Interface Overview

The threat defense device includes data interfaces that you can configure in different modes, as well as a management interface.

Management Interface

In Version 7.3 and earlier, the physical management interface is shared between the Diagnostic logical interface and the Management logical interface. In Version 7.4 and later, the Diagnostic interface is merged with Management for a simplified user experience.

Management Interface

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. It uses its own IP address and static routing. You can configure its settings at the CLI using the **configure network** command. You can also view its status on the **Devices** > **Device Management** > **Devices** > **Interfaces** page. If you change the IP address at the CLI after you add it to the management center, you can match the IP address in the Secure Firewall Management Center in the **Devices** > **Device Management** > **Devices** > **Management** area.

You can alternatively manage the threat defense using a data interface instead of the Management interface.

Diagnostic Interface

For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available.

If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically.

If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Note that support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. To manually merge the Management and Diagnostic interfaces, see Merge the Management and Diagnostic Interfaces, on page 35. Configurations that prevent an automatic merge include the following:

- A data interface named "management"—This name is reserved for use with the merged Management interface.

- IP Address on Diagnostic

- DNS enabled on Diagnostic

- Syslog, SNMP, RADIUS or AD (for remote access VPN) source interface is Diagnostic

- RADIUS or AD (for remote access VPN) with no source interface specified, and there is at least one interface configured as management-only (including Diagnostic)—The default route lookup for these services has changed from the management-only routing table to the data routing table, with no fallback to management. Therefore, you cannot use a management-only interface other than Management.

- Static routes on Diagnostic

- Dynamic routing on Diagnostic

- HTTP server on Diagnostic

- ICMP on Diagnostic

- DDNS for Diagnostic

- FlexConfig using Diagnostic

For more information about how the legacy Diagnostic interface operates, see the 7.3 version of this guide.

Interface Mode and Types

You can deploy threat defense interfaces in two modes: Regular firewall mode and IPS-only mode. You can include both firewall and IPS-only interfaces on the same device.

Regular Firewall Mode

Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this traffic according to your security policy.

The types of firewall interfaces you can configure depends on the firewall mode set for the device: routed or transparent mode. See Transparent or Routed Firewall Mode for more information.

- Routed mode interfaces (routed firewall mode only)—Each interface that you want to route between is on a different subnet.

- Bridge group interfaces (routed and transparent firewall mode)—You can group together multiple interfaces on a network, and the threat defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. In routed mode, the threat defense device routes between BVIs and regular routed interfaces. In transparent mode, each bridge group is separate and cannot communicate with each other.

IPS-Only Mode

IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. You might want to implement IPS-only interfaces if you have a separate firewall protecting these interfaces and do not want the overhead of firewall functions.

Note The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes.

IPS-only interfaces can be deployed as the following types:

- Inline Set, with optional Tap mode—An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the threat defense to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

  With tap mode, the threat defense is deployed inline, but the network traffic flow is undisturbed. Instead, the threat defense makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline. For example, you can set up the cabling between the threat defense and the network as if the threat defense were inline and analyze the kinds of intrusion events the threat defense generates. Based on the results, you can modify your intrusion policy and add the drop rules that best protect your network without impacting its efficiency. When you are ready to deploy the threat defense inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the threat defense and the network.

  Note Tap mode *significantly* impacts threat defense performance, depending on the traffic.

  Note Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode or the firewall-type interfaces.

- Passive or ERSPAN Passive—Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the

switch. This function provides the system visibility within the network without being in the flow of network traffic. When you configure the threat defense in a passive deployment, the threat defense cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally. and no traffic received on these interfaces is retransmitted. Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches, and uses GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the threat defense is in routed firewall mode.

Note   Using SR-IOV interfaces as passive interfaces on NGFWv is not supported on some Intel network adapters (such as Intel X710 or 82599) using SR-IOV drivers due to a promiscuous mode restriction. In such cases, use a network adapter that supports this functionality. See Intel Ethernet Products for more information on Intel network adapters.

Security Zones and Interface Groups

Each interface can be assigned to a *security zone* and/or *interface group*. You then apply your security policy based on zones or groups. For example, you can assign the "inside" interface on one or more devices to the "inside" zone; and the "outside" interfaces to the "outside" zone. You can then configure your access control policy to enable traffic to go from the inside zone to the outside zone for every device using the same zones.

To view the interfaces that belong to each object, choose **Objects** > **Object Management** and click **Interface**. This page lists the security zones and interface groups configured on your managed devices. You can expand each interface object to view the type of interfaces in each interface object.

Note   Policies that apply to **any** zone (a global policy) apply to interfaces in zones as well as any interfaces that are not assigned to a zone.

Note   The Management interface does not belong to a zone or interface group.

Security Zones Vs. Interface Groups

There are two types of interface objects:

- Security zones—An interface can belong to only one security zone.

- Interface groups—An interface can belong to multiple interface groups (and to one security zone).

  You can use interface groups in NAT policies, prefilter policies, and QoS policies, as well as features that let you specify the interface name directly, such as Syslog servers or DNS servers.

Some policies only support security zones, while other policies support zones and groups. Unless you need the functionality an interface group provides, you should default to using security zones because security zones are supported for all features.

You cannot change an existing security zone to an interface group or vice-versa; instead you must create a new interface object.

✎

Note   Although tunnel zones are not interface objects, you can use them in place of security zones in certain configurations; see Tunnel Zones and Prefiltering.

Interface Object Types

See the following interface object types:

- Passive—For IPS-only passive or ERSPAN interfaces.

- Inline—For IPS-only inline set interfaces.

- Switched—For regular firewall bridge group interfaces.

- Routed—For regular firewall routed interfaces.

- ASA—(Security zones only) For legacy ASA FirePOWER device interfaces.

- Management—(Interface groups only) For management-only interfaces.

- Loopback—(Interface groups only) For loopback interfaces.

All interfaces in an interface object must be of the same type. After you create an interface object, you cannot change the type of interfaces it contains.

Interface Names

Note that the interface (or zone name) itself does not provide any default behavior in regards to the security policy. We recommend using names that are self-describing to avoid mistakes in future configuration. A good name signifies a logical segment or traffic specification, for example:

- Names of internal interfaces—InsideV110, InsideV160, InsideV195

- Names of DMZ interfaces—DMZV11, DMZV12, DMZV-TEST

- Names of external interfaces—Outside-ASN78, Outside-ASN91

Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Default Settings for Interfaces

This section lists default settings for interfaces.

Default State of Interfaces

The default state of an interface depends on the type.

- Physical interfaces—Disabled. The exception is the Management interface that is enabled for initial setup.

- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.

- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

- EtherChannel port-channel interfaces (ISA 3000)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.

- EtherChannel port-channel interfaces (Firepower and Secure Firewall models)—Disabled.

Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and in the management center. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and management center.

Default Speed and Duplex

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

By default, the speed and duplex for fiber (SFP) interfaces are set to the maximum speed, with auto-negotiation enabled.

For the Secure Firewall 3100/4200, the speed is set to detect the installed SFP speed.

Create Security Zone and Interface Group Objects

Add security zones and interface groups to which you can assign device interfaces.

Tip You can create empty interface objects and add interfaces to them later. To add an interface, the interface must have a name. You can also create security zones (but not interface groups) while configuring interfaces.

Before you begin

Understand the usage requirements and restrictions for each type of interface object. See .

Procedure

Step 1   Choose **Objects** > **Object Management**.

Step 2   Choose **Interface** from the list of object types.

Step 3   Click **Add > Security Zone** or **Add > Interface Group**.

Step 4   Enter a **Name**.

Step 5   Choose an **Interface Type**.

Step 6   (Optional) From the **Device** > **Interfaces** drop-down list, choose a device that contains interfaces you want to add.

            You do not need to assign interfaces on this screen; you can instead assign interfaces to the zone or group when you configure the interface.

Step 7   Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy Configuration Changes.

Enable the Physical Interface and Configure Ethernet Settings

This section describes how to:

- Enable the physical interface. By default, physical interfaces are disabled (with the exception of the Management interface).

- Set a specific speed and duplex. By default, speed and duplex are set to Auto.

This procedure only covers a small subset of Interface settings. Refrain from setting other parameters at this point. For example, you cannot name an interface that you want to use as part of an EtherChannel interface.

Note   For the Firepower 4100/9300, you configure basic interface settings in FXOS. See Configure a Physical Interface for more information.

Note   For Firepower 1010 switch ports, see Configure Firepower 1010 Switch Ports.

