with the default port security settings on the Cisco Business 250 and 350 Switches starting with firmware version 3.1.

Applicable Devices | Firmware Version

- CBS250 **(Data Sheet)** | 3.1 **(Download latest)**
- CBS350 **(Data Sheet)** | 3.1 **(Download latest)**
- CBS350-2X **(Data Sheet)** | 3.1 **(Download latest)**
- CBS350-4X **(Data Sheet)** | 3.1 **(Download latest)**

Introduction

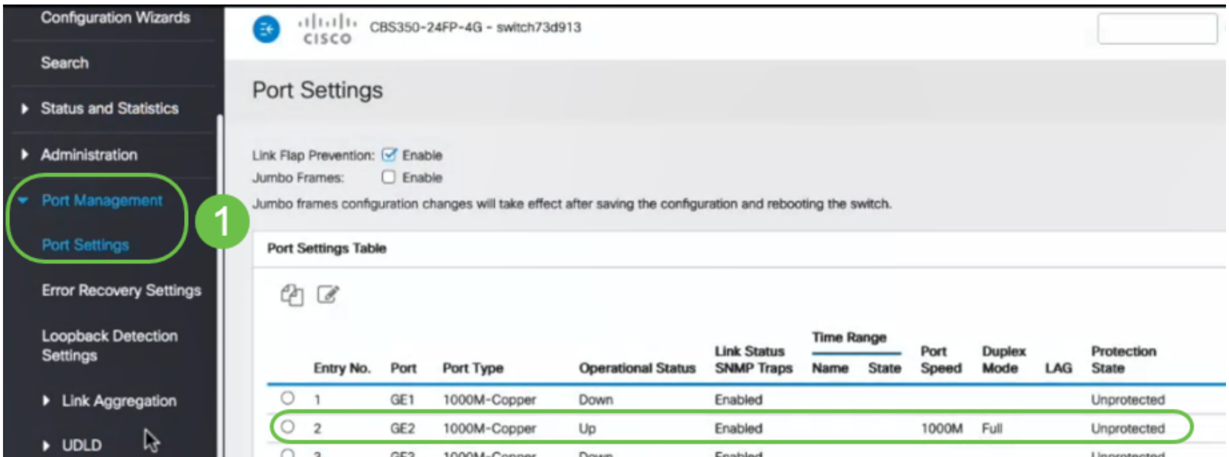
It is important to run the latest version of firmware when a new release comes out. In Spring of 2021, firmware version 3.1 for CBS 250 and 350 switches was released, changing the Port Security default behavior. These changes were made to improve endpoint security. Check out the demonstration to learn more.

Port Security Default Behavior Demonstration (Firmware version 3.1)

In this demonstration, Port Security is enabled on the GE2 interface of a Cisco Business 350 switch upgraded to firmware version 3.1. We will move a PC connected at switch port 2 (GE2) to switch port 4 (GE4) and observe the default behavior of Port Security.

Step 1

First, we navigate to **Port Management > Port Settings** and verify the PC is connected on switch port 2 (GE2) and the *Operational Status* of the port is showing *Up*.



CBS350-24FP-4G - switch73d913

Port Settings

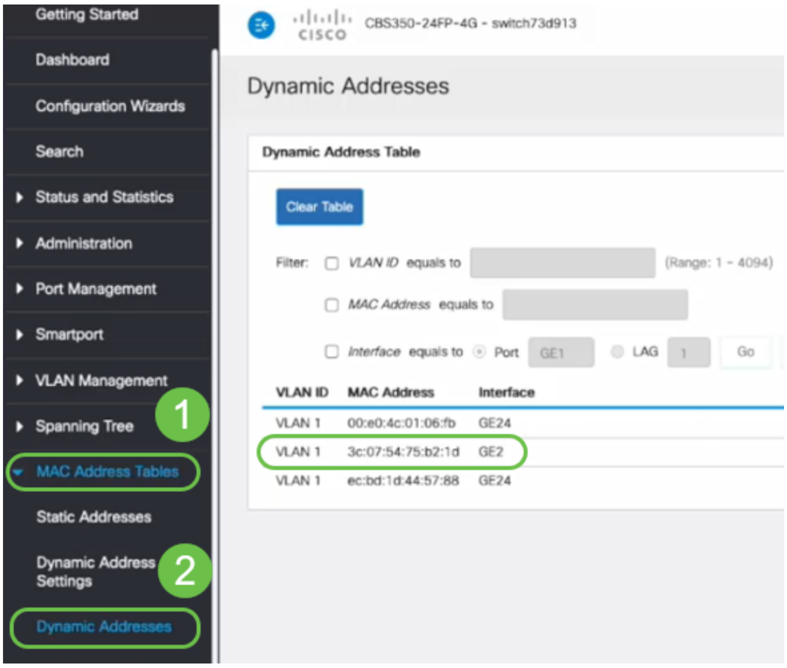
Link Flap Prevention: ☑ Enable
Jumbo Frames: ☐ Enable
Jumbo frames configuration changes will take effect after saving the configuration and rebooting the switch.

