



Interface Overview

The FTD device includes data interfaces that you can configure in different modes, as well as a management/diagnostic interface.

- [Management/Diagnostic Interface, on page 1](#)
- [Interface Mode and Types, on page 2](#)
- [Security Zones and Interface Groups, on page 3](#)
- [Auto-MDI/MDIX Feature, on page 5](#)
- [Default Settings for Interfaces, on page 5](#)
- [Create Security Zone and Interface Group Objects, on page 6](#)
- [Enable the Physical Interface and Configure Ethernet Settings, on page 7](#)
- [Configure EtherChannel Interfaces, on page 9](#)
- [Sync Interface Changes with the FMC, on page 16](#)
- [Manage the Network Module for the Secure Firewall 3100, on page 19](#)
- [History for Interfaces, on page 30](#)

Management/Diagnostic Interface

The physical management interface is shared between the Diagnostic logical interface and the Management logical interface.

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 FMC. It uses its own IP address and static routing. You can configure its settings at the CLI using the **configure network** command. If you change the IP address at the CLI after you add it to the FMC, you can match the IP address in the Firepower Management Center in the **Devices > Device Management > Devices > Management** area.

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

Diagnostic Interface

The Diagnostic logical interface can be configured along with the rest of the data interfaces on the **Devices > Device Management > Interfaces** screen. Using the Diagnostic interface is optional (see the routed and transparent mode deployments for scenarios). The Diagnostic interface only allows management traffic, and

does not allow through traffic. It does not support SSH; you can SSH to data interfaces or to the Management interface only. The Diagnostic interface is useful for SNMP or syslog monitoring.



Note Although the Diagnostic and Management interfaces share a physical port, you must assign different IP addresses to each interface on the same network.

Interface Mode and Types

You can deploy FTD 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 FTD 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 FTD 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 FTD 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 FTD is deployed inline, but the network traffic flow is undisturbed. Instead, the FTD 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 FTD and the network as if the FTD were inline and analyze the kinds of intrusion events the FTD 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 FTD inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the FTD and the network.



Note Tap mode *significantly* impacts FTD 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 FTD in a passive deployment, the FTD 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 FTD 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 Diagnostic/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.

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

Interface Objects and Multitenancy

In a multidomain deployment, you can create interface objects at any level. An interface object created in an ancestor domain can contain interfaces that reside on devices in different domains. In this situation, subdomain users viewing the ancestor interface object configuration in the object manager can see only the interfaces in their domain.

Unless restricted by role, subdomain users can view **and** edit interface objects created in ancestor domains. Subdomain users can add and delete interfaces from these interface objects. They cannot, however, delete or rename the interface objects. You can neither view nor edit interface objects created in descendant domains.

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 FMC. 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 FMC.

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, 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 [Security Zones and Interface Groups, on page 3](#).

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 Diagnostic 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 FMC, you need to refresh the interface listing by clicking **Sync Interfaces from device** on the top left of **Interfaces**. For the Secure Firewall 3100, which supports hot swapping, see [Manage the Network Module for the Secure Firewall 3100, on page 19](#) before you change interfaces on a device.

Procedure

-
- Step 1** Select **Devices > Device Management** and click **Edit** (✎) for your FTD 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 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 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-AOCxM	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate

Step 6 (Optional) (Firepower 1100) Enable Link Layer Discovery Protocol (LLDP) by clicking **Hardware Configuration > LLDP**.

- **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 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 8 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 9 Click **OK**.

Step 10 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 11 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.

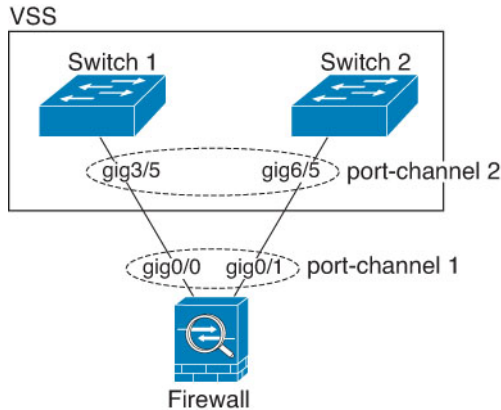
The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The interface is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port numbers and VLAN numbers.

