

Logical Devices on the Firepower 4100/9300

The Firepower 4100/9300 is a flexible security platform on which you can install one or more *logical devices*.

You must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Firewall Chassis Manager or the FXOS CLI. You cannot perform these tasks in the Firewall Device Manager.

This chapter describes basic interface configuration and how to add a standalone or High Availability logical device using the Firewall Chassis Manager. To use the FXOS CLI, see the FXOS CLI configuration guide. For more advanced FXOS procedures and troubleshooting, see the FXOS configuration guide.

- Supported interfaces, on page 1
- Requirements and prerequisites for Firepower 9300 hardware and software combinations, on page 3
- Guidelines and limitations for logical devices, on page 4
- Configure interfaces, on page 4
- Configure a Logical Device, on page 8
- History for Logical Devices, on page 18

Supported interfaces

The Firepower 4100/9300 chassis supports physical interfaces and EtherChannel (port-channel) interfaces. EtherChannel interfaces can include up to 16 member interfaces of the same type.

Chassis management interface

A chassis management interface is a network interface that is used for management of the FXOS chassis by SSH or Firewall Chassis Manager.

The chassis management interface appears at the top of the **Interfaces** tab as **MGMT**. You can only enable or disable this interface on the **Interfaces** tab.

To configure parameters for this interface, you must configure them from the CLI. To view information about this interface in the FXOS CLI, connect to local management and show the management port:

Firepower # **connect local-MGMT**

Firepower(local-MGMT) # **show MGMT-port**

Note The chassis management interface does not support jumbo frames.

Interface types

Physical interfaces and EtherChannel (port-channel) interfaces are categorized into different types by their specific functions.

for different purposes.

These interface types are available, each defined by its specific function and configuration requirements:

- Data—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.
- Data-sharing—Use for regular data. These data interfaces are supported only with container instances and can be shared by one or more logical devices or container instances (Firewall Threat Defense using Firewall Management Center only).
- Mgmt—Use to manage application instances. These interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device. Depending on your application and manager, you can later enable management from a data interface; but you must assign a management interface to the logical device even if you don't intend to use it after you enable data management. For information about the separate chassis management interface, see Chassis management interface, on page 1.

Note Changing the management interface will cause reboot of the logical device. For example, changing management interface from e1/1 to e1/2 causes the logical device to reboot so that the change can take effect.

- Eventing—Use as a secondary management interface for Firewall Threat Defense-using-Firewall Management Center devices.

Note A virtual Ethernet interface is allocated when each application instance is installed. If the application does not use an eventing interface, then the virtual interface will be in an admin down state.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. The Cluster type is only supported on EtherChannel interfaces.The Firewall Device Manager and Security Cloud Control do not support clustering.

FXOS interfaces and application interfaces

The Firepower 4100/9300 manages the basic Ethernet settings of physical interfaces and EtherChannel (port-channel) interfaces. Within the application, you configure higher-level settings. For example, you can only create EtherChannels in FXOS, but you can assign an IP address to the EtherChannel within the application.

These sections describe the interaction between FXOS and the application for interfaces.

VLAN subinterfaces

For all logical devices, you can create VLAN subinterfaces within the application.

Independent interface states in the chassis and in the application

You can administratively enable and disable interfaces in both the chassis and the application. 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 application.

Requirements and prerequisites for Firepower 9300 hardware and software combinations

Review these baseline requirements and prerequisites for FXOS hardware and software combinations.

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See these requirements:

- Security Module Types—You can install modules of different types in the Firepower 9300. For example, you can install the SM-48 as module 1, SM-40 as module 2, and SM-56 as module 3.
- Native and Container instances—When you install a container instance on a security module, that module can only support other container instances. A native instance uses all of the resources for a module, so you can only install a single native instance on a module. You can use native instances on some modules, and container instances on the other module. For example, you can install a native instance on module 1 and module 2, but container instances on module 3.
- High Availability—High Availability is only supported between same-type modules on the Firepower 9300. However, the two chassis can include mixed modules. For example, each chassis has an SM-40, SM-48, and SM-56. You can create High Availability pairs between the SM-40 modules, between the SM-48 modules, and between the SM-56 modules.
- ASA and Firewall Threat Defense application types—You can install different application types on separate modules in the chassis. For example, you can install ASA on module 1 and module 2, and Firewall Threat Defense on module 3.
- ASA or Firewall Threat Defense versions—You can run different versions of an application instance type on separate modules, or as separate container instances on the same module. For example, you can install the Firewall Threat Defense 6.3 on module 1, Firewall Threat Defense 6.4 on module 2, and Firewall Threat Defense 6.5 on module 3.

