



Firepower Threat Defense Logical Devices for the Firepower 4100/9300

The Firepower 4100/9300 is a flexible security platform on which you can install one or more *logical devices*. Before you can add the FTD to the FMC, you must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Firepower Chassis Manager or the FXOS CLI. This chapter describes basic interface configuration and how to add a standalone or High Availability logical device using the Firepower Chassis Manager. To add a clustered logical device, see [Firepower Threat Defense Cluster for the Firepower 4100/9300](#). To use the FXOS CLI, see the FXOS CLI configuration guide. For more advanced FXOS procedures and troubleshooting, see the FXOS configuration guide.

- [About Firepower Interfaces, on page 1](#)
- [About Logical Devices, on page 3](#)
- [Guidelines and Limitations for Logical Devices, on page 3](#)
- [Configure Interfaces, on page 5](#)
- [Configure Logical Devices, on page 7](#)
- [History for Firepower Threat Defense Logical Devices, on page 11](#)

About Firepower 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

The chassis management interface is used for management of the FXOS Chassis by SSH or Firepower Chassis Manager. This interface appears at the top of the **Interfaces** tab as **MGMT**, and you can only enable or disable this interface on the **Interfaces** tab. This interface is separate from the mgmt-type interface that you assign to the logical devices for application management.

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 that the chassis management interface remains up even if the physical cable or SFP module are unplugged, or if the **mgmt-port shut** command is performed.

Interface Types

Each interface can be one of the following types:

- **Data**—Data interfaces cannot be shared between logical devices.
- **Mgmt**—Use management interfaces to manage application instances. They 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. For information about the separate chassis management interface, see [Chassis Management Interface, on page 1](#).

Within the FTD application, the physical management interface is shared between the Diagnostic logical interface and the Management logical interface. The Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firepower Management Center. It uses its own local authentication, IP address, and static routing. See the "Management Interfaces" section in the Firepower Management Center configuration guide *System Configuration* chapter.

The Diagnostic logical interface can be configured along with the rest of the data interfaces on the FMC **Devices > Device Management > Interfaces** screen. Using the Diagnostic interface is optional. The Diagnostic interface only allows management traffic, and does not allow through traffic.

- **Firepower-eventing**—This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the Firepower Management Center configuration guide *System Configuration* chapter. Firepower-eventing 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.
- **Cluster**—Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on Port-channel 48.

Inline Set Link State Propagation for the Firepower Threat Defense

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 system 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.

When you configure an inline set in the FTD application and enable link state propagation, the FTD sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the chassis senses the change and updates the link state of the other interface to match it. Note that the chassis requires up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

About Logical Devices

A logical device lets you run one application instance (either ASA or Firepower Threat Defense) and also one optional decorator application (Radware DefensePro) to form a service chain.

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.



Note For the Firepower 9300, you must install the same application instance type (ASA or Firepower Threat Defense) on all modules in the chassis; different types are not supported at this time. Note that modules can run different versions of an application instance type.

Standalone and Clustered Logical Devices

You can add the following logical device types:

- **Standalone**—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.
- **Cluster**—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three module application instances belong to a single logical device.



Note For the Firepower 9300, all modules must belong to the cluster. You cannot create a standalone logical device on one security module and then create a cluster using the remaining 2 security modules.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

Guidelines and Limitations for Firepower Interfaces

Inline Sets for FTD

- Supported for physical interfaces (both regular and breakout ports) and EtherChannels.
- Link state propagation is supported.

Hardware Bypass

- Supported for the FTD; you can use them as regular interfaces for the ASA.
- The FTD only supports Hardware Bypass with inline sets.
- Hardware Bypass-capable interfaces cannot be configured for breakout ports.
- You cannot include Hardware Bypass interfaces in an EtherChannel and use them for Hardware Bypass; you can use them as regular interfaces in an EtherChannel.

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- Redundant interfaces—A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface, then it is used regardless of the member interface MAC addresses.
- EtherChannels (Firepower Models)—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.
- EtherChannels (ASA Models)—The port-channel interface uses the lowest-numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can configure a MAC address for the port-channel interface. We recommend configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.
- Subinterfaces—All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses.

General Guidelines and Limitations

Firewall Mode

You can set the firewall mode to routed or transparent in the bootstrap configuration for the FTD.

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.
- For more information, see [High Availability System Requirements](#)

Context Mode

- Multiple context mode is only supported on the ASA.

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 () so that it changes to the enabled slider (.

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 () so that it changes to the disabled slider (.

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

Configure a Physical Interface

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.

Before you begin

- Interfaces that are 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 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** To enable the interface, check the **Enable** check box. To disable the interface, uncheck the **Enable** check box.
- Step 4** Choose the interface **Type**: **Data**, **Mgmt**, **Firepower-eventing**, or **Cluster**.
Do not choose the **Cluster** type; by default, the cluster control link is automatically created on Port-channel 48.
- Step 5** (Optional) Choose the speed of the interface from the **Speed** drop-down list.
- Step 6** (Optional) If your interface supports **Auto Negotiation**, click the **Yes** or **No** radio button.
- Step 7** (Optional) Choose the duplex of the interface from the **Duplex** drop-down list.
- Step 8** 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 type. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDU)s between two network devices.

The Firepower 4100/9300 chassis 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.

When the Firepower 4100/9300 chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state 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** state.

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** 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 configure an EtherChannel with a different ID and choose the Cluster type for the interface. 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: Data, Mgmt, Firepower-eventing, or Cluster**.
- Do not choose the **Cluster** type unless you want to use this port-channel as the cluster control link instead of the default.
- Step 6** Set the **Admin Speed** of the member interfaces from the drop-down list.
- Step 7** Set the **Admin Duplex, Full Duplex or Half Duplex**.
- Step 8** 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 interfaces of the same type and speed.
- 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 9** To remove an interface from the port channel, click the **Delete** button to the right of the interface in the Member ID list.
- Step 10** Click **OK**.
-

Configure Logical Devices

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

For clustering, see [Firepower Threat Defense Cluster for the Firepower 4100/9300](#).

Add a Standalone Firepower Threat Defense

Standalone logical devices work either alone or in a High Availability pair. On multiple module devices, like the Firepower 9300, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

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 chassis.



Note You must install the same application instance type on all modules in a chassis, either ASA or Firepower Threat Defense; different application types are not supported at this time. Note that modules can run different versions of a particular application type, but all modules must be configured as the same type of application instance.

- 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 interface 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. Optionally, you can also create a firepower-eventing interface to carry all event traffic (such as web events). See [Interface Types](#), on page 2 for more information.

Procedure

- Step 1** Choose **Logical Devices**.
- The **Logical Devices** page shows a list of logical devices on the chassis.
- Step 2** Click **Add Device**.
- The **Add Device** dialog box appears.
- Step 3** For the **Device Name**, provide a name for the logical device.
- This name is used by the Firepower 4100/9300 chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the security module/engine configuration.
- Step 4** For the **Template**, choose **Cisco Firepower Threat Defense**.
- Step 5** Choose the **Image Version**.
- Step 6** For the **Device Mode**, click the **Standalone** radio button.
- Step 7** Click **OK**.
- You see the Provisioning - *device name* window.
- Step 8** Expand the **Data Ports** area, and click each interface that you want to assign to the device.
- Hardware Bypass-capable ports are shown with the following icon: . If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.
- Step 9** 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 change most values in the application CLI configuration.
- Step 10** On the **General Information** tab, complete the following:
- (On multiple module devices, like 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**.
- c) Choose the management interface **Address Type, IPv4 only, IPv6 only, or IPv4 and IPv6**.
- d) Configure the **Management IP** address.
- e) Enter a **Network Mask** or **Prefix Length**.
- f) Enter a **Network Gateway** address.