Before you begin

If you changed the physical interfaces on the device after you added it to the management center, you need to refresh the interface listing by clicking **Sync Interfaces from device** on the top left of **Interfaces**. For the Secure Firewall 3100/4200, which supports hot swapping, see Manage the Network Module for the Secure Firewall 3100/4200, on page 21 before you change interfaces on a device.

Procedure

Step 1   Select **Devices** > **Device Management** and click **Edit** (✎) for your threat defense device. The **Interfaces** page is selected by default.

Step 2   Click **Edit** (✎) for the interface you want to edit.

Step 3   Enable the interface by checking the **Enabled** check box.

Step 4   (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5   (Optional) Set the duplex and speed by clicking **Hardware Configuration** > **Speed**.

- **Duplex**—Choose **Full** or **Half**. SFP interfaces only support **Full** duplex.

- **Speed**—Choose a speed (varies depending on the model). (Secure Firewall 3100/4200 only) Choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always Full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically.

- **Auto-negotiation**—Set the interface to negotiate the speed, link status, and flow control.

- **Forward Error Correction Mode**—(Secure Firewall 3100/4200 only) For 25 Gbps and higher interfaces, enable Forward Error Correction (FEC). For an EtherChannel member interface, you must configure FEC before you add it to the EtherChannel. The setting chosen when you use **Auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 1: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	Clause 74 FC-FEC	Clause 108 RS-FEC
25G-LR	Clause 74 FC-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

Step 6   (Optional) (Firepower 1100/2100, Secure Firewall 3100/4200) Enable Link Layer Discovery Protocol (LLDP) by clicking **Hardware Configuration** > **Network Connectivity**.

- **Enable LLDP Receive**—Enables the firewall to receive LLDP packets from its peers.

- **Enable LLDP Transmit**—Enables the firewall to send LLDP packets to its peers.

Step 7   (Optional) (Secure Firewall 3100/4200) Enable pause (XOFF) frames for flow control by clicking **Hardware Configuration** > **Network Connectivity**, and checking **Flow Control Send**.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the threat defense port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note   The threat defense supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 8   In the **Mode** drop-down list, choose one of the following:.

- **None**—Choose this setting for regular firewall interfaces and inline sets. The mode will automatically be changed to Routed, Switched, or Inline based on further configuration.

- **Passive**—Choose this setting for passive IPS-only interfaces.

- **Erspan**—Choose this setting for ERSPAN passive IPS-only interfaces.

Step 9   In the **Priority** field, enter a number ranging from 0–65535.

This value is used in the policy based routing configuration. The priority is used to determine how you want to distribute the traffic across multiple egress interfaces.

Step 10   Click **OK**.

Step 11   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Step 12   Continue configuring interfaces.

- Regular Firewall Interfaces

- Inline Sets and Passive Interfaces

Configure EtherChannel Interfaces

This section tells how to configure EtherChannel interfaces.

Note   For the Firepower 4100/9300, you configure EtherChannels in FXOS. See Add an EtherChannel (Port Channel) for more information.

About EtherChannels

This section describes EtherChannels.

About EtherChannels

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Channel Group Interfaces

Each channel group can have up to 8 active interfaces, except for the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The interface is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port numbers and VLAN numbers.

Connecting to an EtherChannel on Another Device

The device to which you connect the threat defense EtherChannel must also support 802.3ad EtherChannels; for example, you can connect to the Catalyst 6500 switch or the Cisco Nexus 7000.

When the switch is part of a Virtual Switching System (VSS) or Virtual Port Channel (vPC), then you can connect threat defense interfaces within the same EtherChannel to separate switches in the VSS/vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch.

Figure 1: Connecting to a VSS/vPC
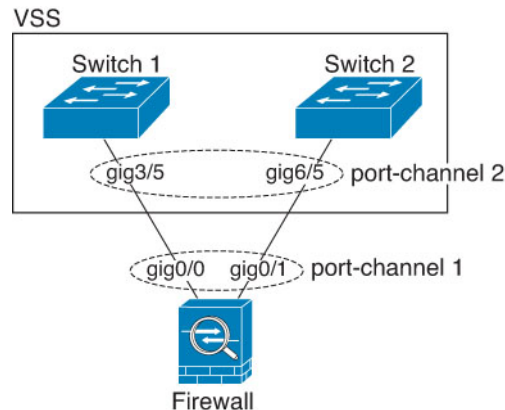
Note If the threat defense device is in transparent firewall mode, and you place the threat defense device between two sets of VSS/vPC switches, then be sure to disable Unidirectional Link Detection (UDLD) on any switch ports connected to the threat defense device with an EtherChannel. If you enable UDLD, then a switch port may receive UDLD packets sourced from both switches in the other VSS/vPC pair. The receiving switch will place the receiving interface in a down state with the reason "UDLD Neighbor mismatch".

If you use the threat defense device in an Active/Standby failover deployment, then you need to create separate EtherChannels on the switches in the VSS/vPC, one for each threat defense device. On each threat defense device, a single EtherChannel connects to both switches. Even if you could group all switch interfaces into a single EtherChannel connecting to both threat defense devices (in this case, the EtherChannel will not be established because of the separate threat defense system IDs), a single EtherChannel would not be desirable because you do not want traffic sent to the standby threat defense device.

Figure 2: Active/Standby Failover and VSS/vPC
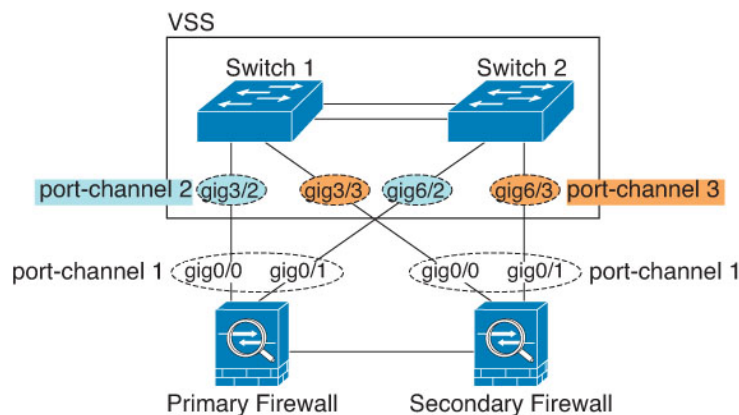
Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.

- Passive—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel. Not supported on hardware models.

- On—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. "On" mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

Load Balancing

The threat defense device distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (this criteria is configurable). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a *hash_value* **mod** *active_links* result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

EtherChannel MAC Address

All interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links.

Firepower and Secure Firewall Hardware

The port-channel interface uses the MAC address of the internal interface Internal-Data 0/1. Alternatively you can manually configure a MAC address for the port-channel interface. All EtherChannel interfaces on a chassis use the same MAC address, so be aware that if you use SNMP polling, for example, multiple interfaces will have the same MAC address.

Note Member interfaces only use the Internal-Data 0/1 MAC address after a reboot. Prior to rebooting, the member interface uses its own MAC address. If you add a new member interface after a reboot, you will have to perform another reboot to update its MAC address.

Guidelines for EtherChannels

Bridge Group

In routed mode, Management Center-defined EtherChannels are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.

High Availability

- When you use an EtherChannel interface as a High Availability link, it must be pre-configured on both units in the High Availability pair; you cannot configure it on the primary unit and expect it to replicate to the secondary unit because *the High Availability link itself is required for replication*.

- If you use an EtherChannel interface for the state link, no special configuration is required; the configuration can replicate from the primary unit as normal. For the Firepower 4100/9300 chassis, all interfaces, including EtherChannels, need to be pre-configured on both units.

- You can monitor EtherChannel interfaces for High Availability. When an active member interface fails over to a standby interface, this activity does not cause the EtherChannel interface to appear to be failed when being monitored for device-level High Availability. Only when all physical interfaces fail does the EtherChannel interface appear to be failed (for an EtherChannel interface, the number of member interfaces allowed to fail is configurable).

- If you use an EtherChannel interface for a High Availability or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a High Availability link. To alter the configuration, you need to temporarily disable High Availability, which prevents High Availability from occurring for the duration.

Model Support

- You cannot add EtherChannels in the management center for the Firepower 4100/9300 or the threat defense virtual. The Firepower 4100/9300 supports EtherChannels, but you must perform all hardware configuration of EtherChannels in FXOS on the chassis.

- You cannot use Firepower 1010 switch ports or VLAN interfaces in EtherChannels.

General EtherChannel Guidelines

- You can configure up to 48 EtherChannels, depending on how many interfaces are available on your model.