Guidelines and limitations for logical devices

This section provides guidelines and limitations for configuring and managing logical devices.

Guidelines and limitations for interface configuration

Default MAC addresses

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- EtherChannels—For an EtherChannel, 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. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.

General Guidelines and Limitations

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.
- The two units in a High Availability Failover configuration must:
  - Be the same model.
  - Have the same interfaces assigned to the High Availability logical devices.
  - Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.
- For more information, see System Requirements for High Availability.

Configure interfaces

By default, physical interfaces are disabled. You can enable interfaces, add EtherChannels, and edit interface properties.

Enable or disable an interface

You can change the **Admin State** of each interface to be enabled or disabled. By default, physical interfaces are disabled.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The Interfaces page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 To enable the interface, click the disabled **Slider disabled** () so that it changes to the enabled **Slider enabled** ().

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from gray to green.

Step 3 To disable the interface, click the enabled **Slider enabled** () so that it changes to the disabled **Slider disabled** ().

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from green to gray.

Configure a physical interface

Configure physical interface settings including enable/disable state, speed, duplex, type, and auto-negotiation to ensure proper network connectivity.

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, it must be physically enabled in FXOS and logically enabled in the application.

Note

- For QSFPH40G-CUxM, auto-negotiation is enabled by default and you cannot disable it.
- If you replace an SFP on a port with a different SFP module, the speed, duplex, and auto-negotiation of the interface is not updated automatically. You must manually reconfigure the interface.

Before you begin

An interface that is already a member of an EtherChannel cannot be modified individually. Be sure to configure settings before you add it to the EtherChannel.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Edit** in the row for the interface you want to edit to open the **Edit Interface** dialog box.

Step 3 Configure the interface settings:

a) To enable the interface, check the **Enable** check box. To disable the interface, uncheck the **Enable** check box.

b) Choose the interface **Type**:

See Interface types, on page 2 for details about interface type usage.

- **Data**
- **Mgmt**
- **Cluster**—Do not choose the **Cluster** type; by default, the cluster control link is automatically created on Port-channel 48.

c) Choose the speed of the interface from the **Speed** drop-down list.

d) If your interface supports **Auto Negotiation**, click the **Yes** or **No** radio button.

If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the platform interface as well. For example, N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, for the port to be connected you must disable the default auto-negotiation on the platform and the switch.

e) Choose the duplex of the interface from the **Duplex** drop-down list.

f) Choose a previously-configured **Network Control Policy**. For more information on how to configure a Network Control Policy, see Configure a Network Control Policy.

g) Explicitly configure **Debounce Time (ms)**. Enter a value between 0-15000 milli-seconds.

Note
Configuring Debounce Time is not supported on 1G interfaces.

Step 4 Click **OK**.

Add an EtherChannel (port channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. 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. 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 Data 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.
- On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

Note It may take up to three minutes for an EtherChannel to come up to an operational state if you change its mode from On to Active or from Active to On.

The Firepower 4100/9300 only supports EtherChannels in Active LACP mode so that each member interface 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.

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.

When the Firepower 4100/9300 creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management interface for a standalone logical device
- The EtherChannel is added as a management interface or cluster control link for a logical device that is part of a cluster
- The EtherChannel is added as a data interface for a logical device that is part of a cluster and at least one unit has joined the cluster

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** or **Down** state.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Add Port Channel** above the interfaces table to open the **Add Port Channel** dialog box.

Step 3 Enter an ID for the port channel in the **Port Channel ID** field. Valid values are between 1 and 47.

Port-channel 48 is reserved for the cluster control link when you deploy a clustered logical device. If you do not want to use Port-channel 48 for the cluster control link, you can delete it and configure a Cluster type EtherChannel with a different ID. For intra-chassis clustering, do not assign any interfaces to the Cluster EtherChannel.