Step 11 On the **Settings** tab, complete the following:

- a) In the **Registration Key** field, enter the key to be shared between Firepower Management Center and the device during registration.
- b) In the **Password** field, enter a password for the device.
- c) In the **Firepower Management Center IP** field, enter the IP address of the managing Firepower Management Center.
- d) In the **Search Domains** field, enter a comma-separated list of search domains for the device.
- e) Choose the **Firewall Mode, Transparent or Routed**.
- f) In the **DNS Servers** field, enter a comma-separated list of DNS servers for the device to use.
- g) In the **Fully Qualified Hostname** field, enter a fully qualified name for the Threat Defense device.
- h) Choose the **Eventing Interface** on which Firepower events should be sent. If not specified, the management interface will be used.

To specify an interface to use for Firepower events, you must configure an interface as a *firepower-eventing* interface. For more information, see [About Firepower Interfaces, on page 1](#).

Step 12 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 13 Click **OK** to close the configuration dialog box.

Step 14 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 specified security module/engine.

Add a High Availability Pair

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

- For High Availability system requirements, see [High Availability System Requirements](#).

Procedure

- Step 1** Each logical device should be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not recommended and may not be supported.
- Step 2** Allocate the same interfaces to each logical device.
- Step 3** 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 4** Enable High Availability on the logical devices. See [Firepower Threat Defense High Availability](#).
- Step 5** 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 Firepower Threat Defense Logical Device

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

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](#).
- You can edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the Firepower Management Center.
- 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 firepower 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 Firepower Threat Defense device reboots (management interface changes cause a reboot), and you sync the configuration in the Firepower Management Center, you can add the (now unallocated) management interface to the EtherChannel as well.
- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the Firepower Management Center. We recommend that you make the interface changes on the slave/standby unit(s) first, and then on the master/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.

Procedure

- Step 1** In the Firepower Chassis Manager, choose **Logical Devices**.
- Step 2** Click the **Edit** icon at the top right to edit the logical device.
- Step 3** Unallocate a data interface by de-selecting the interface in the **Data Ports** area.
- Step 4** Allocate a new data interface by selecting the interface in the **Data Ports** area.
- Step 5** Replace the management or eventing 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/Cluster Information** tab, choose the new **Management Interface** from the drop-down list.
- c) On the **Settings** tab, choose the new **Eventing Interface** from the drop-down list.
- d) Click **OK**.

If you change the IP address of the Management interface, then you must also change the IP address for the device in the Firepower Management Center: go to **Devices > Device Management > Device/Cluster**. In the **Management** area, set the IP address to match the bootstrap configuration address.

Step 6 Click **Save**.

Step 7 Log into the Firepower Management Center.

Step 8 Select **Devices > Device Management** and click the edit icon (✎) for your FTD device. The **Interfaces** tab is selected by default.

Step 9 Click the **Sync Interfaces from device** button on the top left of the **Interfaces** tab.

Step 10 Click **Save**.

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

History for Firepower Threat Defense Logical Devices

Feature	Version	Details
Support for EtherChannels in FTD inline sets	6.2.0	You can now use EtherChannels in a FTD inline set. Supported platforms: Firepower 4100/9300
Inter-chassis clustering for 6 FTD modules	6.2.0	You can now enable inter-chassis clustering for the FTD. You can include up to 6 modules in up to 6 chassis. New/modified Firepower Chassis Manager screens: Logical Devices > Configuration Supported platforms: Firepower 4100/9300

Feature	Version	Details
Hardware bypass support on the Firepower 4100/9300 for supported network modules	6.1.0	<p>Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures.</p> <p>New/Modified screens:</p> <p>Devices > Device Management > Interfaces > Edit Physical Interface</p> <p>Supported platforms: Firepower 4100/9300</p>
Inline set link state propagation support for the FTD	6.1.0	<p>When you configure an inline set in the FTD application and enable link state propagation, the FTD sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down.</p> <p>New/Modified FXOS commands: show fault grep link-down, show interface detail</p> <p>Supported platforms: Firepower 4100/9300</p>
Support for intra-chassis clustering on the FTD on the Firepower 9300	6.0.1	<p>The Firepower 9300 supports intra-chassis clustering with the FTD application.</p> <p>New/Modified Firepower Chassis Manager screen:</p> <p>Logical Devices > Configuration</p> <p>New/Modified FXOS commands: enter mgmt-bootstrap ftd, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement</p> <p>Supported platforms: Firepower 4100/9300</p>