Add Access Control List (ACL) to Interface Binding on Sx500 Series Stackable Switches

Objective

When an Access Control List (ACL) is bound to an interface, its Access Control Element (ACE) rules are applied to packets that arrive at that interface. Packets that do not match any of the ACEs in the Access Control List are matched to a default rule whose action is to drop unmatched packets. Even though each interface can only be bound to one ACL, multiple interfaces can be bound to the same ACL if you group them into a policy map and then bind the policy map to the interface. After an Access Control List is bound to an interface, the ACL cannot be edited, modified, or deleted until it is removed from all the ports to which it is bound. This article explains how to bind an Access Control List to an interface.

If you are unfamiliar with terms in this document, check out Cisco Business: Glossary of New Terms.

Note: Refer to the article Quality of Service (QoS) Policy Class Maps Configuration on Sx500 Series Stackable Switches for further details on policy map configuration.

Applicable Devices

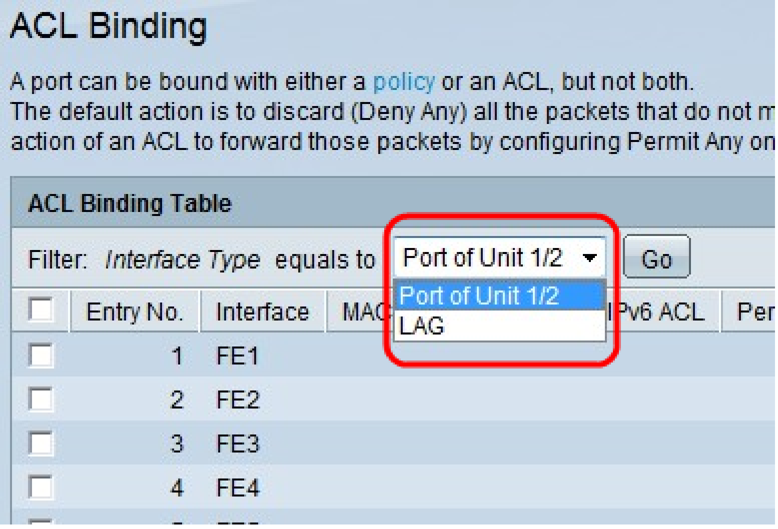
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

ACL to Interface Binding

Step 1. Log in to the Web Configuration utility and choose **Access Control > ACL Binding**. The *ACL Binding* page opens:



ACL Binding

A port can be bound with either a policy or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not m
action of an ACL to forward those packets by configuring Permit Any on

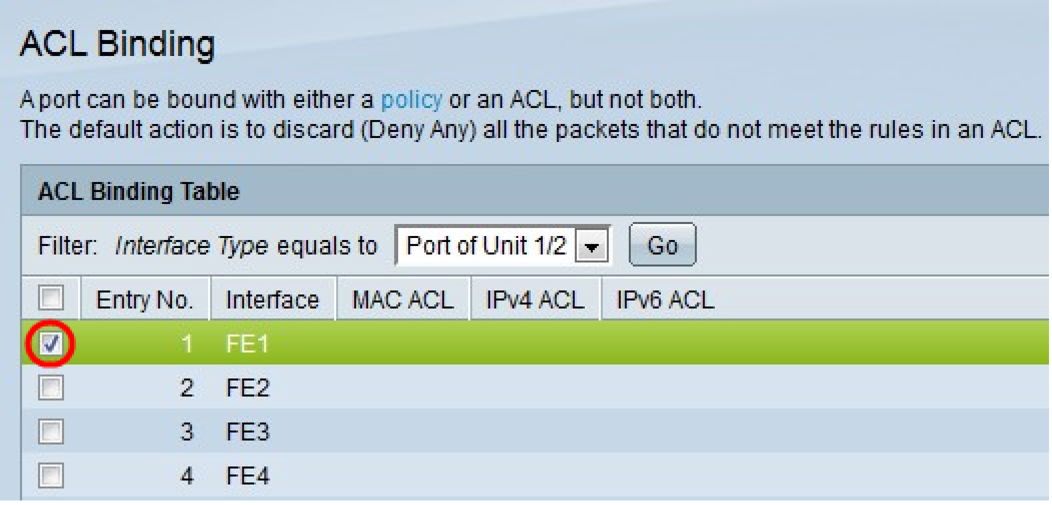
ACL Binding Table

Filter: *Interface Type* equals to Port of Unit 1/2 ▾ Go

☐	Entry No.	Interface	MAC	IPv6 ACL	Per
☐	1	FE1			
☐	2	FE2			
☐	3	FE3			
☐	4	FE4			

Step 2. In the Filter field, choose the type of interface on which you want to configure the ACL from the drop-down list and click **Go**. The possible values are either individual ports or a Link

Aggregation Group (LAG).