Step 4 To enable the port channel, check the **Enable** check box. To disable the port channel, uncheck the **Enable** check box.

Step 5 Choose the interface **Type**:

See Interface types, on page 2 for details about interface type usage.

- **Data**

- **Mgmt**
- **Cluster**

Step 6 Set the required **Admin Speed** for the member interfaces from the drop-down list.

If you add a member interface that is not at the specified speed, it will not successfully join the port channel.

Step 7 For Data interfaces, choose the LACP port-channel **Mode**, **Active** or **On**.

For non-Data interfaces, the mode is always active.

Step 8 Set the required **Admin Duplex** for the member interfaces, **Full Duplex** or **Half Duplex**.

If you add a member interface that is configured with the specified duplex, it will not successfully join the port channel.

Step 9 To add an interface to the port channel, select the interface in the **Available Interface** list and click **Add Interface** to move the interface to the Member ID list.

You can add up to 16 member interfaces of the same media type and capacity. The member interfaces must be set to the same speed and duplex, and must match the speed and duplex that you configured for this port channel. 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.

Tip
You can add multiple interfaces at one time. To select multiple individual interfaces, click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

Step 10 To remove an interface from the port channel, click the **Delete** button to the right of the interface in the Member ID list.

Step 11 Click **OK**.

Configure a Logical Device

Add a standalone logical device or a High Availability pair on the Firepower 4100/9300.

Add a Standalone Firewall Threat Defense for the Firewall Device Manager

You can use the Firewall Device Manager with a native instance. Container instances are not supported. Standalone logical devices work either alone or in a High Availability pair.

Before you begin

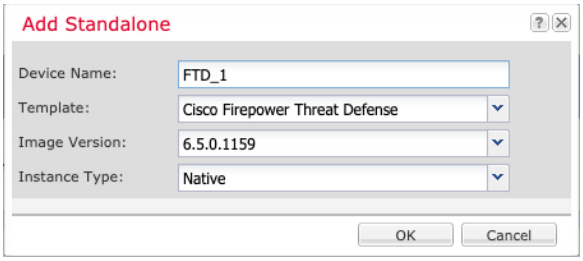
- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).
- You must also configure at least one Data type interface.
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - DNS server IP address
  - Firewall Threat Defense hostname and domain name

Procedure

Step 1 Choose **Logical Devices**.

Step 2 Click **Add** > **Standalone**, and set the following parameters:



a) Provide a **Device Name**.

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

Note
You cannot change this name after you add the logical device.

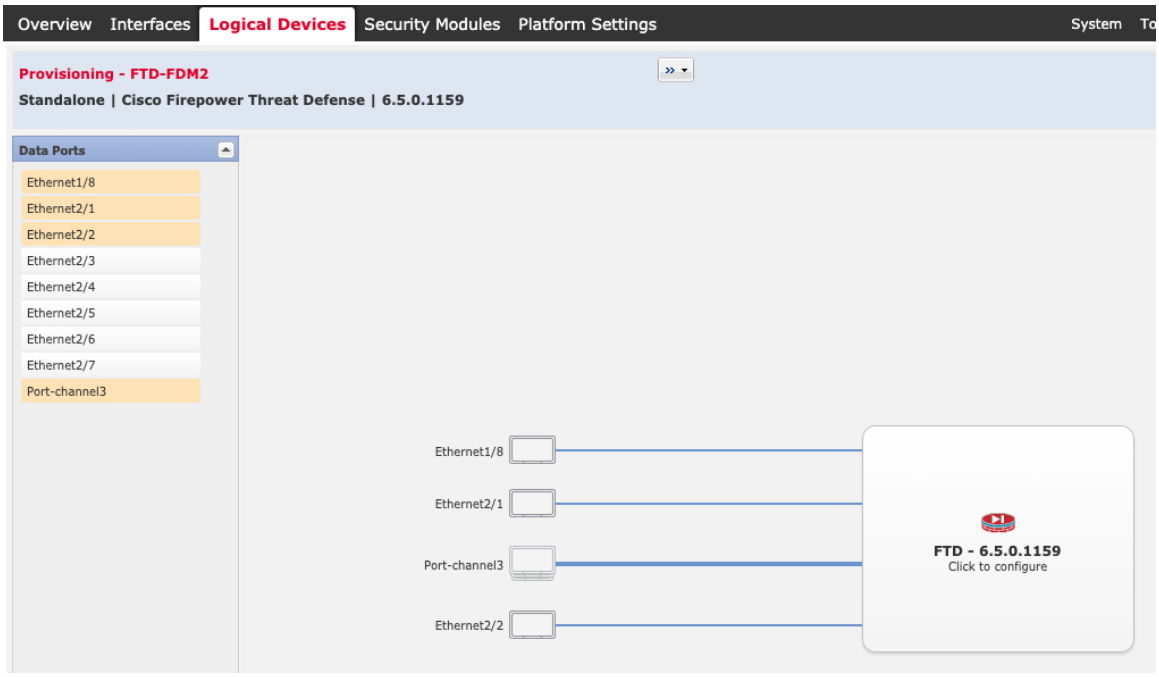
b) For the **Template**, choose **Cisco Firepower Threat Defense**.
c) Choose the **Image Version**.
d) Choose the **Instance Type**: **Native**.

