Port Security Configuration on the 300 Series Managed Switches

Objective

Security in your network is of great importance. A secure network prevents attacks from intruders who can break into your network. One way to enhance security in your network is to configure port security. Port security allows you to configure security on a specific port or Link Aggregation Group (LAG). A LAG combines individual interfaces into a single logical link, which provides an aggregate bandwidth of up to eight physical links. You can limit or allow access to different users on a given port/LAG.

This article explains how to configure port security on the 300 Series Managed Switches.

Applicable Devices

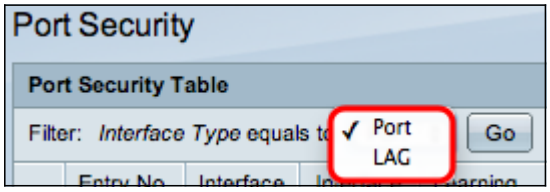
- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

Software Version

- 1.4.0.00p3 [SG300-28SFP-R]
- 6.2.10.18 [All other Applicable Devices]

Port Security Configuration

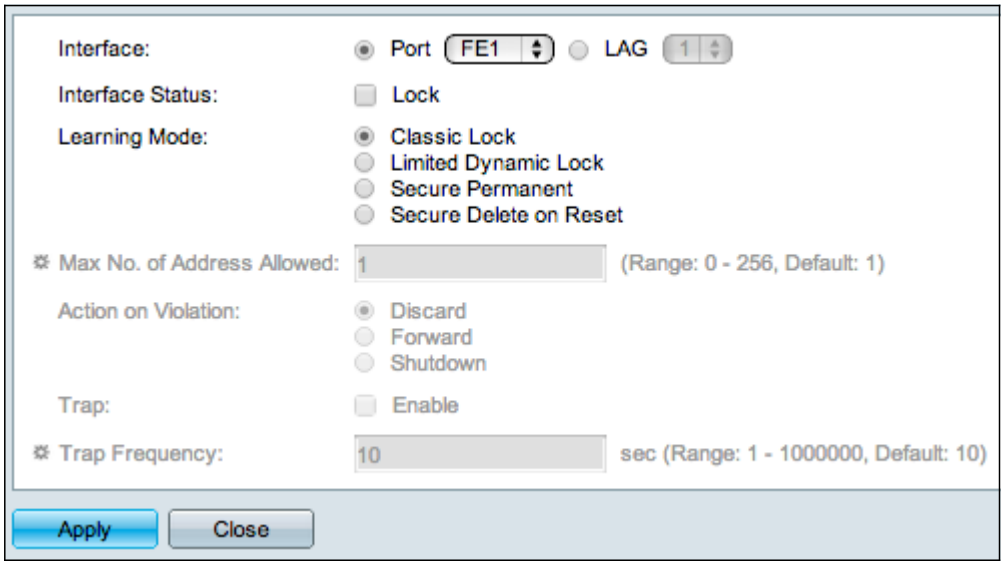
Step 1. Log in to the web configuration utility and choose **Security > Port Security**. The *Port Security* page opens:

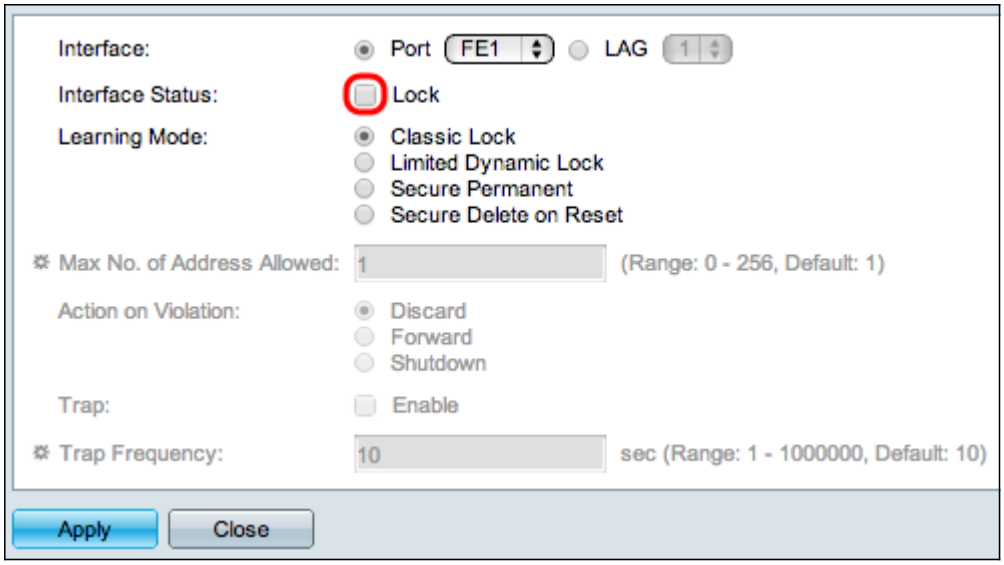


Step 2. From the Interface Type Equals drop down list, choose Port or LAG and Click **Go.**

