Guidelines and Limitations for Firepower Interface Configuration

When you use Cisco Defense Orchestrator (CDO) to configure the device, there are several limitations to interface configuration. If you need any of the following features, you must use Firepower Management Center to configure the device.

**Firewall**

- Routed firewall mode only is supported. You cannot configure transparent firewall mode interfaces.

**Passive**

- At this time, CDO does not identify passive interface mode in the interface table and you cannot configure passive or ERSPAN interfaces. You must use the FDM UI to configure and identify passive interfaces.

**IPS-Only Mode**

- You cannot configure interfaces to be inline (in an inline set), or inline tap, for IPS-only processing. IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. In comparison, 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.
- Optionally, you can configure IPS functions for this firewall mode traffic according to your security policy.

**EtherChannel**

COD currently reads EtherChannel configurations. You must use the FDM UI to create and configure etherChannels for your FTD.

**Port Channel**

Where an EtherChannel bundles individual physical links into one logical link to increase the total bandwidth, a port channel is the logical representation of the EtherChannel on the switch. To create or configure a port channel interface, see [Configure an FTD VLAN for Switch Port Mode](#) for more information.

- Only physical interfaces, redundant interfaces, and subinterfaces are supported as bridge group member interfaces.

**Bridge Groups**

At this time, CDO supports the configuration of one bridge group. To determine if your device supports bridge groups, see [Bridge Group Compatibility in FTD Configurations](#) for more information.

When adding an interface to a bridge group, keep the following in mind:
• The interface must have a name.
• The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP.
• BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
• The interface cannot be Point-to-Point Protocol over Ethernet (PPPoE)
• The interface cannot be associated with a security zone (if it is in a zone). You must delete any NAT rules for the interface before you can add it to a bridge group.
• Enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.
• You can configure the interfaces that will be members of the bridge group. See Configure a Bridge Group for interface requirements and creation.

Point-to-Point Protocol over Ethernet

• You cannot configure Point-to-Point Protocol over Ethernet (PPPoE) for IPv4. If the Internet interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, you must use the FDM to configure these settings.

VLAN

To configure VLAN interfaces and VLAN members, see Configure an FTD VLAN for more information. To configure VLAN for switch port mode, see Configure an FTD VLAN for Switch Port Mode for more information.

• The interface must be physical.
• The interface cannot be management-only.
• The interface cannot be associated as any other type of interface, including BVI, subinterfaces, another VLAN interface, EtherChannel, etc.
• The interface cannot be a member of BVI or etherchannel.
• Device models support varying numbers of VLAN members. See Maximum Number of VLAN Members by Device Model for more information.

Note: To configure VLAN for your environment, see Configure Firepower VLAN Subinterfaces and 802.1Q Trunking for more information.

Network Module Cards

Optional network module installations are limited to the ASA 5515-X, 5525-X, 5545-X, and 5555-X, and the Firepower 2100 series devices.

• Cards are only discovered during bootstrap (that is, initial installation or reimage, or when switching between local/ remove management). CDO sets the correct defaults for speed and duplex for these interfaces. If you replace an optional card with one that changes the speed/duplex options for the interfaces, without changing the total number of interfaces available, reboot the device so that the system recognizes the correct speed/duplex values for the replaced interfaces. From an SSH or Console session with the device, enter the reboot command. Then, using
CDO, edit each physical interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.

**Note:** Replacing a card with one that changes the total number of interfaces, or removing interfaces that were referred to by other objects, can result in unexpected problems. If you need to make this kind of change, please first remove all references to the interfaces you will remove, such as security zone membership, VPN connections, and so forth. We also suggest you do a backup prior to making the change.

### Interfaces on FTDv Devices

- You cannot add or remove interfaces without reinitializing an FTDv device. You must execute these actions in FDM.

**Note:** If you replace interfaces with ones that have different speed/duplex capabilities, reboot the device so that the system recognizes the new speed/duplex values with the following procedure: from the device's CLI console, enter the reboot command. Then, in CDO, edit each interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.