- Each channel group can have up to 8 active interfaces, except for the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

- All interfaces in the channel group must be the same media type and speed capacity. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, except for the Secure Firewall 3100/4200, which supports different interface capacities as long as the speed is set to Detect SFP; in this case the lowest common speed is used.

- The device to which you connect the threat defense EtherChannel must also support 802.3ad EtherChannels.

- The threat defense device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS **vlan dot1Q tag native** command, then the threat defense device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.

- The LACP rate depends on the model. When you set the rate (normal or fast), the device requests that rate from the connecting switch. In return, the device will send at the rate requested by the connecting switch. We recommend that you set the same rate on both sides.

  - Firepower 4100/9300—The LACP rate is set to fast by default in FXOS, but you can configure it as normal (also known as slow).

  - Secure Firewall 3100/4200—The LACP rate is set to normal (slow) by default, but you can configure it as fast on the device.

  - All other models—The LACP rate set to normal (also known as slow), and it is not configurable, which means the device will always request a slow rate from the connecting switch. We recommend setting the rate on the switch to slow, so both sides send LACP messages at the same rate.

- In Cisco IOS software versions earlier than 15.1(1)S2, threat defense did not support connecting an EtherChannel to a switch stack. With default switch settings, if the threat defense EtherChannel is connected cross stack, and if the primary switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

- All the threat defense configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

Configure an EtherChannel

This section describes how to create an EtherChannel port-channel interface, assign interfaces to the EtherChannel, and customize the EtherChannel.

Guidelines

- You can configure up to 48 EtherChannels, depending on the number of interfaces for your model.

- Each channel group can have up to 8 active interfaces, except for the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

- All interfaces in the channel group must be the same media type and speed capacity. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, except for the Secure Firewall 3100/4200, which supports different interface capacities as long as the speed is set to Detect SFP; in this case the lowest common speed is used.

Note For the Firepower 4100/9300, you configure EtherChannels in FXOS. See Add an EtherChannel (Port Channel) for more information.

Before you begin

- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.

Note If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.
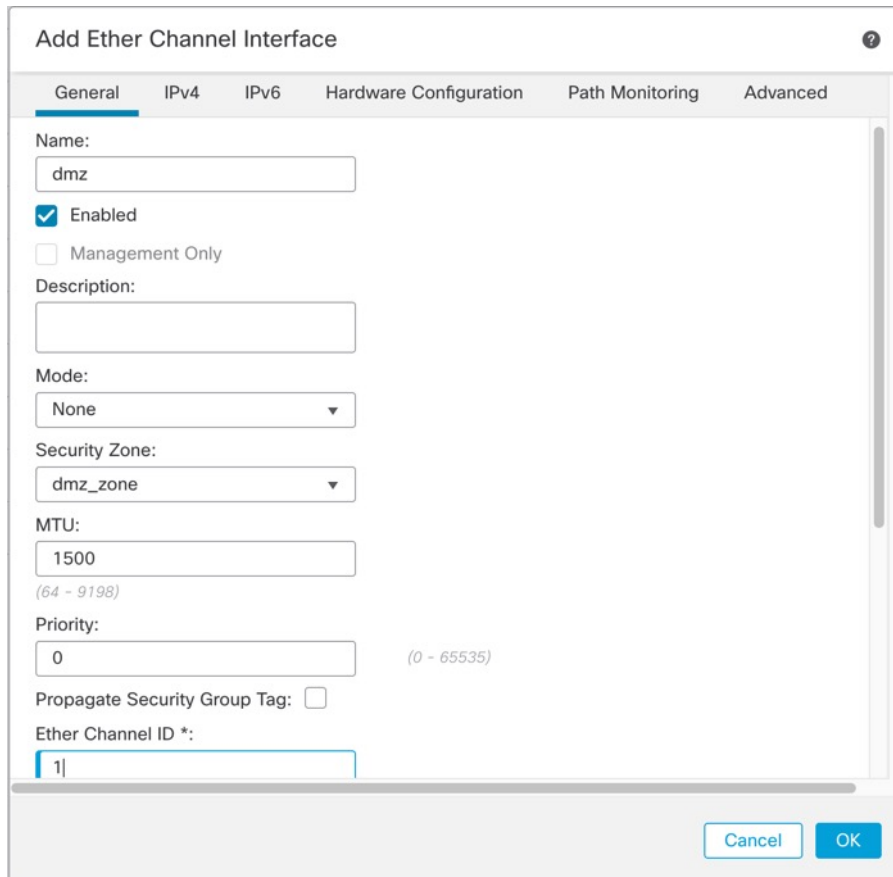
Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** (✐) for your threat defense device. The **Interfaces** page is selected by default.

Step 2 Enable the member interfaces according to Enable the Physical Interface and Configure Ethernet Settings, on page 7.

Step 3 Click **Add Interfaces** > **Ether Channel Interface**.

Step 4 On the **General** tab, set the **Ether Channel ID** to a number between 1 and 48 (1 and 8 for the Firepower 1010).

Figure 3: Add EtherChannel Interface

Step 5   In the **Available Interfaces** area, click an interface and then click **Add** to move it to the **Selected Interfaces** area. Repeat for all interfaces that you want to make members.

Make sure all interfaces are the same type and speed capability.

Figure 4: Available Interfaces

Ether Channel ID *:

1

(1-8)

Available Interfaces ↻

🔍 Search

Ethernet1/1   Add

Selected Interfaces

NVE Only:

☐

Cancel   OK

Step 6   (Optional) Click the **Advanced** tab to customize the EtherChannel. Set the following parameters on the **Information** sub-tab:

Figure 5: Advanced

Add Ether Channel Interface   ❓

General   IPv4   IPv6   Hardware Configuration   Path Monitoring   Advanced

Information

LACP Mode: Active

Active Mac Address:

Standby Mac Address:

- (ISA 3000 only) **Load Balancing**—Select the criteria used to load balance the packets across the group channel interfaces. By default, the threat defense device balances the packet load on interfaces according to the source and destination IP address of the packet. If you want to change the properties on which the packet is categorized, choose a different set of criteria. For example, if your traffic is biased heavily towards the same source and destination IP addresses, then the traffic assignment to interfaces in the EtherChannel will be unbalanced. Changing to a different algorithm can result in more evenly distributed traffic. For more information about load balancing, see Load Balancing, on page 12.

- **LACP Mode**—Choose Active, Passive, or On. We recommend using Active mode (the default). Passive mode is only available for the ISA 3000 only.

- (Secure Firewall 3100/4200 only) **LACP Rate**—Choose Default, Normal, or Fast. The defualt is Normal (also known as slow). Sets the LACP data unit receive rate for a physical interface in the channel group. We recommend that you set the same rate on both sides.

- (ISA 3000 only) **Active Physical Interface: Range**—From the left drop-down list, choose the minimum number of active interfaces required for the EtherChannel to be active, between 1 and 16. The default is 1. From the right drop-down list, choose the maximum number of active interfaces allowed in the EtherChannel, between 1 and 16. The default is 16. If your switch does not support 16 active interfaces, be sure to set this command to 8 or fewer.

- **Active Mac Address**—Set a manual MAC address if desired. The mac_address is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

Step 7 Click the **Hardware Configuration** tab and set the Duplex and Speed for all member interfaces.

Step 8 Click **OK**.

Step 9 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Step 10 (Optional) For regular firewall interfaces, add a VLAN subinterface. See Add a Subinterface.

Step 11 For regular firewall interfaces, configure the routed or transparent mode interface parameters: Configure Routed Mode Interfaces or Configure Bridge Group Interfaces. For IPS-only interfaces, see Inline Sets and Passive Interfaces.

Sync Interface Changes with the Management Center

Interface configuration changes on the device can cause the management center and the device to get out of sync. The management center can detect interface changes by one of the following methods:

- Event sent from the device

- Sync when you deploy from the management center

  If the management center detects interface changes when it attempts to deploy, the deploy will fail. You must first accept the interface changes.

- Manual sync

There are two types of interface changes performed outside of management center that need to be synched:

- Addition or deletion of physical interfaces—Adding a new interface, or deleting an unused interface has minimal impact on the threat defense configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the threat defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the management center.

  When the management center detects changes, the **Interface** page shows status (removed, changed, or added) to the left of each interface.

- Management Center access interface changes—If you configure a data interface for managing management center using the **configure network management-data-interface** command, you must manually make

matching configuration changes in management center and then acknowledge the changes. These interface changes cannot be made automatically.

