



Aggregate Interfaces and LACP

The following topics explain aggregate interface configuration and how LACP functions on managed devices:

- [About Aggregate Interfaces, on page 1](#)
- [LAG Configuration, on page 2](#)
- [Link Aggregation Control Protocol \(LACP\), on page 6](#)
- [Adding Aggregate Switched Interfaces, on page 7](#)
- [Adding Aggregate Routed Interfaces, on page 9](#)
- [Adding Logical Aggregate Interfaces, on page 12](#)
- [Viewing Aggregate Interface Statistics, on page 13](#)
- [Deleting Aggregate Interfaces, on page 13](#)

About Aggregate Interfaces

In the Firepower System, you can group multiple physical Ethernet interfaces into a single logical link on managed devices configured in either a Layer 2 deployment that provides packet switching between networks, or a Layer 3 deployment that routes traffic between interfaces. This single aggregate logical link provides higher bandwidth, redundancy, and load-balancing between two endpoints.

You create aggregate links by creating a switched or routed link aggregation group, or LAG. When you create an aggregation group, a logical interface called an aggregate interface is created. To an upper layer entity a LAG looks like a single logical link and data traffic is transmitted through the aggregate interface. The aggregate link provides increased bandwidth by adding the bandwidth of multiple links together. It also provides redundancy by load-balancing traffic across all available links. If one link fails, the system automatically load-balances traffic across all remaining links.



The endpoints in a LAG can be two 7000 or 8000 Series devices, as shown in the illustration above, or a 7000 or 8000 Series device connected to a third-party access switch or router. The two devices do not have to match, but they must have the same physical configuration and they must support the IEEE 802.ad link aggregation standard. A typical deployment for a LAG might be to aggregate access links between two managed devices, or to create a point-to-point connection between a managed device and an access switch or a router.

Note that you cannot configure aggregate interfaces on NGIPSv devices or ASA FirePOWER modules.

LAG Configuration

There are two types of aggregate interfaces:

- switched — Layer 2 aggregate interfaces
- routed — Layer 3 aggregate interfaces

You implement link aggregation through the use of link aggregation groups (LAGs). You configure a LAG by creating an aggregate switched or routed interface and then associating a set of physical interfaces with the link. All of the physical interfaces must be of the same speed and medium.

You create aggregate links either dynamically or statically. Dynamic link aggregation uses Link Aggregation Control Protocol (LACP), a component of the IEEE 802.3ad link aggregation standard, while static link aggregation does not. LACP enables each device on either end of the LAG to exchange link and system information to determine which links will be actively used in the aggregation. A static LAG configuration requires you to manually maintain link aggregations and deploy load-balancing and link selection policies.

When you create a switched or routed aggregate interface, a link aggregation group of the same type is created and numbered automatically. For example, when you create your first LAG (switched or routed), the aggregate interface can be identified by the **lag0** label in the **Interfaces** tab for your managed device. When you associate physical and logical interfaces with this LAG, they appear nested below the primary LAG in a hierarchical tree menu. Note that a switched LAG can only contain switched physical interfaces, and a routed LAG can only contain routed physical interfaces.

Consider the following requirements when you configure a LAG:

- The Firepower System supports a maximum of 14 LAGs, and assigns a unique ID to each LAG interface in the range of 0 to 13. The LAG ID is not configurable.
- You must configure the LAG on both sides of the link, and you must set the interfaces on either side of the link to the same speed.
- You must associate at least two physical interfaces per LAG, up to a maximum of eight. A physical interface cannot belong to more than one LAG.
- Physical interfaces in a LAG cannot be used in any other mode of operation, either as inline or passive, or be used as part of another logical interface for tagged traffic.
- Physical interfaces in a LAG can span multiple NetMods, but cannot span multiple sensors (i.e. all physical interfaces must reside on the same device).
- A LAG cannot contain a stacking NetMod.

Aggregate Switched Interfaces

You can combine between two and eight physical ports on a managed device to create a switched LAG interface. You must assign a switched LAG interface to a virtual switch before it can handle traffic. A managed device can support up to 14 LAG interfaces.

The range of MTU values can vary depending on the model of the managed device and the interface type.

**Caution**

Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

Related Topics

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)
[Snort® Restart Scenarios](#)

Aggregate Routed Interfaces

You can combine between two and eight physical ports on a 7000 or 8000 Series device to create a routed LAG interface. You must assign a routed LAG interface to a virtual router before it can route traffic. A managed device can support up to 14 LAG interfaces.