Connecting to an EtherChannel on Another Device

The device to which you connect the FTD 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 FTD 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.

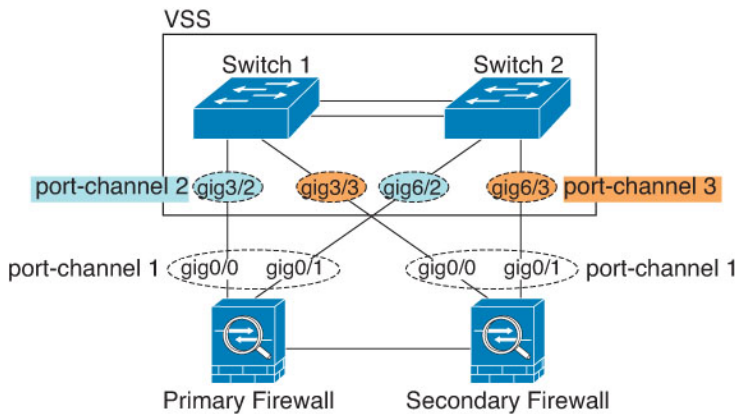
Figure 1: Connecting to a VSS/vPC



Note If the FTD device is in transparent firewall mode, and you place the FTD device between two sets of VSS/vPC switches, then be sure to disable Unidirectional Link Detection (UDLD) on any switch ports connected to the FTD 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 FTD device in an Active/Standby failover deployment, then you need to create separate EtherChannels on the switches in the VSS/vPC, one for each FTD device. On each FTD device, a single EtherChannel connects to both switches. Even if you could group all switch interfaces into a single EtherChannel connecting to both FTD devices (in this case, the EtherChannel will not be established because of the separate FTD system IDs), a single EtherChannel would not be desirable because you do not want traffic sent to the standby FTD 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 (LACPDU) 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 FTD 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, FMC-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 FMC for the Firepower 4100/9300 or the FTDv. 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, 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 FTD EtherChannel must also support 802.3ad EtherChannels.
- The FTD device does not support LACPDU s 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 FTD device will drop the tagged LACPDU s. Be sure to disable native VLAN tagging on the neighboring switch.
- Devices do not support LACP rate fast, except for the ISA 3000; LACP always uses the normal rate. This setting is not configurable. Note that the Firepower 4100/9300, which configures EtherChannels in FXOS, has the LACP rate set to fast by default; on these platforms, the rate is configurable.
- In Cisco IOS software versions earlier than 15.1(1)S2, FTD did not support connecting an EtherChannel to a switch stack. With default switch settings, if the FTD 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 FTD 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, 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 FTD 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

The screenshot shows the 'Add Ether Channel Interface' configuration window. The 'General' tab is selected. The configuration fields are as follows:

- Name:** dmz
- Enabled:**
- Management Only:**
- Description:** (empty)
- Mode:** None
- Security Zone:** dmz_zone
- MTU:** 1500 (range: 64 - 9198)
- Priority:** 0 (range: 0 - 65535)
- Propagate Security Group Tag:**
- Ether Channel ID *:** 1

Buttons for 'Cancel' and 'OK' are located at the bottom right of the window.

- 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 FTD 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 11](#).
- **LACP Mode**—Choose Active, Passive, or On. We recommend using Active mode (the default).
- (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) Add a VLAN subinterface. See [Add a Subinterface](#).

Step 11 Configure the routed or transparent mode interface parameters. See [Configure Routed Mode Interfaces](#) or [Configure Bridge Group Interfaces](#).

Sync Interface Changes with the FMC

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

- Event sent from the device
- Sync when you deploy from the FMC

If the FMC 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 FMC that need to be synced:

- Addition or deletion of physical interfaces—Adding a new interface, or deleting an unused interface has minimal impact on the FTD 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 FTD 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 FMC.