This procedure describes how to manually sync device changes if required and how to acknowledge the detected changes. If device changes are temporary, you should not save the changes in the management center; you should wait until the device is stable, and then re-sync.

Before you begin

- User Roles:
  - Admin
  - Access Admin
 - Network Admin

Procedure

Step 1   Select **Devices** > **Device Management** and click **Edit** (✐) for your threat defense device. The **Interfaces** page is selected by default.

Step 2   If required, click **Sync Device** on the top left of **Interfaces**.

Step 3   After the changes are detected, see the following steps.

Addition or Deletion of Physical Interfaces

a) You will see a red banner on **Interfaces** indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

   If there are any errors, you need to change your policy and rerun the validation.

c) Click **Save**.

   You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

FMC Access Interface Changes

a) You will see a yellow banner in the top right of the **Device** page indicating that the management center access configuration has changed. Click the **View details** link to view the interface changes.
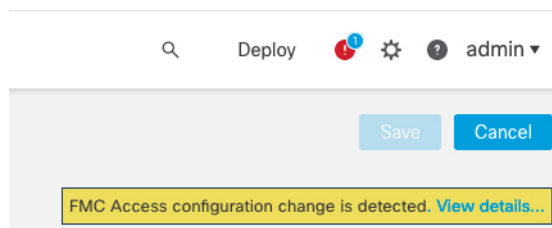
   The **FMC Access - Configuration Details** dialog box opens.

b) Take note of all highlighted configurations, especially the pink highlighted ones. You need to match any values on the threat defense by manually configuring them on the management center.

For example, the pink highlights below show configuration that exists on the threat defense but not yet on the management center.

The following example shows this page after configuring the interface in management center; the interface settings match, and the pink highlight was removed.

   c) Click **Acknowledge**.

We recommend that you do not click **Acknowledge** until you have finished the management center configuration, and are ready to deploy. Clicking **Acknowledge** removes the block on deployment. The next time you deploy, the management center configuration will overwrite any remaining conflicting settings on the threat defense. It is your responsibility to manually fix the configuration in the management center before you re-deploy.

d) You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

Manage the Network Module for the Secure Firewall 3100/4200

If you install a network module before you first power on the device, no action is required; the network module is enabled and ready for use.

To view physical interface details for the device, and to manage the network module, open the **Chassis Operations** page. From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit. The **Chassis Operations** page opens for the device.

Figure 6: Chassis Operations

Click **Refresh** to refresh interface status. Click **Sync Modules** if you made a hardware change on the device that you need to detect.

If you need to make changes to your network module installation after initial bootup, then see the following procedures.

Configure Breakout Ports

You can configure 10GB breakout ports for each 40GB or higher interface. This procedure tells you how to break out and rejoin the ports. breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels.

Changes are immediate; you do not need to deploy to the device. After you break or rejoin, you cannot roll back to the previous interface state.

Before you begin

- You must use a supported breakout cable. See the hardware installation guide for more information.

- The interface cannot be in use for the following before breaking or rejoining:

  - Failover link

  - Cluster control link

  - Have a subinterface

  - EtherChannel member

  - BVI member

  - Manager access interface

- Breaking or rejoining and interface that is used directly in your security policy can impact the configuration; however, the action is not blocked.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 7: Manage Chassis

	Name		Model	Version	Chassis
☐	⌄ Ungrouped (2)				
☐	🟢 **172.16.0.51** Snort 3 172.16.0.51 - Transparent		Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device (in multi-instance mode, this page is called **Chassis Manager**). This page shows physical interface details for the device.

**Step 2** Break out 10GB ports from a 40GB or higher interface.

a) click **Break** () to the right of the interface.

Click **Yes** on the confirmation dialog box. If the interface is in use, you will see an error message. You must resolve any use cases before you can retry the breakout.

For example, to break out the Ethernet2/1 40GB interface, the resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

On the interfaces graphic, a port that is broken out has this appearance:

Figure 8: Breakout Ports
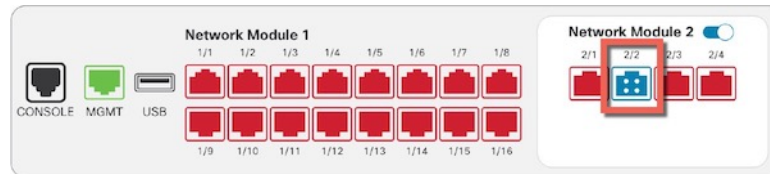
b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 9: Go to Interface Page

⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

c) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 10: View Interface Changes

Interface configuration has changed on device. Click to know more.

Figure 11: Interface Changes

Interface Changes ❓

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
🔺 Ethernet2/2	Physical	Interface is disassociated
🔺 Ethernet2/2/1	Physical	Interface is associated
🔺 Ethernet2/2/2	Physical	Interface is associated
🔺 Ethernet2/2/3	Physical	Interface is associated

Close   Validate Changes

d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Replacing the parent interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity

rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Step 3 Rejoin breakout ports.

You must rejoin all child ports for the interface.

a) Click **Join** (➤➤) to the right of the interface.

Click **Yes** on the confirmation dialog box. If any child ports are in use, you will see an error message. You must resolve any use cases before you can retry the rejoin.

b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.
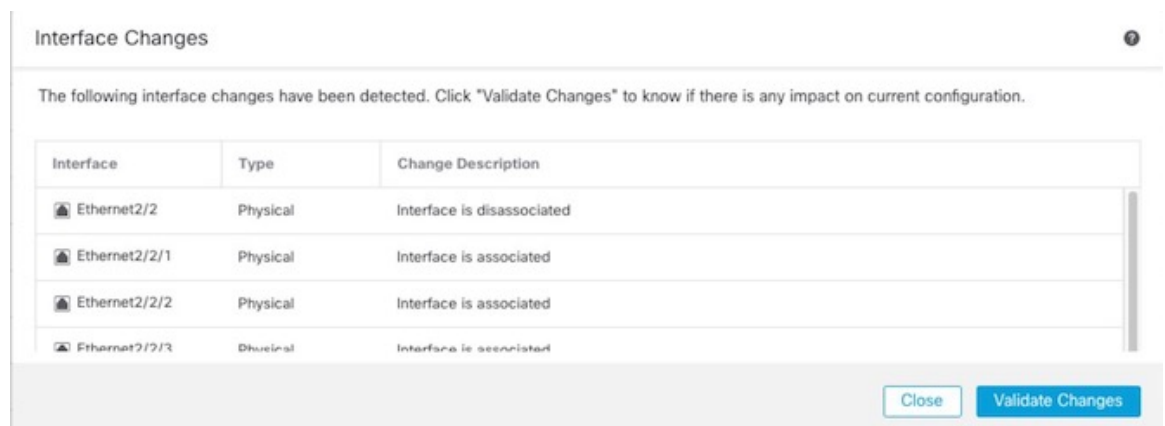
Figure 12: Go to Interface Page

> ⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

c) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 13: View Interface Changes

> Interface configuration has changed on device. Click to know more.

Figure 14: Interface Changes

Interface Changes   ❓

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
🔒 Ethernet2/2	Physical	Interface is disassociated
🔒 Ethernet2/2/1	Physical	Interface is associated
🔒 Ethernet2/2/2	Physical	Interface is associated
🔒 Ethernet2/2/3	Physical	Interface is associated

Close   Validate Changes

d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Replacing the child interfaces that are used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Add a Network Module

To add a network module to a firewall after initial bootup, perform the following steps. Adding a new module requires a reboot.

Procedure

Step 1 Install the network module according to the hardware installation guide.

For clustering or High Availability, install the network module on all nodes.

Step 2 Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node (see Change the Control Node) or active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.

Step 3 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 15: Manage Chassis

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 4 Click **Sync Modules** to update the page with the new network module details.

Step 5 On the interfaces graphic, click the slider ( ) to enable the network module.

Figure 16: Enable the Network Module
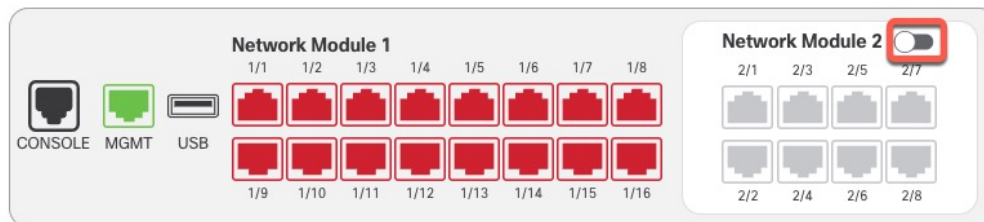
Step 6 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 17: Confirm Enable

Confirm Switching Network Module On ⊠

⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn on the network module?