You can add static Address Resolution Protocol (ARP) entries to a routed LAG interface. If an external host needs to know the MAC address of the destination IP address it needs to send traffic to on your local network, it sends an ARP request. When you configure static ARP entries, the virtual router responds with an IP address and associated MAC address.

Disabling the **ICMP Enable Responses** option for routed LAG interfaces does not prevent ICMP responses in all scenarios. You can still use access control rules to handle connections where the destination IP is the routed interface's IP and the protocol is ICMP; see [Port and ICMP Code Conditions](#).

If you enable the **Inspect Local Router Traffic** option, the system blocks packets before they reach the host, thereby preventing any response. For more information about inspecting local router traffic, see [Advanced Settings](#).

The range of MTU values can vary depending on the model of the managed device and the interface type.

**Caution**

Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

Related Topics

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)
[Snort® Restart Scenarios](#)

Logical Aggregate Interfaces

For each switched or routed aggregate interface, you can add multiple logical interfaces. You must associate each logical LAG interface with a VLAN tag to handle traffic received by the LAG interface with that specific tag. You add logical interfaces to switched or routed aggregate interfaces in the same way you would add them to physical switched or routed interfaces.



Note When you create a LAG interface you also create an “untagged” logical interface by default, which is identified by the **lag n .0** label, where n is an integer from 0 to 13. To be operational, each LAG requires this one logical interface at a minimum. You can associate additional logical interfaces with any LAG to handle VLAN-tagged traffic. Each additional logical interface requires a unique VLAN tag. The Firepower System supports VLAN tags in the range of 1 through 4094.

You can also configure the Cisco Redundancy Protocol (SFRP) on a logical routed interface. SFRP allows devices to act as redundant gateways for specified IP addresses.

Note that disabling the **ICMP Enable Responses** option for logical routed interfaces does not prevent ICMP responses in all scenarios. You can add network-based rules to an access control policy to drop packets where the destination IP is the routed interface’s IP and the protocol is ICMP.

If you have enabled the **Inspect Local Router Traffic** option, which is an advanced setting on the managed device, it drops the packets before they reach the host, thereby preventing any response.

The range of MTU values can vary depending on the model of the managed device and the interface type.



Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

Related Topics

[SFRP](#)

[Advanced Settings](#)

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)

[Snort® Restart Scenarios](#)

Load-Balancing Algorithms

You assign an egress load-balancing algorithm to the LAG that determines how to distribute traffic to the LAG bundle’s member links. The load-balancing algorithm makes hashing decisions based on values in various packet fields, such as Layer 2 MAC addresses, Layer 3 IP addresses, and Layer 4 port numbers (TCP/UDP traffic). The load-balancing algorithm you select applies to all of the LAG bundle’s member links.

Choose the load-balancing algorithm that supports your deployment scenario from the following options when you configure a LAG:

- Destination IP
- Destination MAC
- Destination Port
- Source IP
- Source MAC

- Source Port
- Source and Destination IP
- Source and Destination MAC
- Source and Destination Port



Note You should configure both ends of the LAG to have the same load-balancing algorithm. Higher layer algorithms will back off to lower layer algorithms as necessary (such as a Layer 4 algorithm backing off to Layer 3 for ICMP traffic).

Link Selection Policies

Link aggregation requires the speed and medium of each link to be the same at both endpoints. Because link properties can change dynamically, the link selection policy helps determine how the system manages the link selection process. A link selection policy that maximizes the highest port count supports link redundancy, while a link selection policy that maximizes total bandwidth supports overall link speed. A stable link selection policy attempts to minimize excessive changes in link states.



Note You should configure both ends of the LAG to have the same link selection policy.

Choose the link selection policy that supports your deployment scenario from the following options:

- Highest Port Count — Choose this option for the highest total active port count to provide added redundancy.
- Highest Total Bandwidth — Choose this option to provide the highest total bandwidth for the aggregated link.
- Stable — Choose this option if your primary concern is link stability and reliability. Once you configure a LAG, the active links change only when absolutely necessary (such as link failure) rather than doing so for added port count or bandwidth.
- LACP Priority — Choose this option to use the LACP algorithm to determine which links are active in the LAG. This setting is appropriate if you have undefined deployment goals, or if the device at the other end of the LAG is not managed by the Firepower Management Center.

LACP is a key aspect of automating the link selection method that supports dynamic link aggregation. When LACP is enabled, a link selection policy based on LACP priority uses the following properties of LACP:

LACP system priority

You configure this value on each partnered device running LACP to determine which one is superior in link aggregation. The system with the lower value has the higher system priority. In dynamic link aggregation, the system with the higher LACP system priority sets the selected state of member links on its side first, then the system with the lower priority sets its member links accordingly. You can specify 0 to 65535. If you do not specify a value, the default priority is 32768.