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

- FMC access interface changes—If you configure a data interface for managing FMC using the **configure network management-data-interface** command, you must manually make matching configuration changes in FMC 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 FMC; you should wait until the device is stable, and then re-sync.

Before you begin

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

Procedure

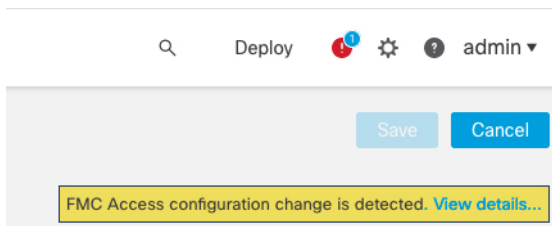
- Step 1** Select **Devices > Device Management** and click **Edit** (✎) for your FTD device. The **Interfaces** page is selected by default.
- Step 2** If required, click **Sync Device** on the top left of **Interfaces**.
- Step 3** After the changes are detected, see the following steps.

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 FMC 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 FTD by manually configuring them on the FMC.

For example, the pink highlights below show configuration that exists on the FTD but not yet on the FMC.

FMC Access - Configuration Details ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

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

FMC Access - Configuration Details ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

c) Click **Acknowledge**.

We recommend that you do not click **Acknowledge** until you have finished the FMC configuration, and are ready to deploy. Clicking **Acknowledge** removes the block on deployment. The next time you deploy,

the FMC configuration will overwrite any remaining conflicting settings on the FTD. It is your responsibility to manually fix the configuration in the FMC 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

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

172.16.0.51 (Chassis Operations)
Network module and interface breakout details for device.

Interfaces

Refresh Sync Modules

Network Module 1

CONSOLE

MGMT

USB

1/1

1/2

1/3

1/4

1/5

1/6

1/7

1/8

1/9

1/10

1/11

1/12

1/13

1/14

1/15

1/16

Network Module 2

2/1

2/3

2/5

2/7

2/2

2/4

2/6

2/8

Physical Interfaces

This view lists only the physical interfaces to perform chassis related advanced operations. To view complete list of physical and logical interfaces, navigate to [Interface page in device details](#)

Interface Name	Duplex	Auto Negotiation	Admin FEC	Admin Speed	Media Type
Ethernet1/1	FULL	No	AUTO	1gbps	rj45
Ethernet1/2	FULL	No	AUTO	1gbps	rj45
Ethernet1/3	FULL	No	AUTO	1gbps	rj45
Ethernet1/4	FULL	No	AUTO	1gbps	rj45

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.

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 FTD 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 7: Manage Chassis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	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.


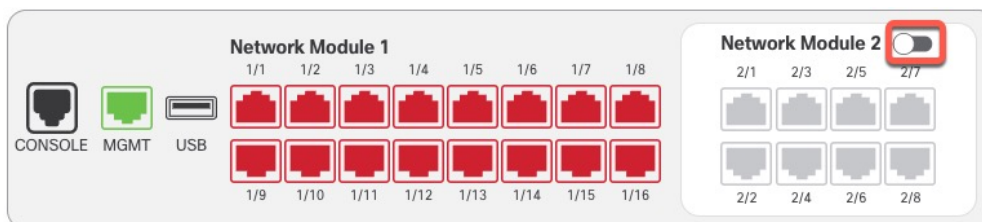
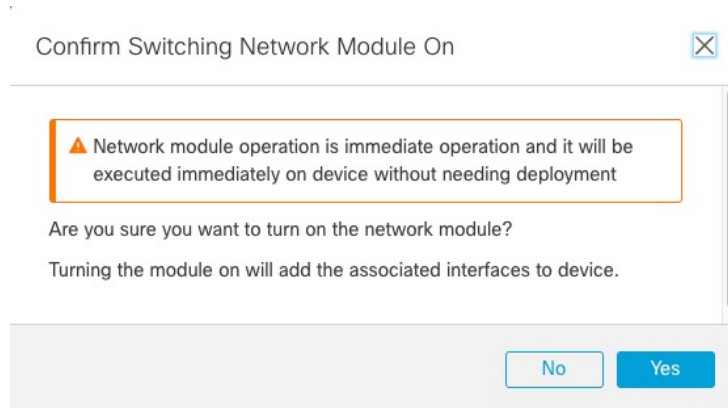
- Step 4** Click **Sync Modules** to update the page with the new network module details.
- Step 5** On the interfaces graphic, click the slider () to enable the network module.

Figure 8: Enable the Network Module



- Step 6** You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 9: Confirm Enable



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 10: Go to Interface Page

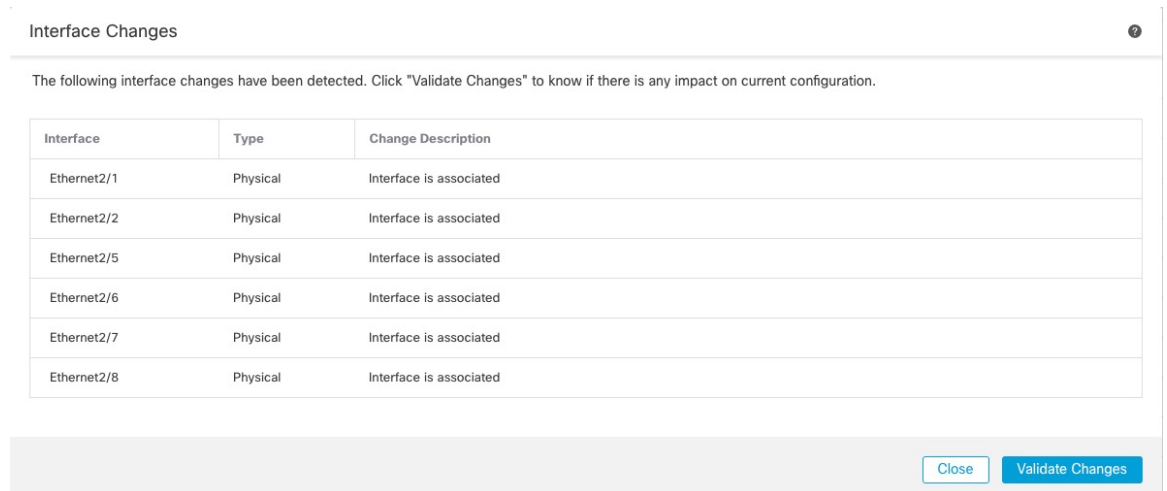
▲ This device has configuration changes that were performed directly on the device. Visit [Interface page](#) in device details

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 11: View Interface Changes

Interface configuration has changed on device. [Click to know more.](#)

Figure 12: Interface 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 13: Manage Chassis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 <small>Snort 3</small> 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.


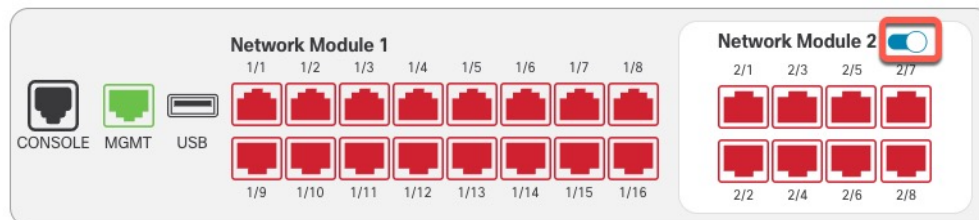
Step 3 On the interfaces graphic, click the slider () to disable the network module.

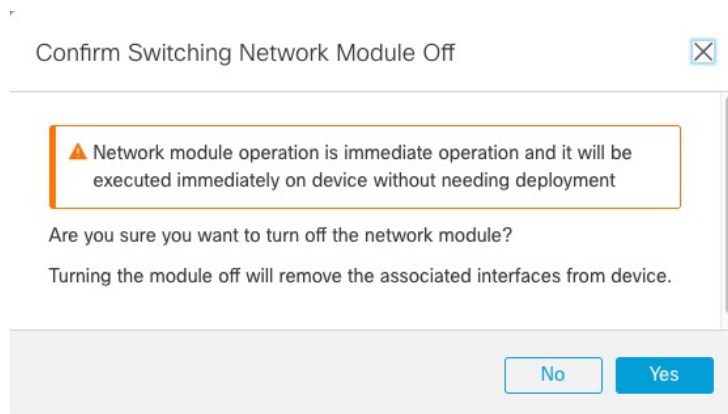
Figure 14: Disable the Network Module



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 15: 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.