Turning the module on will add the associated interfaces to device.

No   Yes

Step 7 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

Figure 18: Go to Interface Page

⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

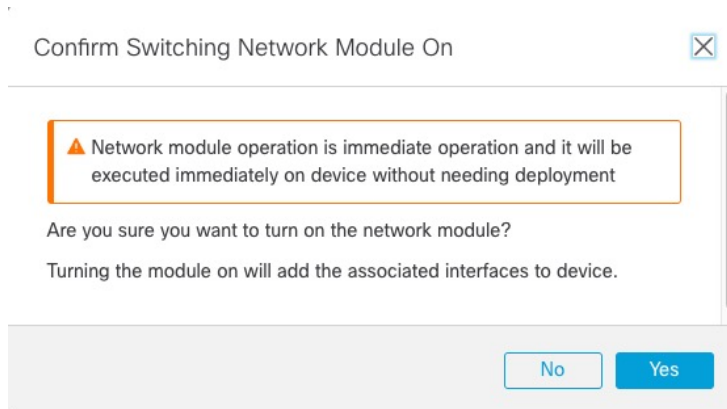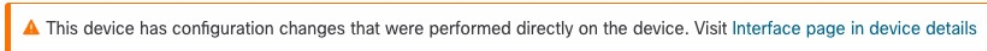**Step 8** (Optional) At the top of the **Interfaces** page, you see a message that the interface configuration has changed. You can click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 19: View Interface Changes

Interface configuration has changed on device. Click to know more.

Figure 20: Interface Changes

Interface Changes   ❓

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is associated
Ethernet2/2	Physical	Interface is associated
Ethernet2/5	Physical	Interface is associated
Ethernet2/6	Physical	Interface is associated
Ethernet2/7	Physical	Interface is associated
Ethernet2/8	Physical	Interface is associated

Close   Validate Changes

Click **Close** to return to the **Interfaces** page. (Because you are adding a new module, there shouldn't be any configuration impact, so you do not need to click **Validate Changes**.)

Step 9 Click **Save** to save the interface changes to the firewall.

Hot Swap the Network Module

You can hot swap a network module for a new module of the same type without having to reboot. However, you must shut down the current module to remove it safely. This procedure describes how to shut down the old module, install a new module, and enable it.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit. You cannot disable a network module if the cluster control link/failover link is on the module.

Before you begin

Procedure

Step 1 For clustering or High Availability, perform the following steps.

- **Clustering**—Ensure the unit you want to perform the hot swap on is a data node (see Change the Control Node); then break the node so it is no longer in the cluster. See Break a Node.

  You will add the node back to the cluster after you perform the hot swap. Alternatively, you can perform all operations on the control node, and the network module changes will sync to all data nodes. However, you will lose use of those interfaces on all nodes during the hot swap.

- **High Availability**—To avoid failing over when you disable the network module:

  - If the failover link is on the network module, you must break High Availability. See Break a High Availability Pair. Disabling the network module with an active failover link is not allowed.

  - Disable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 21: Manage Chassis

	Name		Model	Version	Chassis
☐	⌄ Ungrouped (2)				
☐	🟢 **172.16.0.51** Snort 3 172.16.0.51 - Transparent		Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider (🔵) to disable the network module.

Figure 22: Disable the Network Module
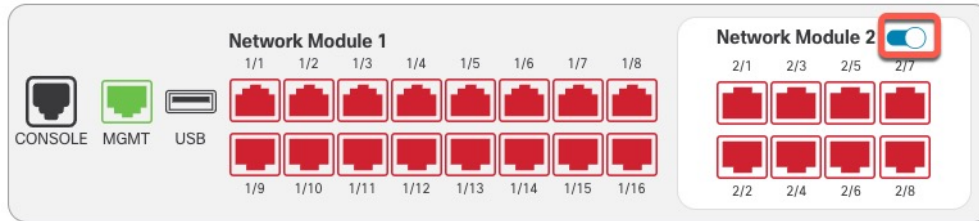
Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

Step 4 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 23: Confirm Disable
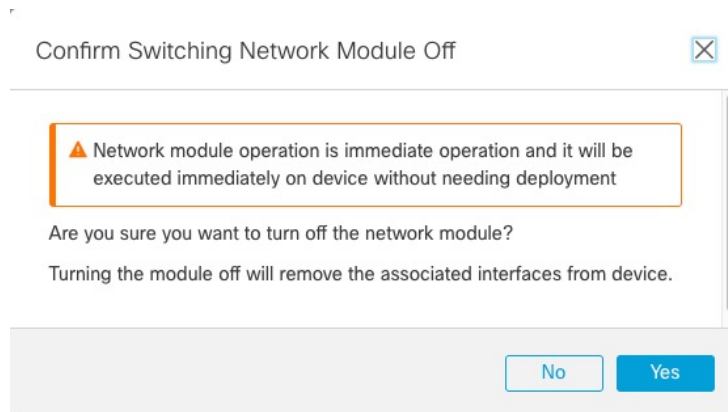
Step 5 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

Step 6 In the management center, enable the new module by clicking the slider ( ).

Figure 24: Enable the Network Module

Step 7 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 25: Confirm Enable

Confirm Switching Network Module On ✕

⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn on the network module?

Turning the module on will add the associated interfaces to device.
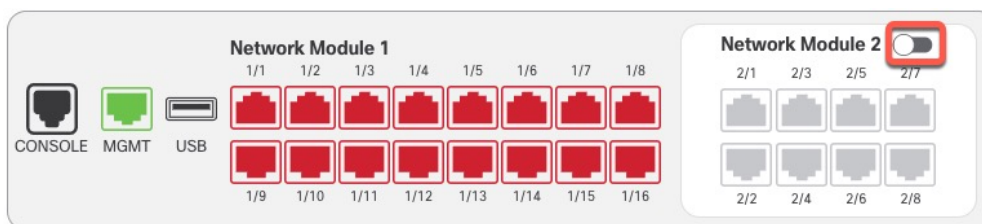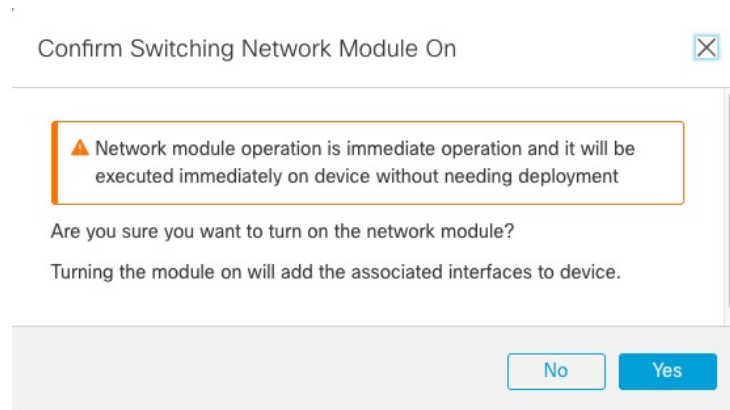
No   Yes

Step 8 For clustering or High Availability, perform the following steps.

- **Clustering**—Add the node back to the cluster. See Add a New Cluster Node.

- **High Availability**—

  - If you broke High Availability, then reform High Availability. See Add a High Availability Pair.

  - Reenable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Replace the Network Module with a Different Type

If you replace a network module with a different type, then a reboot is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit.

Before you begin

For High Availability, you cannot disable a network module if the failover link is on the module. You will have to break High Availability (see Break a High Availability Pair), which means you will have downtime when you reboot the active unit. After the units finish rebooting, you can reform High Availability.

Procedure

Step 1 For clustering or High Availability, perform the following steps.

- **Clustering**—To avoid downtime, you can break each node one at a time so it is no longer in the cluster while you perform the network module replacement. See Break a Node.

  You will add the node back to the cluster after you perform the replacement.

- **High Availability**—To avoid failing over when you replace the network module, disable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 26: Manage Chassis

	Name	Model	Version	Chassis
☐	⌄ Ungrouped (2)			
☐	● **172.16.0.51** Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider (⬤) to disable the network module.