Container instances are not supported with the Firewall Device Manager.

e) Click **OK**.

You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each interface that you want to assign to the device.

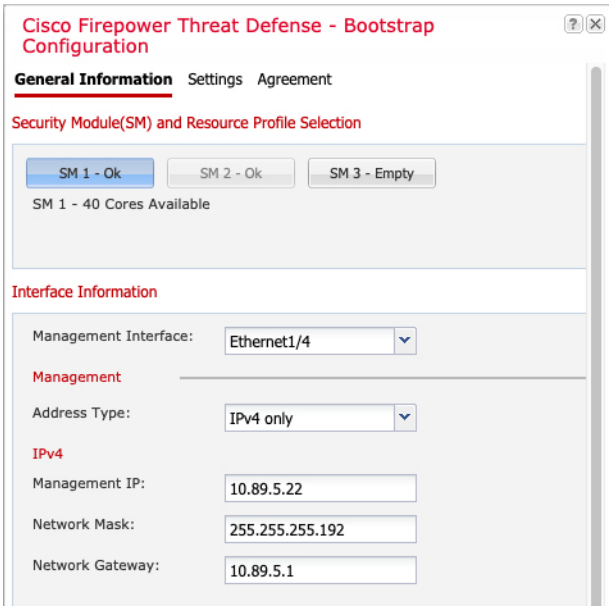


You can only assign data interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in the Firewall Device Manager, including setting the IP addresses.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:



a) (For the Firepower 9300) Under **Security Module Selection** click the security module that you want to use for this logical device.
b) Choose the **Management Interface**.

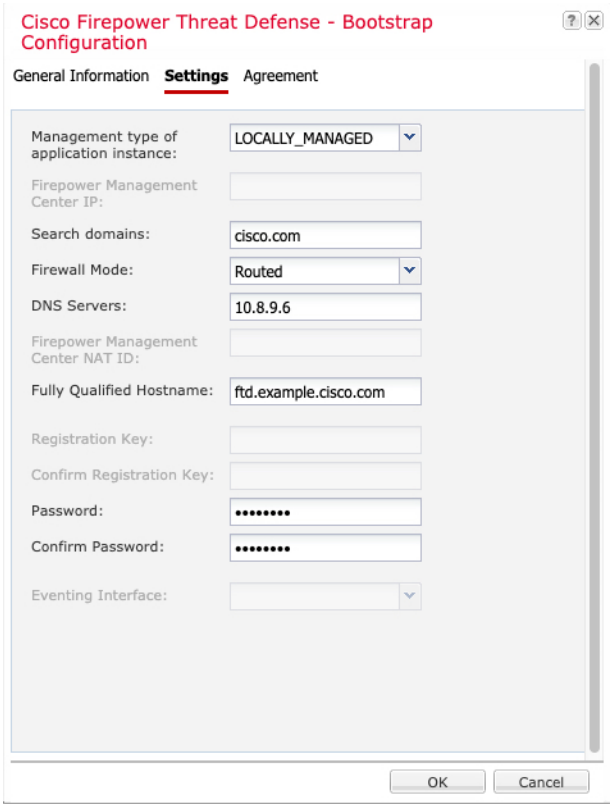
   This interface is used to manage the logical device. This interface is separate from the chassis management port.

c) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.
d) Configure the **Management IP** address.

   Set a unique IP address for this interface.

e) Enter a **Network Mask** or **Prefix Length**.
f) Enter a **Network Gateway** address.

Step 6 On the **Settings** tab, complete the following:



a) In the **Management type of application instance** drop-down list, choose **LOCALLY_MANAGED**.

   Native instances also support the Secure Firewall Management Center as a manager. If you change the manager after you deploy the logical device, then your configuration is erased and the device is reinitialized.

b) Enter the **Search Domains** as a comma-separated list.
c) The **Firewall Mode** only supports **Routed** mode.
d) Enter the **DNS Servers** as a comma-separated list.
e) Enter the **Fully Qualified Hostname** for the Firewall Threat Defense.
f) Enter a **Password** for the Firewall Threat Defense admin user for CLI access.

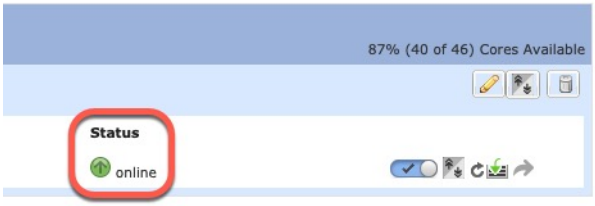
Step 7 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.





Step 10 See the Firewall Device Manager configuration guide to start configuring your security policy.

Add a high availability pair

Firewall Threat Defense High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

Before you begin

Refer to System Requirements for High Availability.

Procedure

Step 1 Allocate the same interfaces to each logical device.

Step 2 Allocate 1 or 2 data interfaces for the failover and state link(s).

These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.

Step 3 Enable High Availability on the logical devices. Refer to High Availability (Failover).

Step 4 If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.

Change an Interface on a Firewall Threat Defense Logical Device

You can allocate or unallocate an interface, or replace a management interface on the Firewall Threat Defense logical device. You can then sync the interface configuration in the Firewall Management Center or the Firewall Device Manager.

Adding a new interface, or deleting an unused interface has minimal impact on the Firewall 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 Firewall Threat Defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. 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 Firewall Management Center or the Firewall Device Manager.

For the Firewall Device Manager: You can migrate the configuration from one interface to another interface before you delete the old interface.

Before you begin

- Configure your interfaces, and add any EtherChannels according to Configure a physical interface, on page 5 and Add an EtherChannel (port channel), on page 6.
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management or eventing interface with a management EtherChannel, then you need to create the EtherChannel with at least 1 unallocated data member interface, and then replace the current management interface with the EtherChannel. After the Firewall Threat Defense device reboots (management interface changes cause a reboot), and you sync the configuration in the Firewall Management Center or the Firewall Device Manager, you can add the (now unallocated) management interface to the EtherChannel as well.
- For High Availability, make sure you add or remove the interface on all units before you sync the configuration in the Firewall Management Center or the Firewall Device Manager. We recommend that you make the interface changes on the standby unit first, and then on the active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.
- In mult-instance mode, for changing a sub-interface with an another sub-interface with the same vlan tag, you must first remove all the configuration (including nameif config) of the interface and then unalloacte the interface from Firewall Chassis Manager. Once unallocated, add the new interface and then use sync interfaces from the Firewall Management Center.

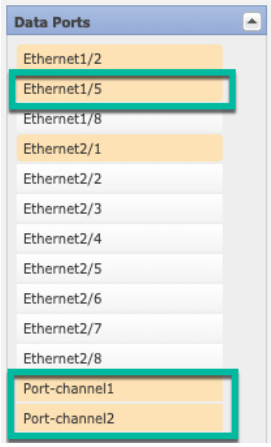
Procedure

Step 1 In the Firewall Chassis Manager, choose **Logical Devices**.

Step 2 Click the **Edit** icon at the top right to edit the logical device.

Step 3 Allocate a new data interface by selecting the interface in the **Data Ports** area.