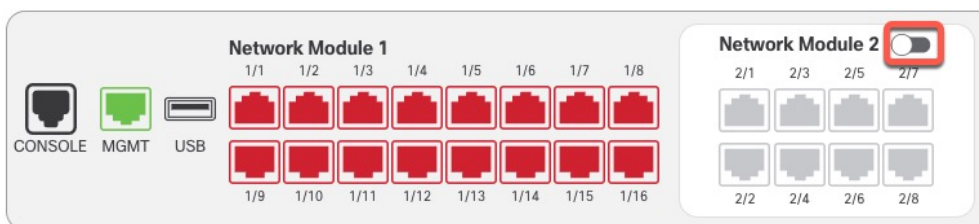
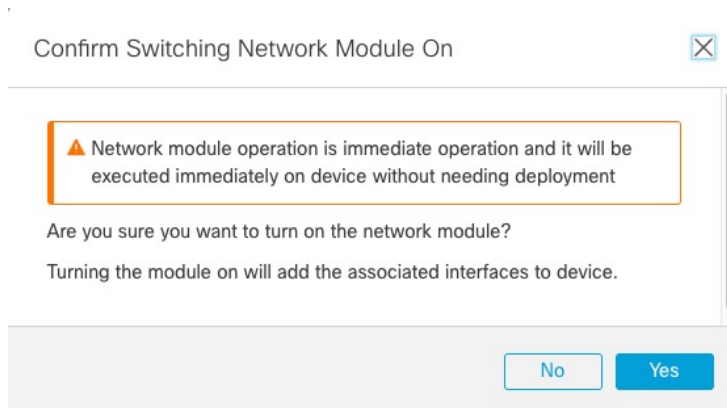
Step 6 In the FMC, enable the new module by clicking the slider ().

Figure 16: Enable the Network Module



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

Figure 17: Confirm Enable



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 18: Manage Chassis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	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.


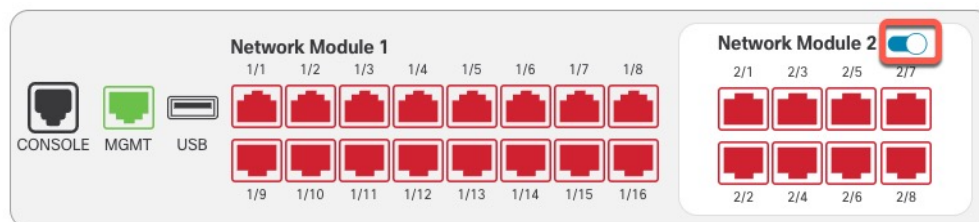
Step 3 On the interfaces graphic, click the slider () to disable the network module.

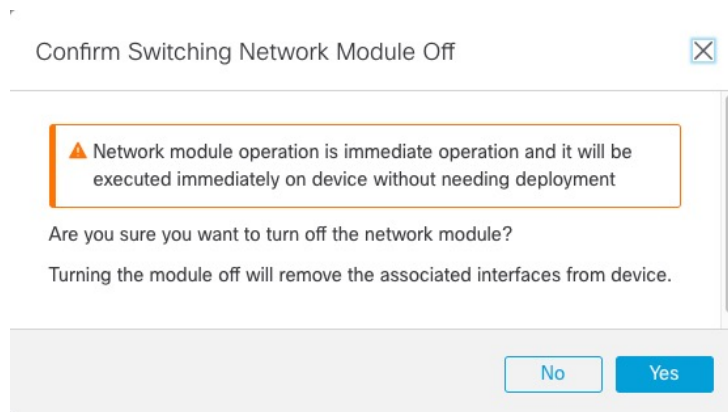
Figure 19: Disable the Network Module



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 20: 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 FTD High Availability Pair](#)), and reboot the former control node/active unit.