LACP link priority

You configure this value on each link belonging to the aggregation group. The link priority determines the active and standby links in the LAG. Links with lower values have higher priority. If an active link goes down, the standby link with the highest priority is selected to replace the downed link. However, if two or more links have the same LACP link priority, the link with the lowest physical port number is selected as the standby link. You can specify 0 to 65535. If you do not specify a value, the default priority is 32768.

Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP), a component of IEEE 802.3ad, is a method of exchanging system and port information to create and maintain LAG bundles. When you enable LACP, each device on either end of the LAG uses LACP to determine which links will be actively used in the aggregation. LACP provides availability and redundancy by exchanging LACP packets (or control messages) between links. It learns the capabilities of the links dynamically and informs the other links. Once LACP identifies correctly matched links, it facilitates grouping the links into the LAG. If a link fails, traffic continues on the remaining links. LACP must be enabled at both ends of the LAG for the link to be operational.

LACP

When you enable LACP, you need to specify a transmission mode for each end of the LAG that determines how LACP packets are exchanged between partnered devices. There are two options for LACP mode:

- Active — Choose this mode to place a device into an active negotiating state, in which the device initiates negotiations with remote links by sending LACP packets.
- Passive — Choose this mode to place a device into a passive negotiating state, in which the device responds to LACP packets it receives but does not initiate LACP negotiation.



Note Both modes allow LACP to negotiate between links to determine if they can form a link bundle based on criteria such as port speed. However, you should avoid a passive-passive configuration, which essentially places both ends of the LAG in listening mode.

LACP has a timer which defines how often LACP packets are sent between devices. LACP exchanges packets at these rates:

- Slow — 30 seconds
- Fast — 1 second

The device where this option is applied expects to receive LACP packets with this frequency from the partner device on the other side of the LAG.




Note When a LAG is configured on a managed device that is part of a device stack, only the primary device participates in LACP communication with the partner system. All secondary devices forward LACP messages to the primary device. The primary device relays any dynamic LAG modifications to the secondary devices.

Adding Aggregate Switched Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can combine between two and eight physical ports on a managed device to create a switched LAG interface. You must assign a switched LAG interface to a virtual switch before it can handle traffic. A managed device can support up to 14 LAG interfaces.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Click **Edit** () next to the device where you want to configure the switched LAG interface.
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Choose **Add Aggregate Interface** from the **Add** drop-down menu.
- Step 4** Click **Switched** to display the switched LAG interface options.
- Step 5** If you want to apply a security zone, do one of the following:
 - Choose an existing security zone from the **Security Zone** drop-down list.
 - Choose **New** to add a new security zone; see [Creating Security Zone and Interface Group Objects](#).
- Step 6** Specify a virtual switch:
 - Choose an existing virtual switch from the **Virtual Switch** drop-down list.
 - Choose **New** to add a new virtual switch; see [Adding Virtual Switches](#).
- Step 7** Check the **Enabled** check box to allow the switched LAG interface to handle traffic.
If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.
- Step 8** From the **Mode**, choose an option to designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to auto negotiate speed and duplex settings.
Mode settings are available only for copper interfaces.
Interfaces on 8000 Series appliances do not support half-duplex options. When links auto negotiate speed, all active links are selected for the LAG based on the same speed setting.
- Step 9** From the **MDI/MDIX** drop-down list, choose an option to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

MDI/MDIX settings are available only for copper interfaces.

By default, MDI/MDIX is set to Auto-MDIX, which automatically handles switching between MDI and MDIX to attain link.