Do not delete any interfaces yet.



Step 4 Replace the management interface:

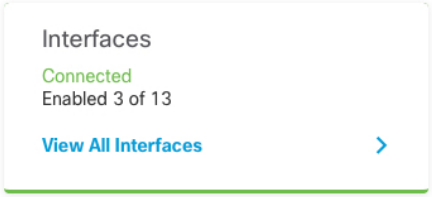
For these types of interfaces, the device reboots after you save your changes.

a) Click the device icon in the center of the page.
b) On the **General** tab, choose the new **Management Interface** from the drop-down list.
c) Click **OK**.

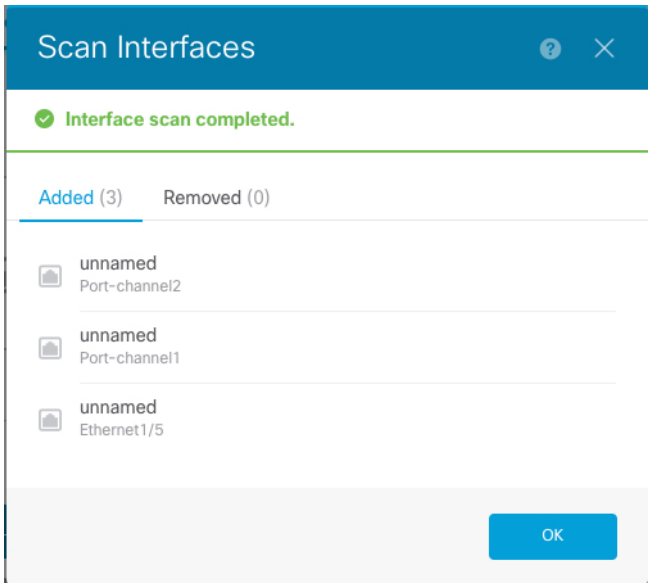
Step 5 Click **Save**.

Step 6 Sync and migrate the interfaces in the Firewall Device Manager.

a) Log into the Firewall Device Manager.
b) Click **Device**, then click the **View All Interfaces** link in the **Interfaces** summary.



c) Click the **Scan Interfaces icon**.
d) Wait for the interfaces to scan, and then click **OK**.



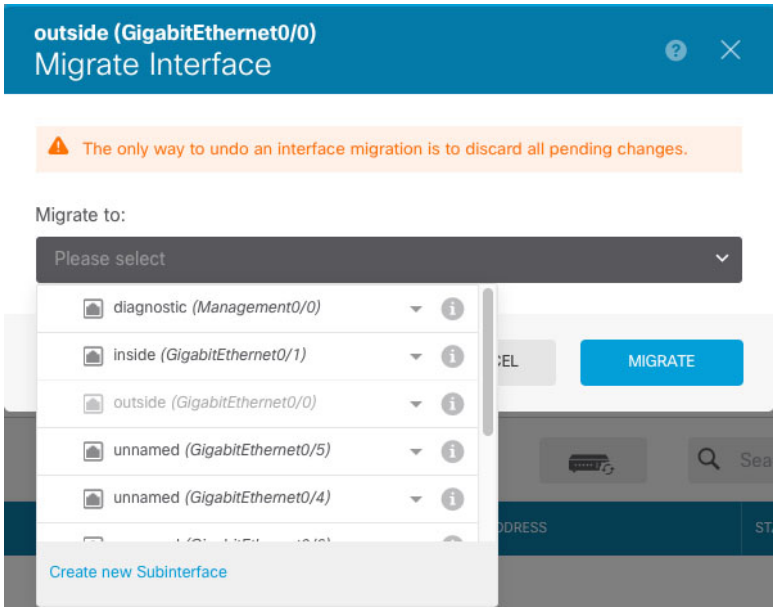
e) Configure the new interfaces with names, IP addresses, and so on.

If you want to use the existing IP address and name of an interface that you want to delete, then you need to reconfigure the old interface with a dummy name and IP address so that you can use those settings on the new interface.

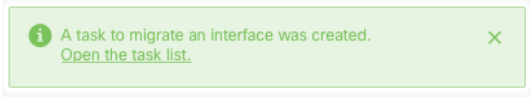
f) To replace an old interface with a new interface, click the Replace icon for the old interface.