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


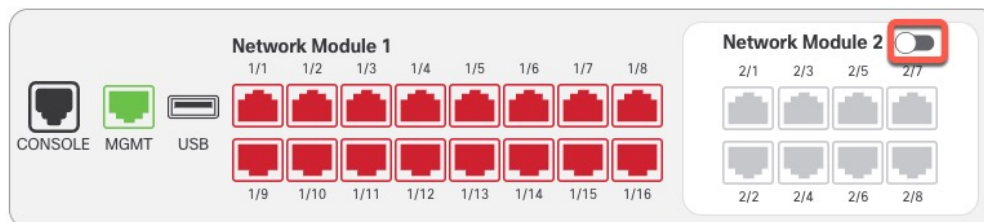
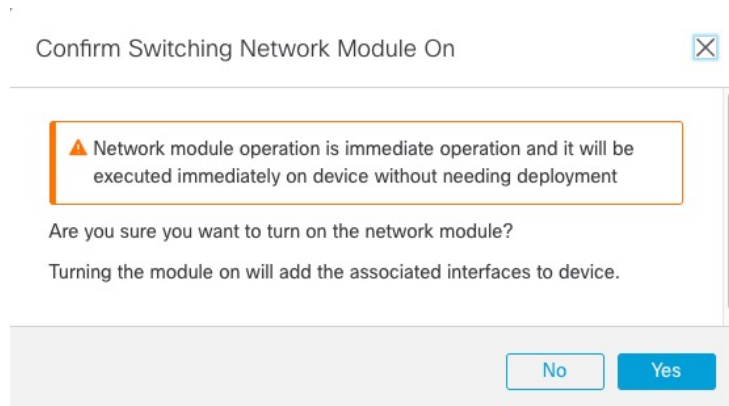
Step 8 Enable the new module by clicking the slider ()

Figure 21: Enable the Network Module



Step 9 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 22: 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 23: Go to Interface Page

 This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

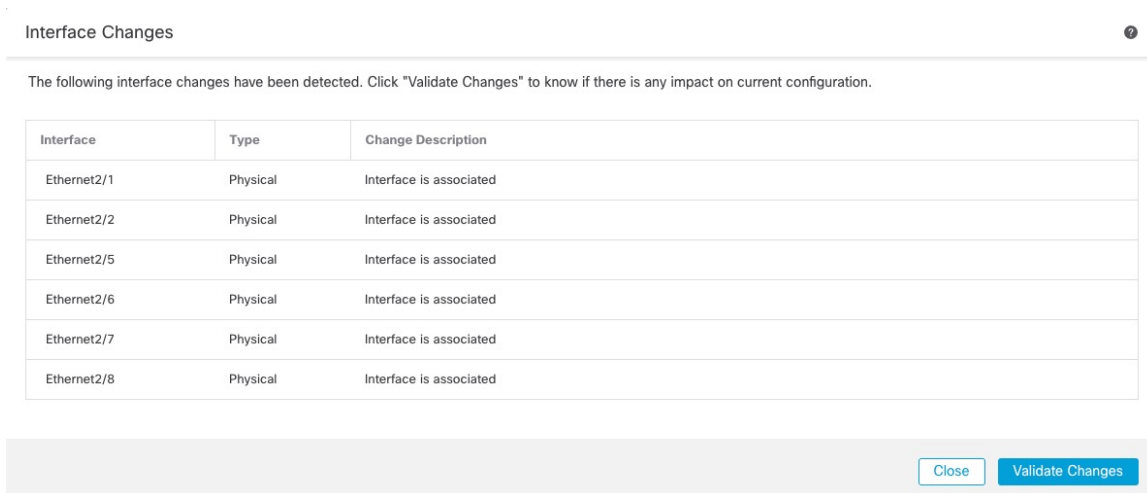
Step 11 If the network module has *fewer* interfaces:

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

Figure 24: View Interface Changes

Interface configuration has changed on device. [Click to know more.](#)

Figure 25: 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 26: Manage Chassis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 <small>Short 3</small> 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.