- Step 10** Enter a maximum transmission unit (MTU) in the **MTU** field.
- The range within which you can set the MTU can vary depending on the Firepower System device model and interface type. See [MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#) for more information.
- Step 11** Under **Link Aggregation**, choose one or more physical interfaces from **Available Interfaces** to add to the LAG bundle.
- Tip** To remove physical interfaces from the LAG bundle, choose one or more physical interfaces and click the **Remove Selected icon**. To remove all physical interfaces from the LAG bundle, click the **Remove All icon**. Deleting the LAG interface from the Interfaces tab also removes the interfaces.
- Step 12** Choose an option from the **Load-Balancing Algorithm** drop-down list.
- Step 13** Choose a **Link Selection Policy** from the drop-down list.
- Tip** Choose **LACP Priority** if you are configuring an aggregate interface between a Firepower System device and a third-party network device.
- Step 14** If you chose **LACP Priority** as the **Link Selection Policy**, assign a value for **System Priority** and click the **Configure Interface Priority** link to assign a priority value for each interface in the LAG.
- Step 15** Choose either **Inner** or **Outer** from the **Tunnel Level** drop-down list.
- Note** The tunnel level only applies to IPv4 traffic when Layer 3 load balancing is configured. The outer tunnel is always used for Layer 2 and IPv6 traffic. If the **Tunnel Level** is not explicitly set, the default is **Outer**.
- Step 16** Under **LACP**, check the **Enabled** check box to allow the switched LAG interface to handle traffic using the Link Aggregation Control Protocol.
- If you clear the check box, the LAG interface becomes a static configuration and the Firepower System will use all of the physical interfaces selected for the aggregation.
- Step 17** Click a **Rate** radio button to set the frequency that determines how often LACP control messages are received from the partner device:
- Click **Slow** to receive packets every 30 seconds.
 - Click **Fast** to receive packets every 1 second.
- Step 18** Click a **Mode** radio button to establish the listening mode of the device:
- Click **Active** to initiate negotiations with remote links by sending LACP packets to the partner device.
 - Click **Passive** to respond to LACP packets received.
- Step 19** Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)
[Snort® Restart Scenarios](#)

Adding Aggregate Routed Interfaces


Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can combine between two and eight physical ports on a managed device to create a routed LAG interface. You must assign a routed LAG interface to a virtual router before it can route traffic. A managed device can support up to 14 LAG interfaces.



Caution Adding a routed interface pair on 7000 or 8000 Series devices restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Click **Edit** () next to the device where you want to configure the routed LAG interface.
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Choose **Add Aggregate Interface** from the **Add** drop-down menu.
- Step 4** Click **Routed** to display the routed LAG interface options.
- Step 5** If you want to apply a security zone, do one of the following:
 - Choose an existing security zone from the **Security Zone** drop-down list.
 - Choose **New** to add a new security zone; see [Creating Security Zone and Interface Group Objects](#).
- Step 6** Specify a virtual router:
 - Choose an existing virtual router from the **Virtual Router** drop-down list.
 - Choose **New** to add a new virtual router; [Adding Virtual Routers](#).
- Step 7** Check the **Enabled** check box to allow the routed LAG interface to handle traffic.
If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.
- Step 8** From the **Mode** drop-down list, choose an option to designate the link mode, or choose **Autonegotiation** to specify that the LAG interface is configured to auto negotiate speed and duplex settings.
Mode settings are available only for copper interfaces.

Interfaces on 8000 Series appliances do not support half-duplex options. When links auto negotiate speed, all active links are selected for the LAG based on the same speed setting.

- Step 9** Choose an option from the **MDI/MDIX** drop-down list to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX. MDI/MDIX settings are available only for copper interfaces. By default, MDI/MDIX is set to Auto-MDIX, which automatically handles switching between MDI and MDIX to attain link.
- Step 10** Enter a maximum transmission unit (MTU) in the **MTU** field. The range of MTU values can vary depending on the model of the managed device and the interface type.
- Caution** Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.
- Step 11** If you want to allow the LAG interface to respond to ICMP traffic such as pings and traceroute, check the **Enable Responses** check box next to **ICMP**.
- Step 12** If you want to enable the LAG interface to broadcast router advertisements, check the **Enable Router Advertisement** check box next to **IPv6 NDP**.
- Step 13** Click **Add** to add an IP address.
- Step 14** In the **Address** field, enter the routed LAG interface's IP address and subnet mask using CIDR notation. Note the following:
- You cannot add network and broadcast addresses, or the static MAC addresses 00:00:00:00:00:00 and FF:FF:FF:FF:FF:FF.
 - You cannot add identical IP addresses, regardless of subnet mask, to interfaces in virtual routers.
- Step 15** If your organization uses IPv6 addresses and you want to set the IP address of the LAG interface automatically, check the **Address Autoconfiguration** check box next to the **IPv6** field.
- Step 16** For **Type**, choose either Normal or SFRP.
- Step 17** If you chose SFRP for **Type**, set options as described in [SFRP](#).
- Step 18** Click **OK**.
- Note** When adding an IP address to a routed interface of a 7000 or 8000 Series device in a high-availability pair, you must add a corresponding IP address to the routed interface on the high-availability peer.
- Step 19** Click **Add** to add a static ARP entry.
- Step 20** Enter an IP address the **IP Address** field.
- Step 21** Enter a MAC address to associate with the IP address in the **MAC Address** field. Use the standard format (for example, 01:23:45:67:89:AB).
- Step 22** Click **OK**.
- Step 23** Under **Link Aggregation**, choose one or more physical interfaces from **Available Interfaces** to add to the LAG bundle.