Port Settings Table

	Entry No.	Port	Port Type	Operational Status	Link Status SNMP Traps	Time Range Name	Time Range State	Port Speed	Duplex Mode	LAG	Protection State
○	1	GE1	1000M-Copper	Down	Enabled						Unprotected
○	2	GE2	1000M-Copper	Up	Enabled			1000M	Full		Unprotected
○	3	GE3	1000M-Copper	Down	Enabled						Unprotected

Step 2

Next, we navigate to **MAC Address Tables** > **Dynamic Addresses** and verify the MAC address of the PC associated to switch port 2 (GE2).



Dynamic Addresses

Dynamic Address Table

Filter: □ *VLAN ID* equals to (Range: 1 - 4094)

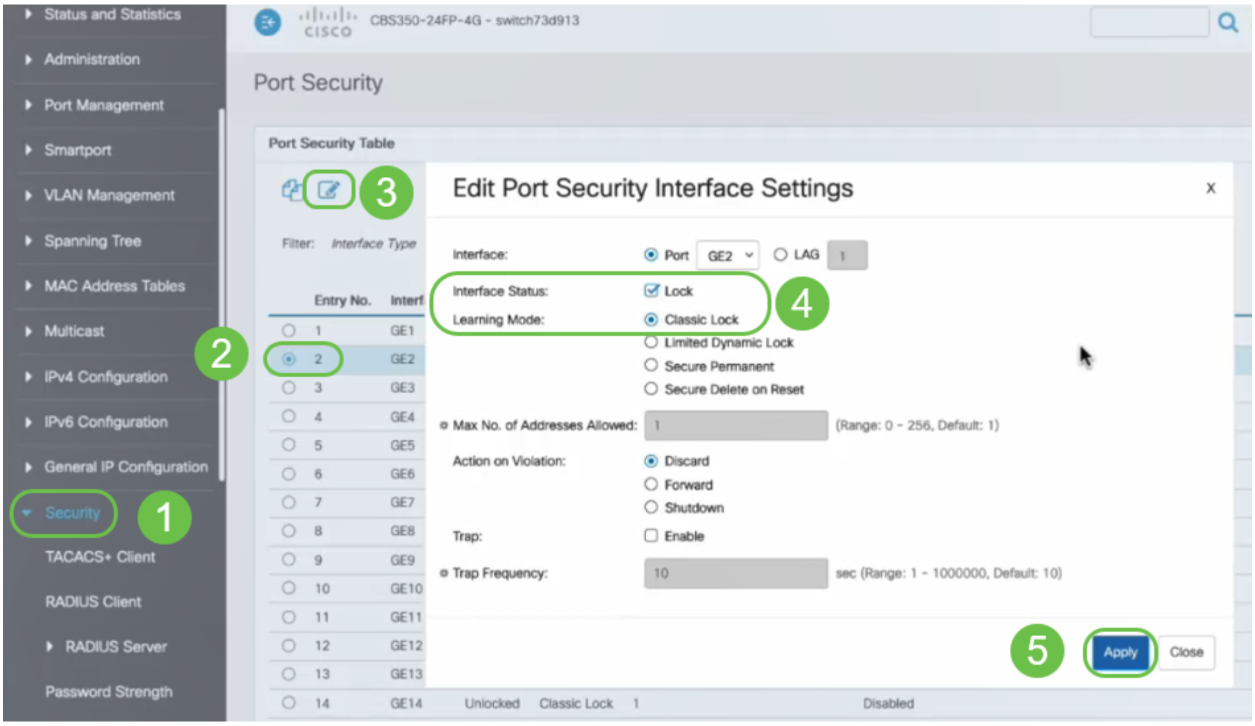
□ *MAC Address* equals to

□ *Interface* equals to ● Port GE1 ○ LAG 1

VLAN ID	MAC Address	Interface
VLAN 1	00:e0:4c:01:06:fb	GE24
VLAN 1	3c:07:54:75:b2:1d	GE2
VLAN 1	ec:bd:1d:44:57:88	GE24

Step 3

We navigate to the **Security** menu, select switch port 2 (**GE2**), and click on the **edit icon**. We enable the **Lock** option beside *Interface Status*. *Learning Mode* will be shown as **Classic Lock**. We leave *Action on Violation* as *Discard* and click **Apply**.