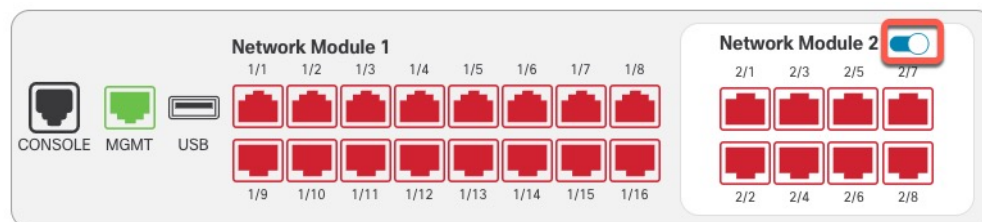
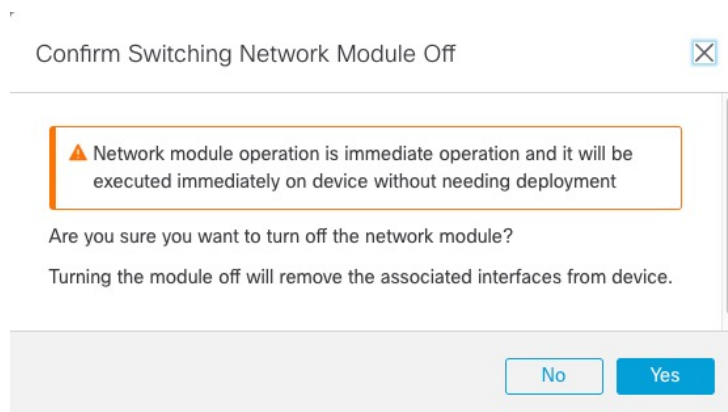
Step 2 On the interfaces graphic, click the slider () to disable the network module.

Figure 27: Disable the Network Module



Step 3 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 28: 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 29: Go to Interface Page

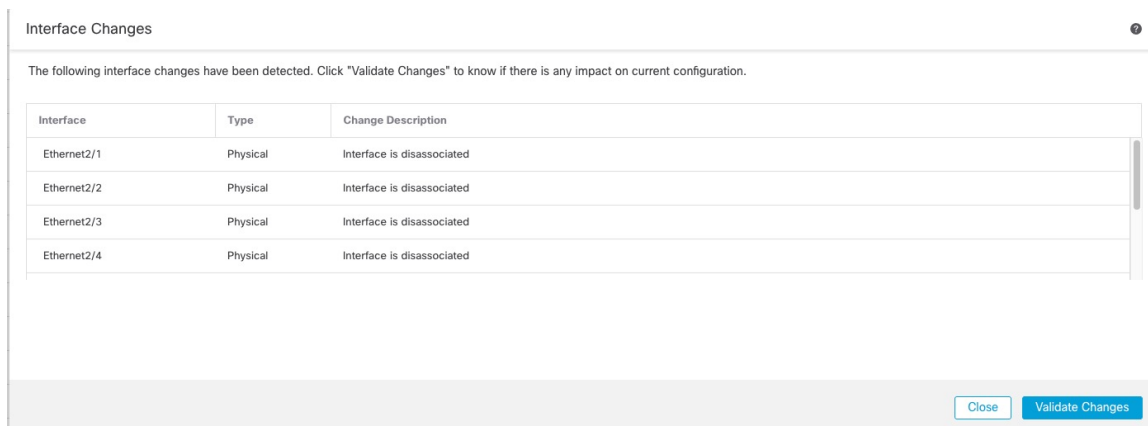
▲ This device has configuration changes that were performed directly on the device. Visit [Interface page](#) in device details

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

Figure 30: 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 31: 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 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 FTD High Availability Pair](#)), and reboot the former control node/active unit.

History for Interfaces

Feature	Minimum FMC	Minimum FTD	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 FMC, 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