ACL Binding

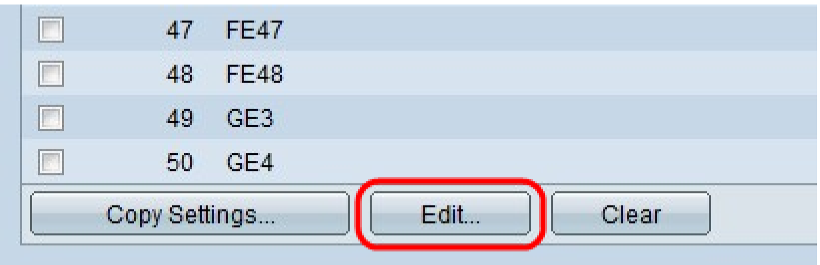
A port can be bound with either a policy or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL.

ACL Binding Table

Filter: *Interface Type* equals to Port of Unit 1/2

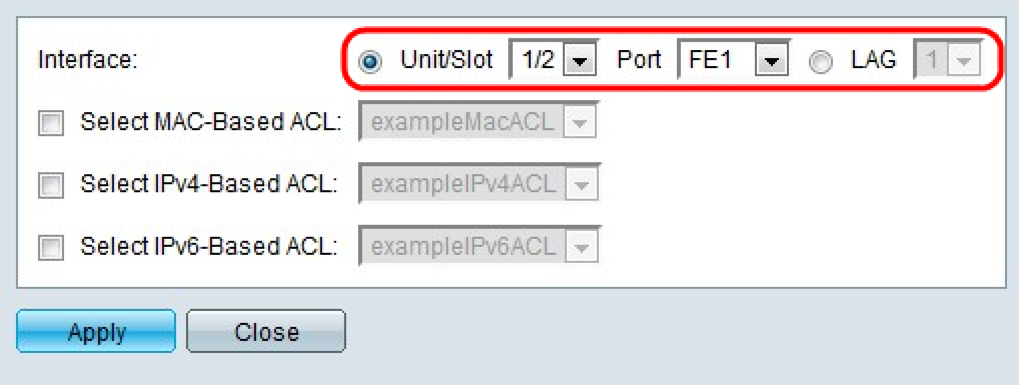
□	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL
☑	1	FE1			
□	2	FE2			
□	3	FE3			
□	4	FE4			

Step 3. Check the check box next to the desired interface.



□	47	FE47
□	48	FE48
□	49	GE3
□	50	GE4

Step 4. Click **Edit** to edit the configuration.



Interface: ● Unit/Slot 1/2 Port FE1 ○ LAG 1

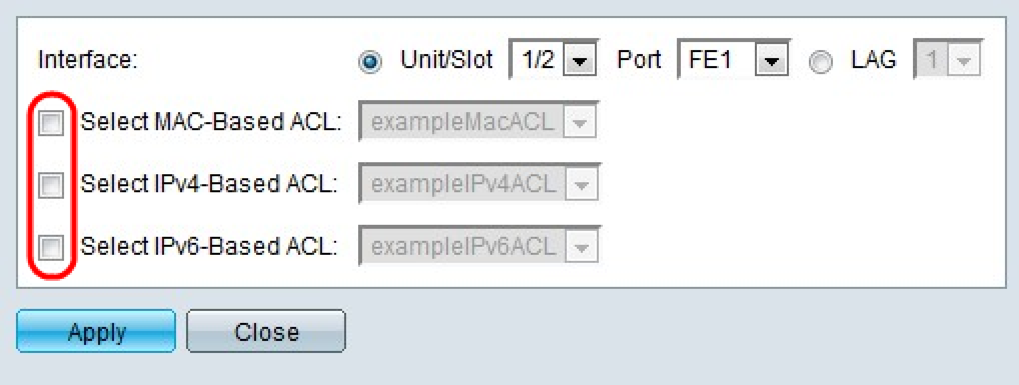
□ Select MAC-Based ACL: exampleMacACL

□ Select IPv4-Based ACL: exampleIPv4ACL

□ Select IPv6-Based ACL: exampleIPv6ACL

Step 5. (Optional) Click the radio button that corresponds to the desired interface type in the Interface field.

- Unit/Slot — From the Unit/Slot drop-down list, choose the appropriate Unit/Slot. The unit identifies whether the switch is the active or member in the stack. The slot identifies which switch is connected to which slot (slot 1 is SF500 and slot 2 is SG500).
- Port — From the Port drop-down list, choose the appropriate port to configure.
- LAG — Choose the LAG from the LAG drop-down list. A Link Aggregate Group (LAG) is used to link multiple ports together. LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices to optimize port usage.


Interface: ● Unit/Slot 1/2 Port FE1 ○ LAG 1

□ Select MAC-Based ACL: exampleMacACL

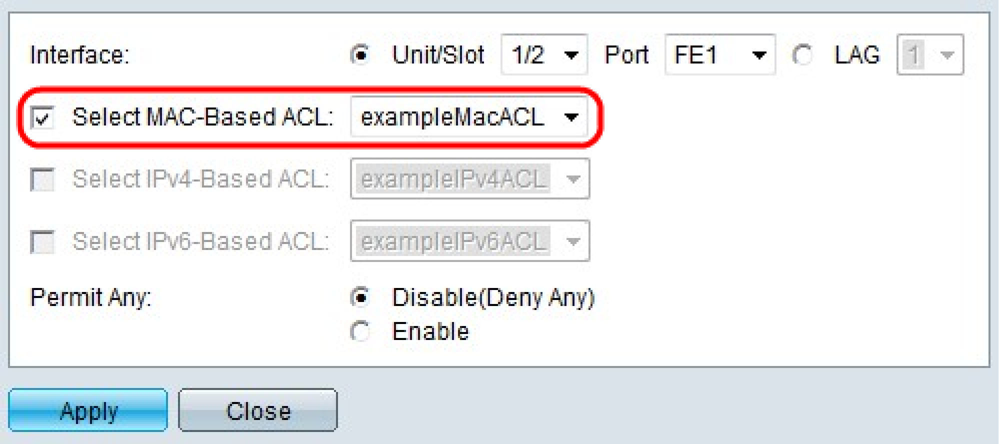
□ Select IPv4-Based ACL: exampleIPv4ACL

□ Select IPv6-Based ACL: exampleIPv6ACL

Step 6. Check the check box(es) next to the desired option(s) for binding:

- Select MAC Based ACL — Choose a MAC-based ACL to be bound to the interface. Refer to the article entitled *Configuration of MAC Based ACLs and ACEs on Sx500 Series Stackable Switches* for further details on MAC-based ACL configuration.
- Select IPv4 Based ACL — Choose a IPv4-based ACL to be bound to the interface. Refer to the article entitled *Configuration of IPv4-Based Access Control Lists (ACL) and Access Control Entries (ACE) on Sx500 Series Stackable Switches* for further details on IPv4-based ACL configuration.
- Select IPv6 Based ACL — Choose a IPv6-based ACL to be bound to the interface. Refer to the article entitled *Configuration of IPv6-Based Access Control Lists (ACL) and Access Control Entries (ACE) on Sx500 Series Stackable Switches* for further details on IPv6-based ACL configuration.

Note: IP Source Guard should not be activated on the interface if Permit Any needs to be defined.