Port Security

Port Security Table

Filter: *Interface Type*

	Entry No.	Interf
○	1	GE1
●	2	GE2
○	3	GE3
○	4	GE4
○	5	GE5
○	6	GE6
○	7	GE7
○	8	GE8
○	9	GE9
○	10	GE10
○	11	GE11
○	12	GE12
○	13	GE13
○	14	GE14

14 GE14 Unlocked Classic Lock 1 Disabled

Edit Port Security Interface Settings

Interface: ● Port GE2 ○ LAG 1

Interface Status: ☑ Lock

Learning Mode: ● Classic Lock
○ Limited Dynamic Lock
○ Secure Permanent
○ Secure Delete on Reset

Max No. of Addresses Allowed: 1 (Range: 0 - 256, Default: 1)

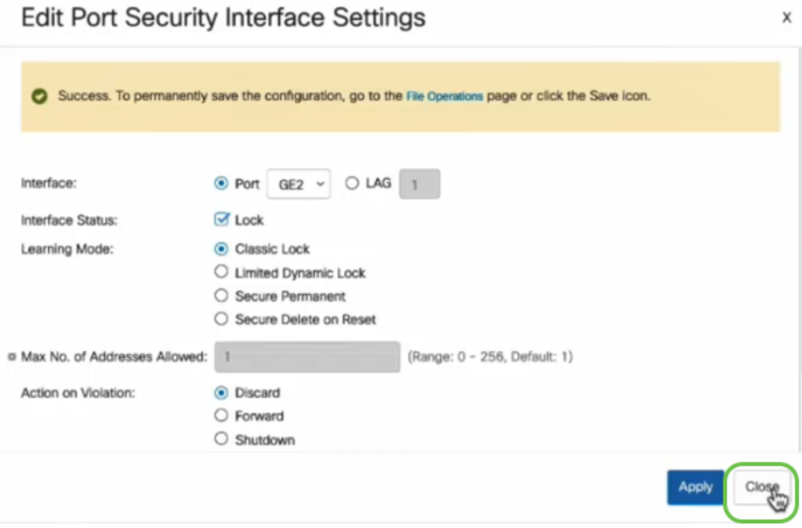
Action on Violation: ● Discard
○ Forward
○ Shutdown

Trap: □ Enable

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

Step 4

A success notification will appear on the screen, so we click **Close**.


Edit Port Security Interface Settings

Success. To permanently save the configuration, go to the File Operations page or click the Save icon.

