Configuring Port Security (J-Web Procedure)

To configure port security on the EX-series switch using the J-Web interface:

1. From the Configure menu select the option Security > Port Security.

   The first part of the screen displays a VLAN list with the VLAN name, VLAN identifier, port members, and port security VLAN features.

   The second part of the screen displays a list of all ports and whether security features have been enabled on the ports.

2. Click one:

   - Edit — Click this option to modify the security features for the selected port or VLAN.

     Enter information as specified in Table 1 to modify Port Security settings on VLANs.

     Enter information as specified in Table 2 to modify Port Security settings on interfaces.

   - Activate/Deactivate — Click this option to enable or disable security on the switch.

Table 1: Port Security Settings on VLANs

Field	Function	Your Action
DHCP Snooping	Allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. Builds and maintains a database of valid IP addresses/MAC address bindings. (By default, access ports are untrusted and trunk ports are trusted.)	Select to enable DHCP snooping on a specified VLAN or all VLANs.
ARP Inspection	Uses information in the DHCP snooping database to validate ARP packets on the LAN and protect against ARP cache poisoning.	Select to enable ARP inspection on a specified VLAN or all VLANs. (Configure any port on which you do not want ARP inspection to occur as a trusted DHCP server port.)
MAC Movement	Prevents hosts whose MAC addresses have not been learned by the switch from accessing the network. Specifies the number of times per second that a MAC address can move to a new interface.	Enter the desired number. The default is unlimited.

Table 1: Port Security Settings on VLANs *(continued)*

Field	Function	Your Action
MAC Movement Action	Specifies the action to be taken if the MAC move limit is exceeded.	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—Block data traffic on the interface and generate an alarm. ■ None— No action to be taken.

Table 2: Port Security on Interfaces

Field	Function	Your Action
Trust DHCP	Specifies trusting DHCP packets on the selected interface. By default trunk ports are dhcp-trusted.	Select to enable DHCP trust.
MAC Limit	Specifies the number of MAC addresses that can be learned on a single Layer 2 access port. This option is not valid for trunk ports.	Enter the desired number.
MAC Limit Action	Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.	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—Block data traffic on the interface and generate an alarm. ■ None— No action to be taken.
Allowed MAC List	Specifies the MAC addresses that are allowed for the interface.	To add a MAC address: 1. Click Add. 2. Enter the MAC address. 3. Click OK.

Related Topics

- Configuring Port Security (CLI Procedure)
- Monitoring Port Security
- Port Security for EX-series Switches Overview
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch