

## interface

---

**Syntax** interface (all | *interface-name*) {  
    allowed-mac {  
        *mac-address-list*;  
    }  
    (dhcp-trusted | no-dhcp-trusted);  
    mac-limit *limit* action *action*;  
    no-allowed-mac-log;  
    static-ip *ip-address* {  
        vlan *vlan-name*;  
        mac *mac-address*;  
    }  
}

**Hierarchy Level** [edit ethernet-switching-options secure-access-port]

**Release Information** Statement introduced in JUNOS Release 9.0 for EX-series switches.  
static-ip introduced in JUNOS Release 9.2 for EX-series switches.  
no-allowed-mac-log introduced in JUNOS Release 9.3 for EX-series switches.

**Description** Apply port security features to all interfaces or to the specified interface.  
  
The statements are explained separately.

**Options** all—Apply port security features to all interfaces.

*interface-name* —Apply port security features to the specified interface.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

- Related Topics**
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
  - Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks
  - Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks
  - Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks
  - Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks
  - Configuring MAC Limiting (CLI Procedure)
  - Enabling a Trusted DHCP Server (CLI Procedure)
  - Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)