Interface: ● Port GE2 ○ LAG 1

Interface Status: ☑ Lock

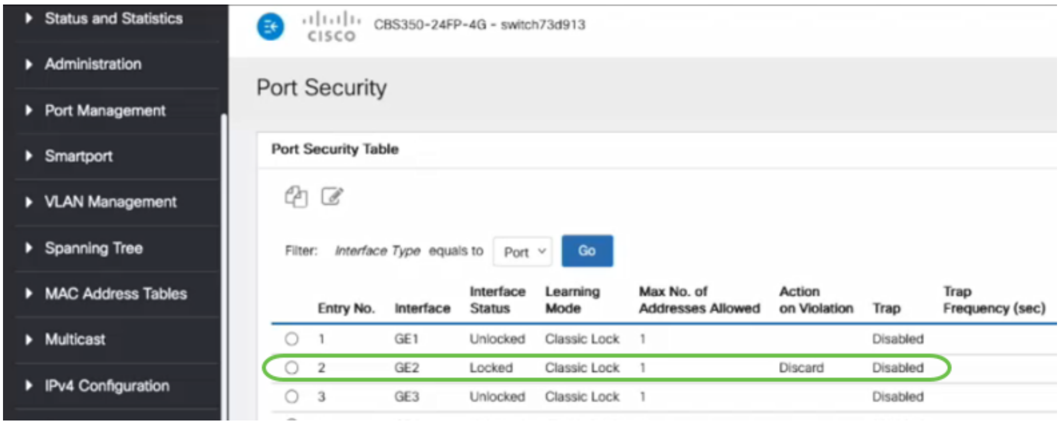
Learning Mode: ● Classic Lock ○ Limited Dynamic Lock ○ Secure Permanent ○ Secure Delete on Reset

Max No. of Addresses Allowed: 1 (Range: 0 - 256, Default: 1)

Action on Violation: ● Discard ○ Forward ○ Shutdown

Step 5

The GE2 *Interface Status* will show as *Locked*.



Port Security

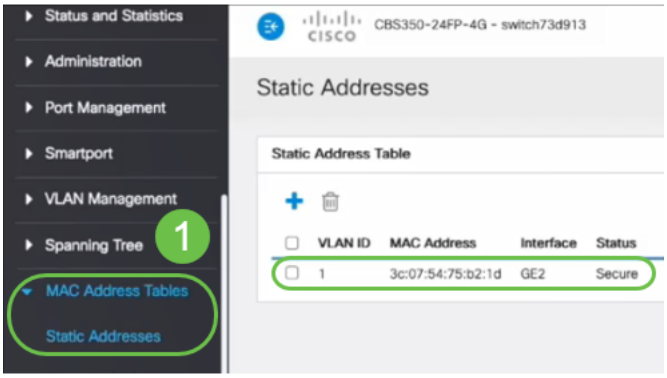
Port Security Table

Filter: *Interface Type* equals to Port Go

	Entry No.	Interface	Interface Status	Learning Mode	Max No. of Addresses Allowed	Action on Violation	Trap	Trap Frequency (sec)
○	1	GE1	Unlocked	Classic Lock	1		Disabled	
○	2	GE2	Locked	Classic Lock	1	Discard	Disabled	
○	3	GE3	Unlocked	Classic Lock	1		Disabled	

Step 6

We navigate to **MAC Address Tables > Static Addresses**. The PC MAC address associated with the GE2 interface will be reflected under the *Static Addresses* table.