Figure 27: Disable the Network Module
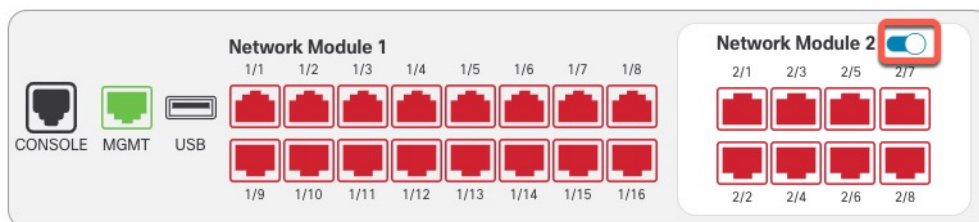
Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

Step 4 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 28: Confirm Disable
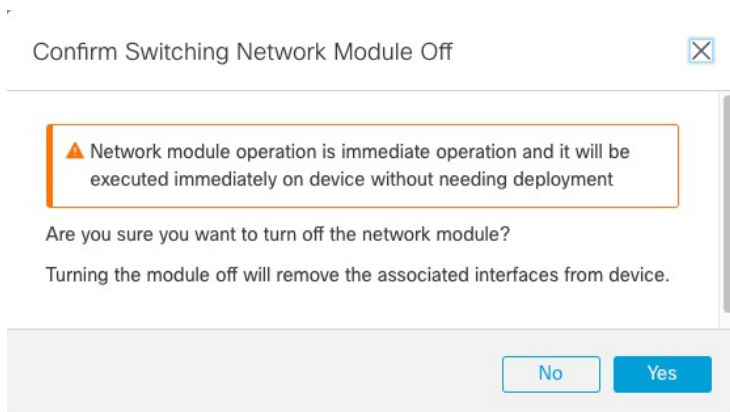
Step 5 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

Step 6   Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node (see Change the Control Node) or active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.

Step 7   In the management center, click **Sync Modules** to update the page with the new network module details.

Step 8   Enable the new module by clicking the slider (   ).

Figure 29: Enable the Network Module
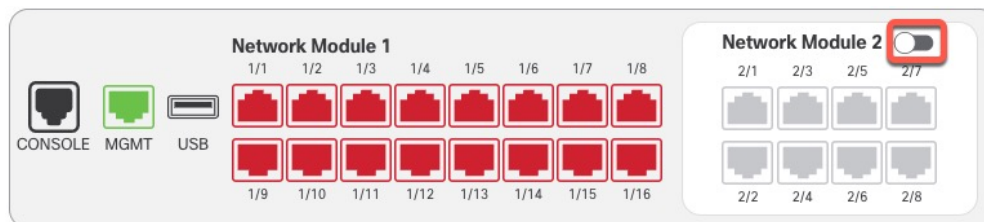
Step 9   You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 30: Confirm Enable
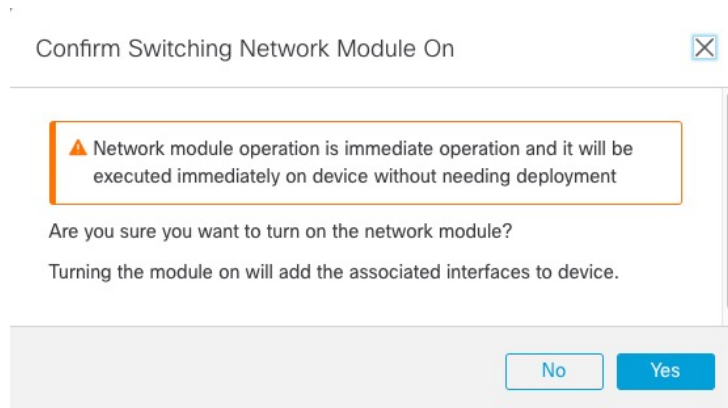
Step 10   Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 31: Go to Interface Page

Step 11   If the network module has *fewer* interfaces:

a) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 32: View Interface Changes
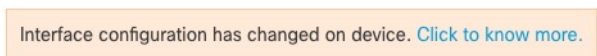
Figure 33: Interface Changes
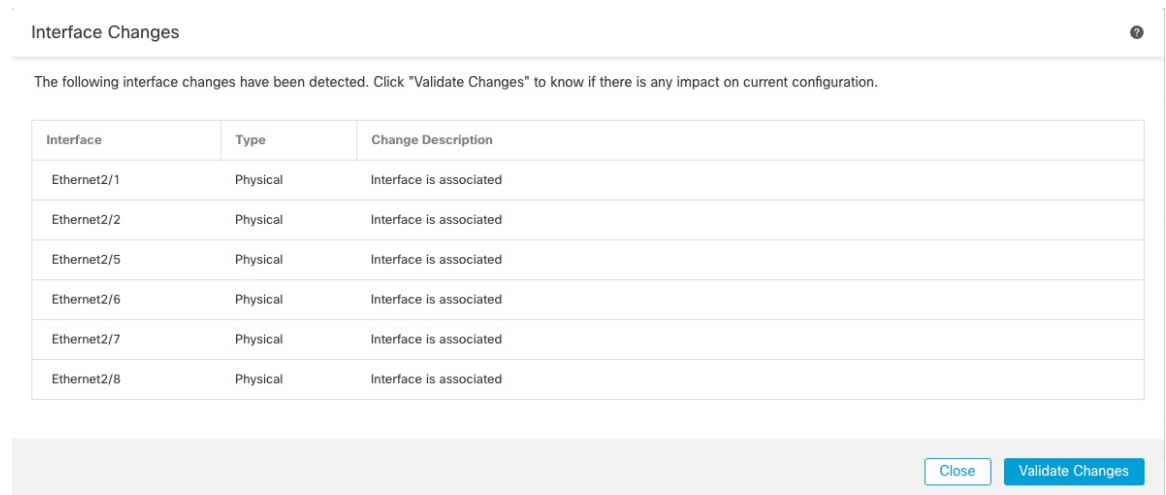
b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 12   To change the interface speed, see Enable the Physical Interface and Configure Ethernet Settings, on page 7.

The default speed is set to Detect SFP, which detects the correct speed from the SFP installed. You only need to fix the speed if you manually set the speed to a particular value and you now need a new speed.

Step 13   Click **Save** to save the interface changes to the firewall.

Step 14   If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the network module changes.

Step 15   For clustering or High Availability, perform the following steps.

- **Clustering**—Add the node back to the cluster. See Add a New Cluster Node.

- **High Availability**—Reenable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Remove the Network Module

If you want to permanently remove the network module, follow these steps. Removing a network module requires a reboot.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit.

Before you begin

For clustering or High Availability, make sure the cluster/failover link is not on the network module.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 34: Manage Chassis

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 2 On the interfaces graphic, click the slider (⬤) to disable the network module.

Figure 35: Disable the Network Module
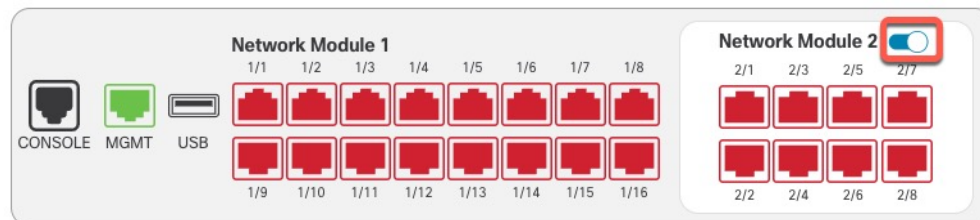
Step 3 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 36: Confirm Disable
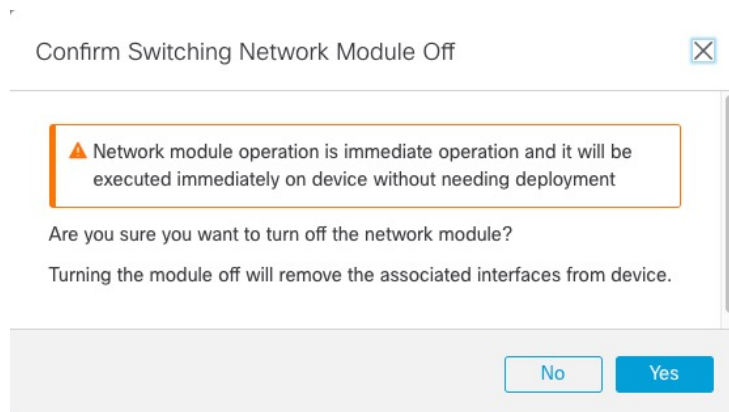
Step 4 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

Figure 37: Go to Interface Page

⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

Step 5   At the top of the **Interfaces** page, you see a message that the interface configuration has changed.