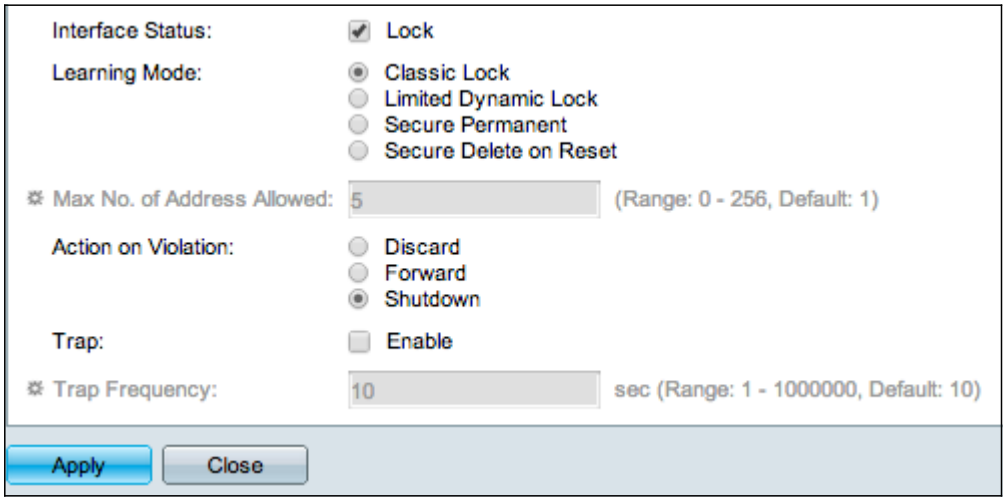
Step 3. Click the radio button of the interface for which you want to edit its security settings.

Step 4. Click **Edit**. The *Edit Port Security Interface Settings* window appears:





Step 5. (Optional) To lock the interface so it won't be able to send and receive data traffic, in the Interface Status field, check the **Lock** check box.



Step 6. In the Learning Mode field, click the radio button of the desired learning mode. The available options are:

- Classic Lock — Locks the port immediately, regardless of the number of devices that have already been learned.
- Limited Dynamic Lock — Deletes the current MAC address related to the port to lock it. The port can learn a specific amount of devices.
- Secure Permanent — Keeps the current MAC address related to the port, and can learn a specific number of of devices.
- Secure Delete on Reset — Deletes the current MAC address related to the port after reset. After the switch is reset, the port can learn a specific amount of devices.

Step 7. In the Max No. of Addresses Allowed field, enter the maximum number of MAC addresses the port is allowed to learn. If 0 is entered, then the port only supports static addresses.

Step 8. If you lock the port in Step 5, then in the Action on Violation field, click the radio button of the action to be taken when a violation occurs. The available options are:

- Discard —The packets are discarded if the source is unknown.
- Forward — The packets are forwarded if the source is unknown.
- Shutdown — The packets are discarded and the port is shut down.

Step 9. (Optional) A trap is triggered every time a packet is received on a locked port, which ensures the packet won't violate the locked port. To enable traps, check the **Enable** check box in the Trap field. Trap is a synchronous notification from agent to manager which includes current sysUpTime value, they are generated when a condition has been met on the Simple Network Management Protocol (SNMP) agent. These conditions are defined in the Management Information Base (MIB)

Step 10. If traps are enabled in Step 9, enter the minimum time in seconds between each trap in the Trap Frequency field.

Step 11. Click **Apply**.

The picture below shows the changes in the configured port.

Note: To apply the port security configuration of one port to multiple ports, refer to the section *Apply a Port Security Configuration to Multiple Ports*.

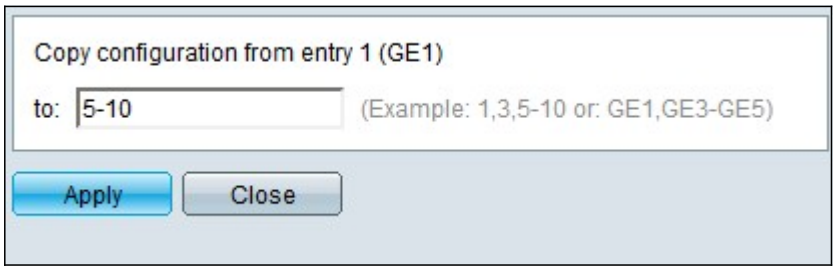
Apply a Port Security Configuration to Multiple Ports

This section explains how to apply the security port configuration of a single port, to multiple ports.

Step 1. Log in to the web configuration utility and choose **Security > Port Security**. The *Port Security* page opens:

Step 2. Click the radio button of the port which you want to apply its configuration to multiple ports.

Step 3. Click **Copy Settings**. The *Copy Settings* window appears.



Step 4. In the to field, enter the range of ports that will have the same port security

configuration of the port you chose in Step 2. You can use the port numbers or the name of the ports as input. You can enter each port separated by a comma ,such as 1, 3, 5 or GE1, GE3, GE5, or you can enter a range of ports, such as 1-5 or GE1-GE5.

Step 5. Click **Apply** to save your configuration.

The below image shows the application of a single port security configuration, to multiple ports.