Enabling a Trusted DHCP Server (J-Web Procedure)

You can configure any interface on the EX Series switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

You configure a trusted DHCP server on an interface, not on a VLAN. By default, all access interfaces are untrusted and all trunk interfaces are trusted.

To enable a trusted DHCP server on one or more interfaces by using the J-Web interface:

1. Select Configure>Security>Port Security.
2. Select one or more interfaces from the Port list.
3. Click the Edit button. If a message appears asking if you want to enable port security, click Yes.
4. Select the Trust DHCP 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 a Trusted DHCP Server (CLI Procedure)
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks
- Verifying That a Trusted DHCP Server Is Working Correctly
- Monitoring Port Security
- Understanding Trusted DHCP Servers for Port Security on EX Series Switches

Published: 2009-07-23