

# IP Source Guard Configuration on Sx500 Series Stackable Switches

## Objective

IP Source Guard is a security feature that can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighboring host. When IP Source Guard is enabled, the switch only transmits client IP traffic to IP addresses contained in the DHCP Snooping Binding database. If the packet that a host sends matches an entry in the database, the switch forwards the packet. If the packet does not match an entry in the database it is dropped.

In a real time scenario, one way in which IP Source Guard is used is to help prevent man-in-the-middle attacks where an untrusted third party attempts to masquerade as a genuine user. Based on the addresses which are configured in the IP source guard binding database, only the traffic from the client with that IP address is allowed and the rest of the packets are dropped.

**Note:** DHCP Snooping should be enabled for IP Source Guard to function. In order to get more details on how to enable DHCP Snooping please refer to the article *DHCP Snooping Configuration on SX500 Series Stackable Switches*. It is also necessary to configure the binding database to specify which IP addresses are allowed. More details on this can be found in the article *Configuration of DHCP Snooping Binding Database on SX500 Series Stackable Switches*.

This article explains how to configure IP Source Guard on the Sx500 Series Stackable Switches.

## Applicable Devices

- Sx500 Series Stackable Switches

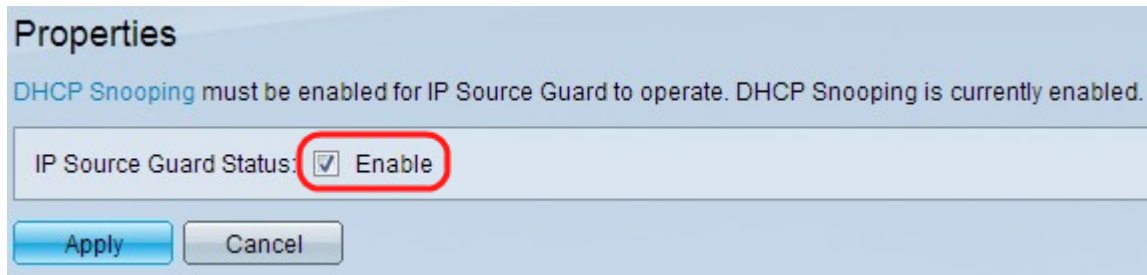
## Software Version

- v1.2.7.76

## Configure IP Source Guard Settings

### Globally Enable IP Source Guard Settings

Step 1. Log in to the web configuration utility and choose **Security > IP Source Guard > Properties**. The *IP Source Guard Properties* page opens:



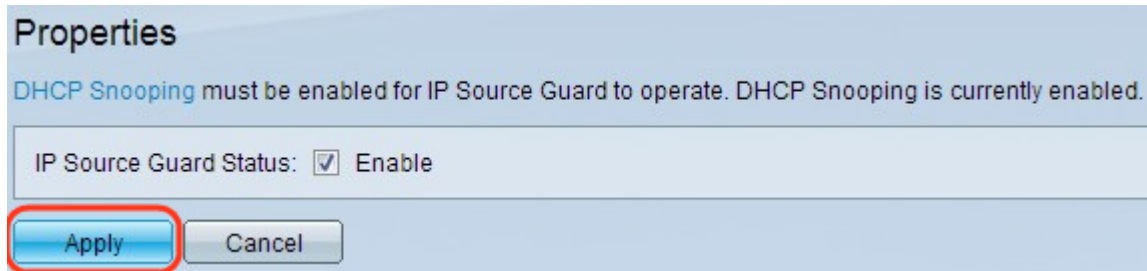
**Properties**

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: ☒ Enable

Apply Cancel

Step 2. Check the **Enable** check box to enable IP Source Guard globally.



**Properties**

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: ☒ Enable

Apply Cancel

Step 3. Click **Apply** to apply the settings.

## Edit Interface Settings for IP Source Guard

If the IP Source Guard is enabled on an untrusted port or LAG, the DHCP packets which are transmitted are allowed by the DHCP Snooping Database. If the IP address is enabled with a filter then packet transmission is allowed as follows:

- IPv4 Traffic — The IPv4 traffic which is associated with the source IP address of the particular port is allowed.
- Non IPv4 Traffic — All non-IPv4 traffic is allowed.

Step 1. Log in to the web configuration utility and choose **Security > IP Source Guard > Interface Settings**. The *Interface Settings* page opens:

### Interface Settings

DHCP Snooping must be enabled for IP Source Guard to operate. IP

#### Interface Settings Table

Filter: *Interface Type* equals to

	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Step 2. Choose an interface type from the Interface Type drop-down list and click **Go** in the Filter field.

The Interface Settings Table consists of the following parameters.

- Interface — Shows the Interface to which the IP Source Guard is applied.
- IP Source Guard — Shows whether IP Source Guard is enabled or not.
- DHCP Snooping Trusted Interface — Shows whether it is a DHCP trusted interface or not. Trusted interfaces can receive traffic only from within the network. IP Source Guard is usually configured on DHCP interfaces which are not trusted. An untrusted interface is an interface that is configured such that it can receive messages from outside the network.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to Port of Unit 1/2 <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input checked="" type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No
<input type="button" value="Copy Settings..."/> <input checked="" type="button" value="Edit..."/>				

Step 3. Click the radio button which corresponds to the interface to be edited and click **Edit** at the bottom of the page. The *Edit Interface Settings* window appears.

Interface:
☒ Unit/Slot
1/2
Port
FE1
☐ LAG
1

IP Source Guard: ☒ Enabled

Step 4. Check **Enable** in the IP Source Guard field to enable IP Source Guard on the current interface.

Interface:
☒ Unit/Slot
1/2
Port
FE1
☐ LAG
1

IP Source Guard: ☒ Enabled

Step 5. Click **Apply**. The changes are displayed.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	Yes	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No
<input type="button" value="Copy Settings..."/> <input type="button" value="Edit..."/>				

## Copy Interface Settings for IP Source Guard

Step 1. Log in to the web configuration utility and choose **Security > IP Source Guard > Interface Settings**. The *Interface Settings* page opens:

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	Yes	No
<input checked="" type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No
<input type="button" value="Copy Settings..."/> <input type="button" value="Edit..."/>				

Step 2. Click the radio button for the desired interface and click **Copy Settings**. The *Copy Settings* window appears.

Copy configuration from entry 2 (FE2)  
to:  (Example: 1,3,5-10 or FE1,FE3-FE5)

Step 3. Enter the interface(s) or range(s) of interfaces to which the chosen entry needs to be

copied and click **Apply**. The settings are applied.