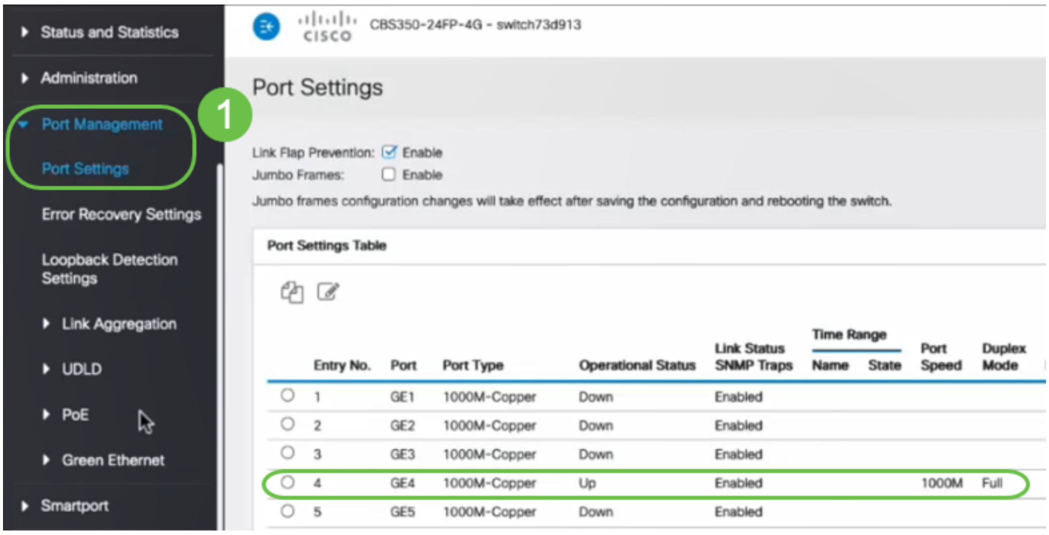
Static Addresses

Static Address Table

□	VLAN ID	MAC Address	Interface	Status
□	1	3c:07:54:75:b2:1d	GE2	Secure

Step 7

We will move the PC from switch port 2 (GE2) to switch port 4 (GE4) and make sure the *Operational Status* of the GE4 interface shows *Up*.



Port Settings

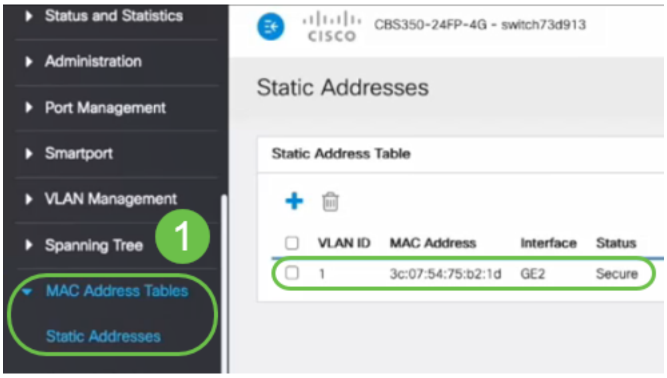
Link Flap Prevention: ☑ Enable
Jumbo Frames: □ Enable
Jumbo frames configuration changes will take effect after saving the configuration and rebooting the switch.

Port Settings Table

	Entry No.	Port	Port Type	Operational Status	Link Status SNMP Traps	Time Range Name	Time Range State	Port Speed	Duplex Mode
○	1	GE1	1000M-Copper	Down	Enabled				
○	2	GE2	1000M-Copper	Down	Enabled				
○	3	GE3	1000M-Copper	Down	Enabled				
○	4	GE4	1000M-Copper	Up	Enabled			1000M	Full
○	5	GE5	1000M-Copper	Down	Enabled				

Step 8

We navigate to **MAC Address Tables > Static Addresses**. The PC MAC address associated with the GE2 interface will still appear under the *Static Addresses* table.