Tip To remove physical interfaces from the LAG bundle, choose one or more physical interfaces and click the **Remove Selected icon** . To remove all physical interfaces from the LAG bundle, click the **Remove All icon**. Deleting the LAG interface from the **Interfaces** tab also removes the interfaces.

Step 24 Choose a **Load-Balancing Algorithm** from the drop-down list.

Step 25 Choose a **Link Selection Policy** from the drop-down list.

Tip Choose **LACP Priority** if you are configuring an aggregate interface between a Firepower System device and a third-party network device.

Step 26 If you chose **LACP Priority** as the **Link Selection Policy**, assign a value for **System Priority** and click the **Configure Interface Priority** link to assign a priority value for each interface in the LAG.

Step 27 Choose either **Inner** or **Outer** from the **Tunnel Level** drop-down list.

Note The tunnel level only applies to IPv4 traffic when Layer 3 load balancing is configured. The outer tunnel is always used for Layer 2 and IPv6 traffic. If the **Tunnel Level** is not explicitly set, the default is **Outer**.

Step 28 Under **LACP**, check the **Enabled** check box to allow the routed LAG interface to handle traffic using the Link Aggregation Control Protocol.

If you clear the check box, the LAG interface becomes a static configuration and the Firepower System will use all of the physical interfaces for the aggregation.

Step 29 Click a **Rate** radio button to set the frequency that determines how often LACP control messages are received from the partner device.

- Click **Slow** to receive packets every 30 seconds.
- Click **Fast** to receive packets every 1 second.

Step 30 Click a **Mode** radio button to establish the listening mode of the device.

- Click **Active** to initiate negotiations with remote links by sending LACP packets to the partner device.
- Click **Passive** to respond to LACP packets received.

Step 31 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[Advanced Settings](#)

Adding Logical Aggregate Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

For each switched or routed aggregate interface, you can add multiple logical interfaces. You must associate each logical LAG interface with a VLAN tag to handle traffic received by the LAG interface with that specific tag. You add logical interfaces to switched or routed aggregate interfaces in the same way you would add them to physical switched or routed interfaces.



Note When you create a LAG interface you also create an “untagged” logical interface by default, which is identified by the **lag n .0** label, where n is an integer from 0 to 13. To be operational, each LAG requires this one logical interface at a minimum. You can associate additional logical interfaces with any LAG to handle VLAN-tagged traffic. Each additional logical interface requires a unique VLAN tag. The Firepower System supports VLAN tags in the range of 1 through 4094.



Caution Adding a routed interface pair on 7000 or 8000 Series devices restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to add the logical LAG interface, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** From the **Add** drop-down menu, choose **Add Logical Interface**.
- Step 4** Click **Switched** to display the switched interface options, or click **Routed** to display the routed interface options.
- Step 5** Choose an available LAG from the **Interface** drop-down list. The aggregate interface is identified by the **lag n** label, where n is an integer from 0 to 13.
- Step 6** Configure the remaining settings appropriate to the interface type you chose:
 - Switched — See [Adding Logical Switched Interfaces](#) for more information on adding a logical interface to a switched interface.
 - Routed — See [Adding Logical Routed Interfaces](#) for more information on adding a logical interface to a routed interface.

Related Topics[SFRP](#)[Advanced Settings](#)[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)[Snort® Restart Scenarios](#)

Viewing Aggregate Interface Statistics

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can view protocol and traffic statistics for each aggregate interface. The statistics show LACP protocol information such as LACP key and partner information, packets received, packets transmitter, and packets dropped. Statistics are further refined per member interface to show traffic and link information on a per-port basis.

Aggregate interface information is also presented to the dashboard via predefined dashboard widgets. The Current Interface Status widget shows the status of all interfaces on the appliance, enabled or unused. The Interface Traffic widget shows the rate of traffic received (Rx) and transmitted (Tx) on the appliance's interfaces over the dashboard time range. See [Predefined Dashboard Widgets](#).

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to view the logical aggregate interface statistics, click the edit icon (✎). In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Next to the interface where you want to view the interface statistics, click the view icon (🔍).
-



Deleting Aggregate Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

The aggregate interface can be identified by the **lag n** label, where **n** can be an integer from 0 to 13.

Procedure

-
- Step 1** Choose **Devices > Device Management**.

- Step 2** Next to the device where you want to delete the aggregate interface, click the edit icon ().
- In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Next to the aggregate interface you want to delete, click the delete icon (.
- Step 4** When prompted, confirm that you want to delete the aggregate interface.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).