Figure 38: View Interface Changes

Interface configuration has changed on device. Click to know more.

a) Click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 39: Interface Changes
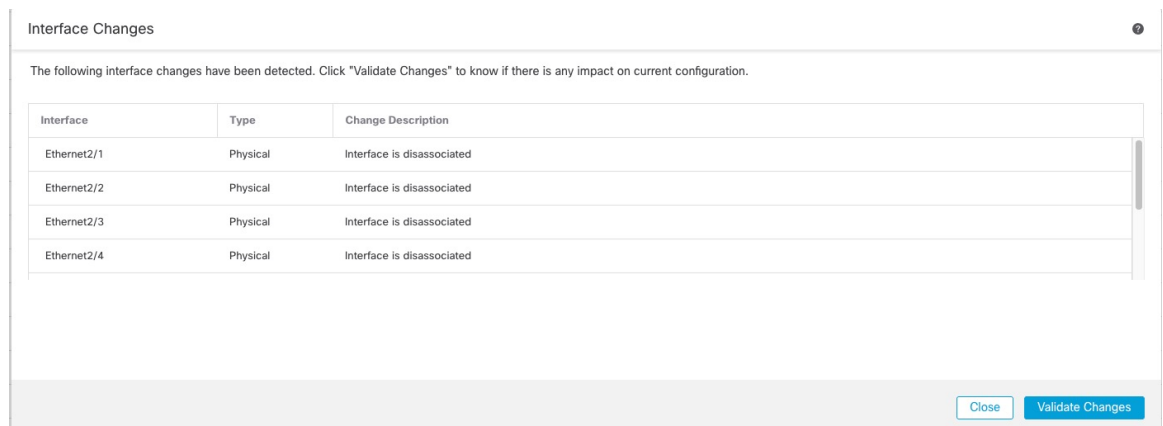
Interface Changes			?

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is disassociated
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/3	Physical	Interface is disassociated
Ethernet2/4	Physical	Interface is disassociated

Close   Validate Changes

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 6   Click **Save** to save the interface changes to the firewall.

Step 7   If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

Step 8   Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node (see Change the Control Node) or active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.

Merge the Management and Diagnostic Interfaces

Threat Defense 7.4 and later supports a merged Management and Diagnostic interface. If you have any configuration using the Diagnostic interface, then the interfaces will not be merged automatically, and you will need to perform the following procedure. This procedure requires you to acknowledge configuration changes, and in some cases, manually fix the configuration.

The Backup/Restore and management center configuration rollback functions save and restore the merged state, either non-merged or merged. For example, if you merge the interfaces, and then restore an old non-merged configuration, then the restored configuration will be in a non-merged state.

The following table shows the available configuration on the legacy Diagnostic interface, and how the merge is completed.

Table 2: Management Center Merged Management Interface Support

Legacy Diagnostic Interface Configuration	Merge Behavior	Supported on Management?
Interfaces		The "management" interface is now shown in read-only mode on the **Interfaces** page.
• IP address	Manual removal required.	The current Management IP address is used instead. For High Availability and clustering, the Management interface does not support a standby IP address or IP address pool; each unit has its own IP address that is maintained across failovers. Therefore, you cannot use a single management IP address to communicate with the current active/control unit. Set at the CLI using the **configure network ipv4** or **configure network ipv6** command.
• "diagnostic" name	Automatically changed to "management". **Note** No other interfaces can be named "management". You must change the name to proceed with the merge.	Changed to "management".

Legacy Diagnostic Interface Configuration	Merge Behavior	Supported on Management?
Static Routes	Manual removal required.	**No support.** The Management interface has a separate Linux routing table from the data interfaces. The threat defense actually has two "data" routing tables: for data interfaces and for management-only interfaces (which used to include Diagnostic, but also includes any interfaces you set to management-only). Depending on the traffic type, the threat defense checks one routing table, and then falls back to the other routing table. This route lookup no longer includes the Diagnostic interface, and does not include the Linux routing table for Management. See Routing Table for Management Traffic for more information. You can add static routes for the Linux routing table at the CLI using the **configure network static-routes** command **Note** The *default* route is set with the **configure network ipv4** or **configure network ipv6** command.
Dynamic Routing	Manual removal required.	**No support.**
HTTP server	No change.	**No support.** This setting will no longer work on the merged device, but it is not removed from the Platform Settings. Platform Settings can be used for multiple devices, some of which may not yet be merged.
ICMP	No change.	**No support.** This setting will no longer work on the merged device, but it is not removed from the Platform Settings. Platform Settings can be used for multiple devices, some of which may not yet be merged.
Syslog Server	Automatically moved to Management interface.	Yes. The syslog server configuration already has the option to send syslogs out of the Management interface (starting in 6.3). If you had specifically chosen the Diagnostic interface for syslogs, it will be moved to use Management. **Note** If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. **Note** The merged Management interface does not support Secure Syslogs.
SMTP	No change.	**No support.** The threat defense checks the data routing table only for the SMTP server, so you cannot use the Management interface or any other management-only interfaces. See Routing Table for Management Traffic for more information.

Legacy Diagnostic Interface Configuration	Merge Behavior	Supported on Management?
SNMP	Automatically moved to Management interface.	Yes. The SNMP host configuration already has the option to allow SNMP hosts on the Management interface (starting in 6.3). If you had specifically chosen the Diagnostic interface for SNMP, it will be moved to use Management. **Note** If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices.
RADIUS server	Automatically moved to Management interface.	Yes. If you had specifically chosen the Diagnostic interface, it will be moved to use Management. **Note** If you specified a route lookup to find the source interface, then the threat defense will no longer be able to send traffic out of a management-only interface; you must explicitly select Management as the source interface. Other management-only interfaces cannot be used.
AD server	Automatically moved to Management interface.	Yes. If you had specifically chosen the Diagnostic interface, it will be moved to use Management. **Note** If you specified a route lookup to find the source interface, then the threat defense will no longer be able to send traffic out of a management-only interface; you must explicitly select Management as the source interface. Other management-only interfaces cannot be used.
DDNS	Manual removal required.	**No support.**
DHCP server	Manual removal required.	**No support.**
DNS server	Automatically moved to Management interface.	Yes. If you checked the **Enable DNS Lookup via diagnostic interface also** check box, then it will be moved to use Management. There is a routing lookup change when you do not choose any interfaces or check the **Enable DNS Lookup via diagnostic/management interface also** check box: the threat defense uses the data routing table only, and does not fall back to using the management-only routing table. Therefore, you cannot use a management-only interface for DNS other than the Management interface. **Note** The Management interface also has a separate DNS lookup setting for its management traffic only. Set at the CLI using the **configure network dns** command.

Legacy Diagnostic Interface Configuration	Merge Behavior	Supported on Management?
FlexConfig	Manual removal required.	**No support.**

Before you begin

- To view the current mode of the device, enter the **show management-interface convergence** command at the threat defense CLI. The following output shows that the Management interfaces are merged:

```
> show management-interface convergence
management-interface convergence
>
```

The following output shows that the Management interfaces are not merged:

```
> show management-interface convergence
no management-interface convergence
>
```

- For High Availability pairs and clusters, perform this task on the active/control unit. The merged configuration will be replicated automatically to the standby/data units.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) for your threat defense. The **Interfaces** page is selected by default. .

Step 2 Edit the Diagnostic interface, and remove the IP address.

You cannot complete the merge until after you have removed the Diagnostic IP address.

Step 3 Click **Management Interface Merge** in the **Management Interface action needed** area.

The **Management Interface Merge** dialog box shows all the occurrences of the Diagnostic interface in the configuration. For any occurrences that require you to manually remove or change the configuration, they will appear with a warning icon. Platform Settings that will no longer work on your device are marked with a caution icon and require your acknowledgement.

Management Interface Merge   ? ✕

ⓘ • The management interface merge will be synced to the standby unit. The IP addresses
       shown in the "Review Uses" section shows the active unit's active address.
    • After you click Proceed, IP address changes will be saved, and you cannot revert the
       management interface merge, even if you discard the deployment.
    • Diagnostic interface static routing is no longer supported; you must delete the route before
       you can proceed. Learn more
    • HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead
of two IP addresses. The merged interface will be called Management and use the current
management IP address. You will need to update all external services that communicate with
Diagnostic IP address.
Learn more
Review the Diagnostic IP uses below. The ❌ symbol shows configuration uses that you must edit
manually before you can proceed.

REVIEW 4 USES ⟳ Refresh   Do you acknowledge the
                                                             change?