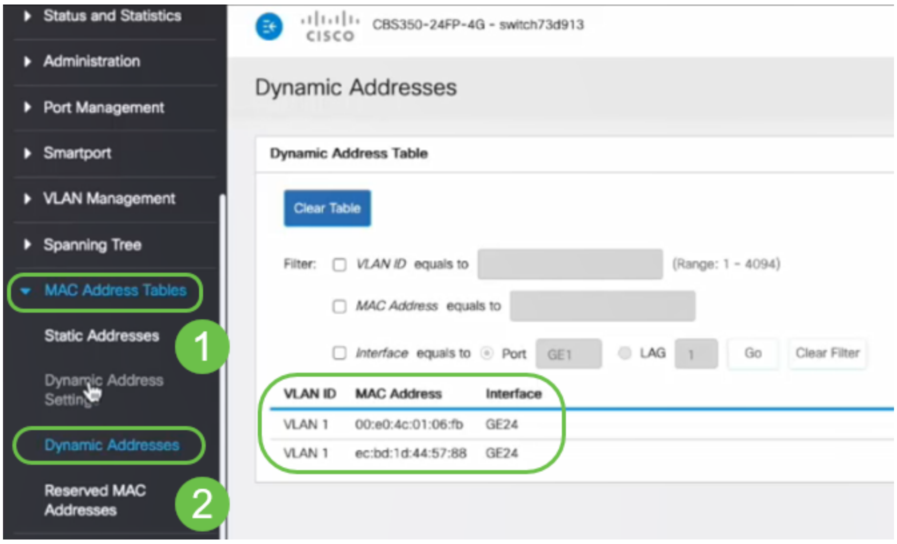
Static Addresses

Static Address Table

□	VLAN ID	MAC Address	Interface	Status
□	1	3c:07:54:75:b2:1d	GE2	Secure

Step 9

We navigate to **MAC Address Tables > Dynamic Addresses**. The PC (MAC address 3c:07:54:75:b2:1d) is connected to the GE4 interface. Even though the GE4 interface *Operational Status* is *Up*, the PC will be not able to get a Dynamic Host Configuration Protocol (DHCP) IP address. From the *Dynamic Address Table*, we can verify the same.



Dynamic Addresses

Dynamic Address Table

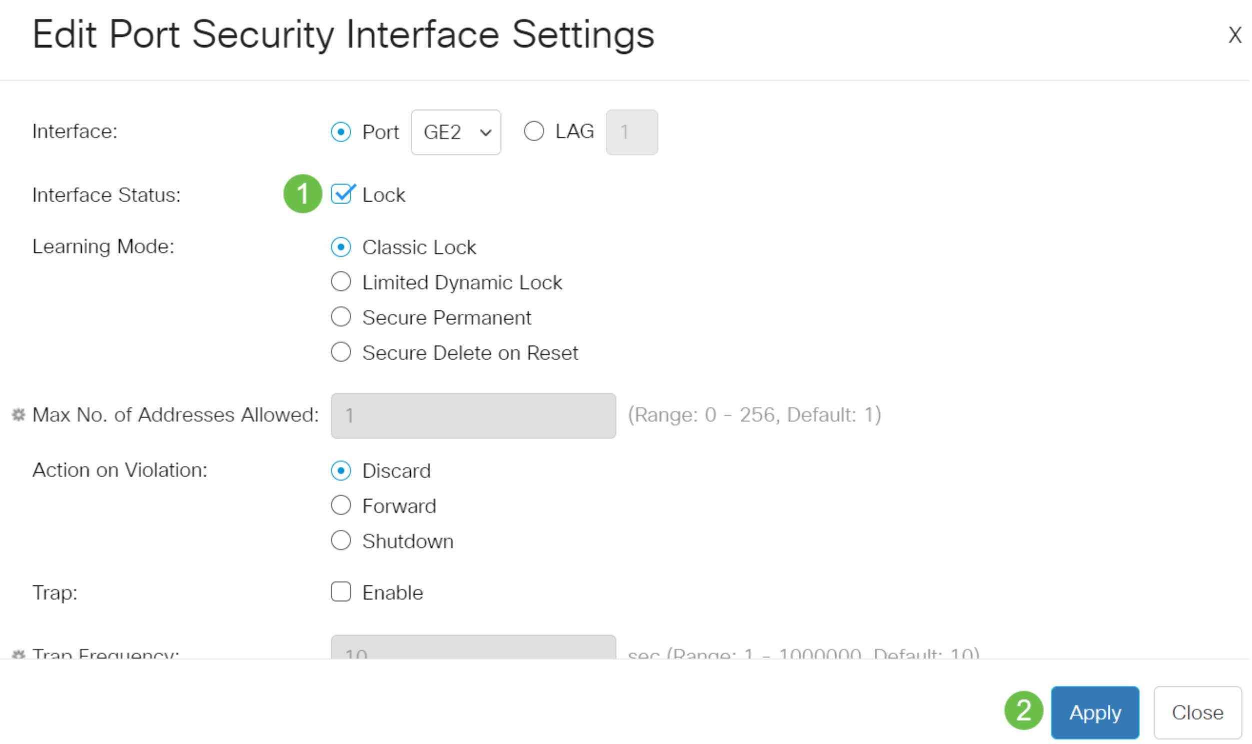
Filter: □ *VLAN ID* equals to (Range: 1 - 4094)
□ *MAC Address* equals to
□ *Interface* equals to ○ Port GE1 ○ LAG 1

VLAN ID	MAC Address	Interface
VLAN 1	00:e0:4c:01:06:fb	GE24
VLAN 1	ec:bd:1d:44:57:88	GE24

connected to the GE2 interface because the *Static Address Table* shows that MAC address binding with the GE2 interface. If we want to remove the PC MAC address from the GE2 interface so we can use it on another port, we need to unlock the port by following the optional steps that follow.