This process replaces the old interface with the new interface in all configuration settings that refer to the interface.

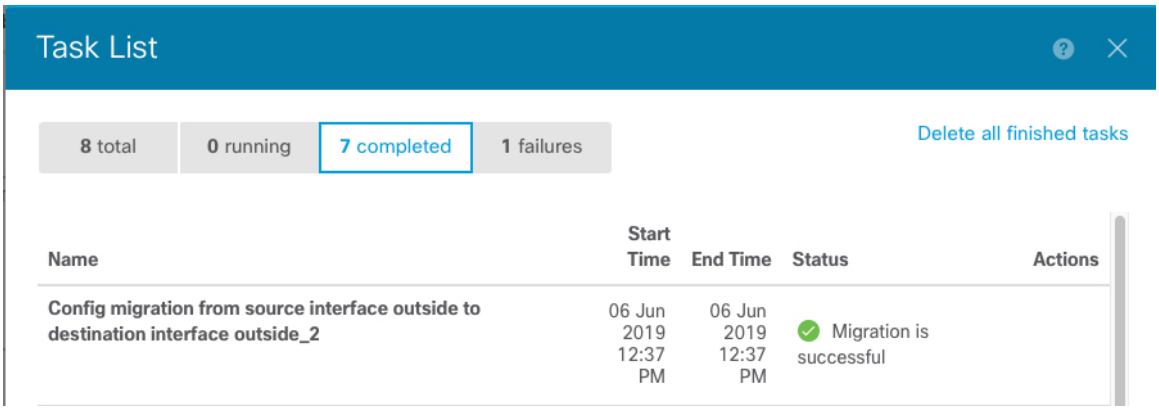
g) Choose the new interface from the **Replacement Interface** drop-down list.



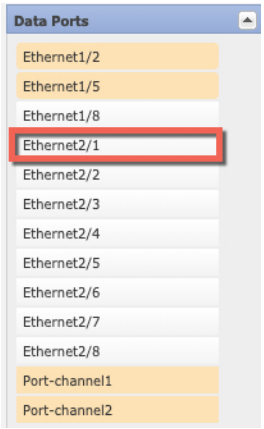
h) A message appears on the **Interfaces** page. Click the link in the message.



i) Check the **Task List** to ensure that the migration was successful.



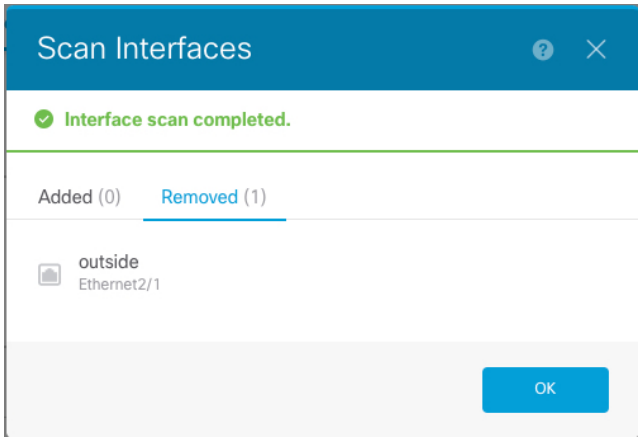
Step 7 In the Firewall Chassis Manager, unallocate a data interface by de-selecting the interface in the **Data Ports** area.



Step 8 Click **Save**.

Step 9 Sync the interfaces again in the Firewall Management Center or the Firewall Device Manager.

Figure 1: Firewall Device Manager Scan Interfaces



Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

Procedure

Step 1 Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2 Connect to the application console.

connect ftd *name*

To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

Step 3 Exit the application console to the FXOS module CLI.

- Firewall Threat Defense—Enter **exit**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

History for Logical Devices

Feature	Version	Details
Support for the Firewall Device Manager on the Firepower 4100/9300.	6.5.0	You can now use the Firewall Device Manager with Firewall Threat Defense logical devices on the Firepower 4100/9300. Firewall Device Manager does not support Multi-Instance capability; only native instances are supported. **Note** Requires FXOS 2.7.1.