❌ **Management Interface**
    Management interface (Management1/1) has (IPv4/IPv6) address con... See
    more

❌ **Static Route Setting**
    Static Route Setting under virtual router [Global] with manageme... See more

❌ **RIP**
    RIP with management interface (management) are not valid when th... See
    more

⚠ **HTTP Access**   ☐
    Management interface (management) is used in (HTTP Access) of PF... See
    more

                                               Cancel   Proceed

Step 4 If you need to manually remove or change any listed configurations, do the following.

a) Click **Cancel** to close the **Management Interface Merge** dialog box.

b) Navigate to the feature area. You can then delete the item, or choose a data interface instead.

c) Reopen the **Management Interface Merge** dialog box.

There should no longer be any warnings.

Step 5 For each configuration caution, click the box in **Do you acknowledge the change?** column, and then click
Proceed.

Management Interface Merge   ? ✕

> ⓘ   • The management interface merge will be synced to the standby unit. The IP addresses
>   shown in the "Review Uses" section shows the active unit's active address.
>   • After you click Proceed, IP address changes will be saved, and you cannot revert the
>   management interface merge, even if you discard the deployment.
>   • Diagnostic interface static routing is no longer supported; you must delete the route before
>   you can proceed.   Learn more
>   • HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead
of two IP addresses. The merged interface will be called Management and use the current
management IP address. You will need to update all external services that communicate with
Diagnostic IP address.
Learn more
Review the Diagnostic IP uses below. The ❌ symbol shows configuration uses that you must edit
manually before you can proceed.

REVIEW 2 USES   ⟳ Refresh   Do you acknowledge the
                                                          change?

⚠ **HTTP Access**   ☑
    Management interface (management) is used in (HTTP Access) of PF... See
    more

⚠ **ICMP Access**   ☑
    Management interface (management) is used in (ICMP Access) of PF... See
    more

                                                    Cancel   Proceed

After the configuration is merged, you see a success banner:

> ✓ The Management interface merge was saved and is ready to be deployed.   ✕
>   Note that you cannot undo the configuration changes related to merge; you must manually reconfigure the Diagnostic interface and related configuration.

Step 6   Deploy the new merged configuration.

Caution   After you deploy the merged configuration, you can unmerge the interfaces from management center;
              however the Diagnostic interface will have to be reconfigured manually. See Unmerge the Management
              Interface, on page 41. Also, if you restore a configuration that is unmerged, or roll back to an unmerged
              configuration, then the device will revert to that unmerged configuration.

After the merge, the Management interface is shown on the **Interfaces** page, although it is read-only.

Step 7   After the merge, if you had any external services that communicated with the Diagnostic interface, you need
              to change their configuration to use the Management interface IP address.

              For example:

                 • SNMP client

                 • RADIUS server—RADIUS servers often verify the IP address for incoming traffic, so you need to change
                   that IP address to the Management address. Moreover, for a High Availability pair, you need to allow

both the primary and secondary Management IP addresses; the Diagnostic interface used to support a single "floating" IP address that stayed with the active unit, but Management does not support that functionality.

Unmerge the Management Interface

The threat defense 7.4 and later supports a merged Management and Diagnostic interface. If you need to unmerge your interfaces, perform this procedure. We recommend using unmerged mode temporarily while you migrate your network to a merged mode deployment. Separate Management and Diagnostic interfaces may not be supported in all future releases.

Unmerging the interfaces does not restore your original Diagnostic configuration (if you upgraded and then merged your interfaces). You will need to reconfigure the Diagnostic interface manually. Also, the Management interface will now be named "management"; you cannot rename it "diagnostic."

Alternatively, if you used the Backup function to save an old unmerged configuration, you can restore that configuration or you can use the or management center configuration rollback feature, and the device will be in an unmerged state with the Diagnostic configuration intact.

Before you begin

- To view the current mode of the device, enter the **show management-interface convergence** command at the threat defense CLI. The following output shows that the Management interfaces are merged:

```
> show management-interface convergence
management-interface convergence
>
```

The following output shows that the Management interfaces are not merged:

```
> show management-interface convergence
no management-interface convergence
>
```

- For High Availability pairs and clusters, perform this task on the active/control unit. The merged configuration will be replicated automatically to the standby/data units.

Procedure

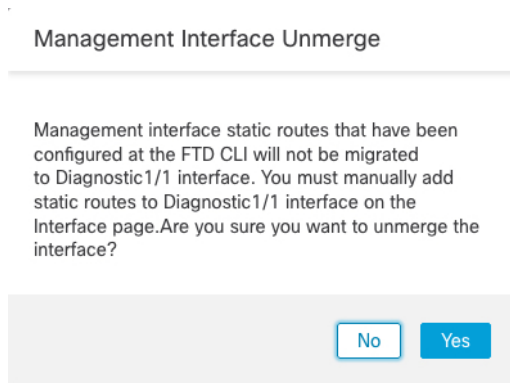**Step 1**   Choose **Devices** > **Device Management**, and click **Edit** (✎) for your threat defense. The **Interfaces** page is selected by default. .

Step 2   For the Management interface, click **Unmerge Management Interface** (↺).

Figure 40: Management Interface Selection

| 🖧 Management1/1 | management | Physical | | Global | 🔍 ↺ |

Step 3   Click **Yes** to confirm that you want to unmerge the interface.

Figure 41: Unmerge Confirmation

Management Interface Unmerge

Management interface static routes that have been configured at the FTD CLI will not be migrated to Diagnostic1/1 interface. You must manually add static routes to Diagnostic1/1 interface on the Interface page.Are you sure you want to unmerge the interface?

No   Yes

Step 4   Deploy the new unmerged configuration.

Note   If you restore a configuration that is merged, or roll back to a merged configuration, then the device will revert to that merged configuration.

After the merge, the Management interface is no longer shown on the **Interfaces** page.

History for Interfaces

Feature	Minimum Management Center	Minimum Threat Defense	Details
Loopback and Management type interface group objects	Any	7.4	You can now create interface group objects that include only management-only interfaces or only loopback interfaces. You can then use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are supported for any feature that supports loopback interfaces. Note that DNS does not support management interfaces. New/Modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merged Management and Diagnostic interfaces	Any	7.4	For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically.
			If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Note that support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible.
			Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration.
			New/Modified screens: **Devices** > **Device Management** > **Interfaces**
			New/Modified commands: **show management-interface convergence**
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to Clause 108 RS-FEC from Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers	Any	7.2.4/7.3	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to Clause 108 RS-FEC instead of Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers.
			Supported platforms: Secure Firewall 3100
LLDP support for the Firepower 2100, Secure Firewall 3100	Any	7.2	You can enable Link Layer Discovery Protocol (LLDP) for Firepower 2100 and Secure Firewall 3100 interfaces.
			New/Modified screens:
			Devices > **Device Management** > **Interfaces** > **Hardware Configuration** > **Network Connectivity**
			New/Modified commands: **show lldp status, show lldp neighbors, show lldp statistics**
			Supported platforms: Firepower 2100, Secure Firewall 3100
Pause Frames for Flow Control for the Secure Firewall 3100	Any	7.2	If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.
			New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Network Connectivity**
			Supported platforms: Secure Firewall 3100

Feature	Minimum Management Center	Minimum Threat Defense	Details
Support for Forward Error Correction for the Secure Firewall 3100	Any	7.1	Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction (FEC). FEC is enabled by default and set to Auto. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **Hardware Configuration**
Support for setting the speed based on the SFP for the Secure Firewall 3100	Any	7.1	The Secure Firewall 3100 supports speed detection for interfaces based on the SFP installed. Detect SFP is enabled by default. This option is useful if you later change the network module to a different model, and want the speed to update automatically. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **Hardware Configuration**
LLDP support for the Firepower 1100	Any	7.1	You can enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **LLDP** New/Modified commands: **show lldp status, show lldp neighbors, show lldp statistics** Supported platforms: Firepower 1100
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved	Any	7.1	Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in management center, hardware changes are detected more effectively. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Speed** Supported platforms: Firepower 1000, 2100, Secure Firewall 3100
Firepower 1100/2100 series fiber interfaces now support disabling auto-negotiation	Any	6.7	You can now configure a Firepower 1100/2100 series fiber interface to disable flow control and link status negotiation. Previously, when you set the fiber interface speed (1000 or 10000 Mbps) on these devices, flow control and link status negotiation was automatically enabled. You could not disable it. Now, you can deselect **Auto-negotiation** and set the speed to 1000 to disable flow control and link status negotiation. You cannot disable negotiation at 10000 Mbps. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Speed** Supported platforms: Firepower 1100, 2100