

Enabling Dynamic ARP Inspection (J-Web Procedure)

Dynamic ARP inspection (DAI) protects EX Series switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

To enable DAI on 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 if you want to enable port security, click **Yes**.
4. Select the **Enable ARP Inspection on VLAN** check box and then click **OK**.
5. Click **OK** after the command 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 or interfaces (ports), the message asking if you want to enable port security appears.

- Related Topics**
- Enabling Dynamic ARP Inspection (CLI Procedure)
 - Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
 - Example: Configuring DHCP Snooping, DAI, and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch
 - Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
 - Verifying That DAI Is Working Correctly
 - Monitoring Port Security
 - Understanding DAI for Port Security on EX Series Switches

Published: 2009-07-23