

## Configuring MAC Move Limiting (J-Web Procedure)

---

MAC move limiting detects MAC address movement and MAC address spoofing on access ports. MAC address movements are tracked, and if a MAC address moves more than the configured number of times within one second, the configured (or default) action is performed. You enable this feature on VLANs.



**NOTE:** Although you enable this feature on VLANs, the MAC move limitation pertains to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, If the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not move more than once.

---

In the default configuration, the MAC move limit within each VLAN is unlimited; the default action that the switch will take if the specified MAC move limit is exceeded is **drop**.

To enable MAC move limiting for MAC addresses within one or more VLANs by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more VLANs from the **VLAN List**.
3. Click the **Edit** button. If a message appears asking whether you want to enable port security, click **Yes**.
4. To set a MAC move limit:
  1. Type a limit value in the **MAC Movement** box.
  2. Select an action from the **MAC Movement Action** box (optional). The switch takes this action when an individual MAC address exceeds the MAC move limit. If you do not select an action, the switch applies the default action, **drop**.

Select one:

- **Log**—Generate a system log entry, an SNMP trap, or an alarm.
- **Drop**—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)
- **Shutdown**—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a **disable timeout** value. See *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)* . If you have not configured autorecovery from the disabled state, you can bring up the interfaces by running the **clear ethernet-switching port-error** command.
- **None**— No action to be taken.

3. Click **OK**.
5. Click **OK** after the configuration has been successfully delivered.



**NOTE:** You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs, a message asking whether you want to enable port security appears.

- 
- Related Topics**
- Configuring MAC Move Limiting (CLI Procedure)
  - Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
  - Verifying That MAC Move Limiting Is Working Correctly
  - Monitoring Port Security
  - Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches

---

Published: 2009-07-23