Step 10 (Optional)

We uncheck the **Lock** radio button and click **Apply**.



Edit Port Security Interface Settings

Interface: ● Port GE2 ○ LAG 1

Interface Status: 1 ☑ Lock

Learning Mode: ● Classic Lock ○ Limited Dynamic Lock ○ Secure Permanent ○ Secure Delete on Reset

Max No. of Addresses Allowed: 1 (Range: 0 - 256, Default: 1)

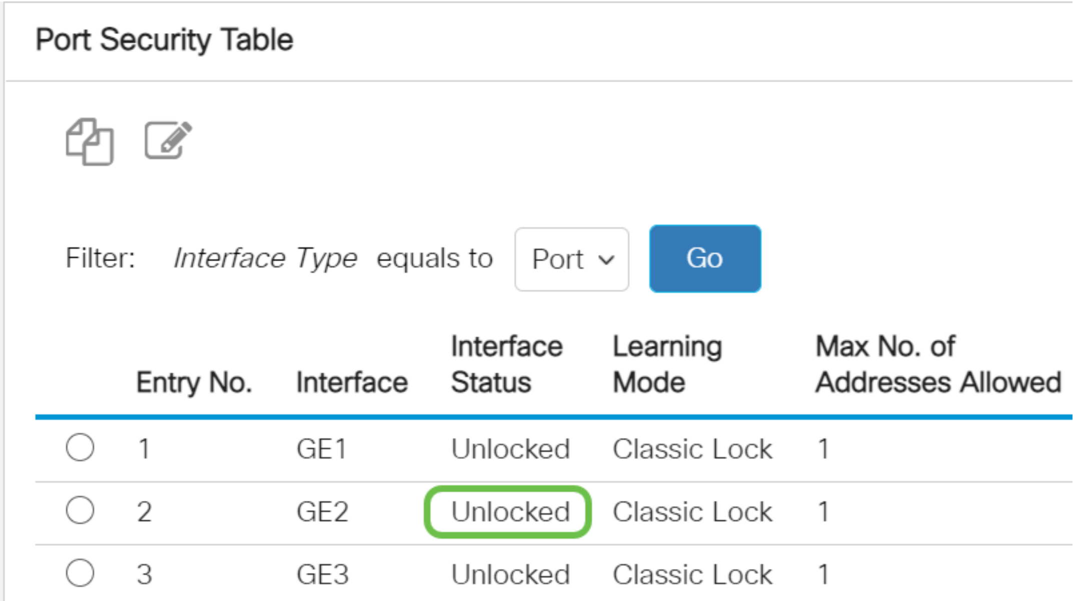
Action on Violation: ● Discard ○ Forward ○ Shutdown

Trap: □ Enable

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

Step 11 (Optional)

The *Interface Status* will now show as unlocked.



Port Security Table

Filter: *Interface Type* equals to Port

	Entry No.	Interface	Interface Status	Learning Mode	Max No. of Addresses Allowed
○	1	GE1	Unlocked	Classic Lock	1
○	2	GE2	Unlocked	Classic Lock	1
○	3	GE3	Unlocked	Classic Lock	1

Step 12

Finally, we click the **save icon** to permanently save the configuration.

Conclusion

There you go, now you know the new port security default behavior from firmware version 3.1 and beyond!

Looking for more articles on your CBS250 or CBS350 switch? Check out any of the links below for more information!

SNMP Settings **SNMP Views** **SNMP Groups** **DHCP Image Upgrade** **Password Strength** **TCP and UDP Settings** **Time Settings** **Upgrade Firmware** **Smartport Best Practices** **Troubleshoot: No IP Address** **Troubleshoot Smartports** **Troubleshoot Link Flapping** **Create VLANs**