Interface: ● Unit/Slot 1/2 Port FE1 ○ LAG 1

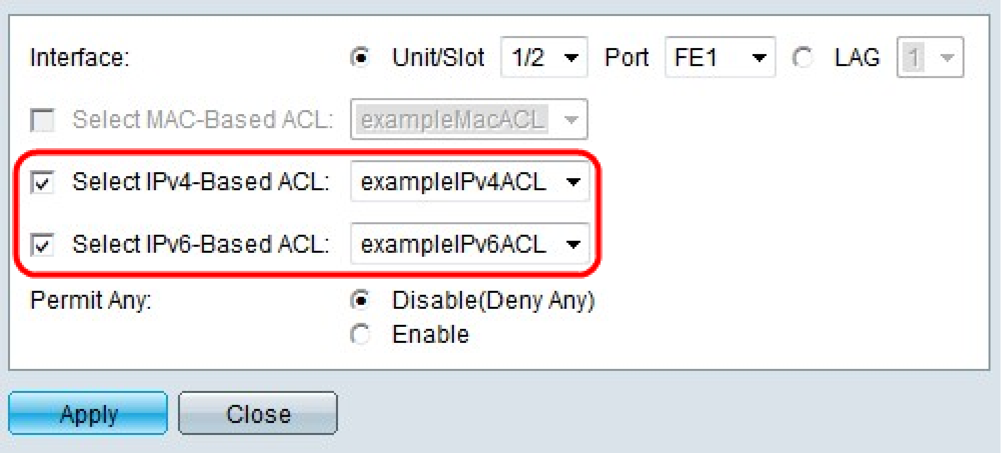
☑ Select MAC-Based ACL: exampleMacACL

□ Select IPv4-Based ACL: exampleIPv4ACL

□ Select IPv6-Based ACL: exampleIPv6ACL

Permit Any: ● Disable(Deny Any) ○ Enable

Step 7. If you chose to check Select MAC Based ACL in Step 6, choose the ACL you would like to bind the interface to from the respective MAC based-ACL drop-down list.



Interface: ● Unit/Slot 1/2 Port FE1 ○ LAG 1

□ Select MAC-Based ACL: exampleMacACL

☑ Select IPv4-Based ACL: exampleIPv4ACL

☑ Select IPv6-Based ACL: exampleIPv6ACL

Permit Any: ● Disable(Deny Any)
○ Enable

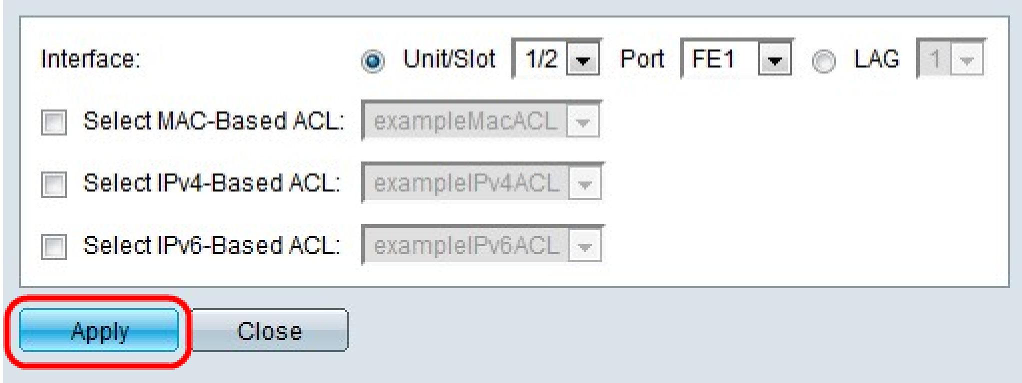
Step 8. If you chose to check Select IPv4-Based ACL in Step 6, choose the ACL you would like to bind the interface to from the respective IPv4 based-ACL drop-down list.

Step 9. If you chose to check Select IPv6-Based ACL in Step 6, choose the ACL you would like to bind the interface to from the respective IPv6 based-ACL drop-down list.

Note: You can have both an IPv4-Based ACL and an IPv6-Based ACL binding on the same interface. However, you cannot have both a MAC-Based ACL and an IPv4 or IPv6-Based ACL on the same interface.

Step 10. Click one of the following options in the Permit Any field:

- Disable (Deny Any) — Packet is denied if it does not match the ACL.
- Enable — Packet is forwarded even if it does not match the ACL.



Interface: ● Unit/Slot 1/2 Port FE1 ○ LAG 1

□ Select MAC-Based ACL: exampleMacACL

□ Select IPv4-Based ACL: exampleIPv4ACL

□ Select IPv6-Based ACL: exampleIPv6ACL

Step 11. Click **Apply**.