

Configure Secure Firewall Management Center without Eth0 as Mgmt

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[About the Management Connection on Secure Firewall Management Center](#)

[Related Documentation](#)

[Pre-Configuration](#)

[Install the Secure Firewall Management Center for Versions 6.5 and Later](#)

[Secure Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later](#)

[Change the Management Interface using Console CLI](#)

[Procedure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure Secure Firewall Management Center(FMC) with a different port instead of the Default Eth0 Interface.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Cisco Secure Firewall Management Center (formerly known as Firepower Management Center)
- Knowledge of basic Networking

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600, and virtual) running software version 5.x and above.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

About the Management Connection on Secure Firewall Management Center

After you configure the device with the FMC information and after you add the device to the FMC, either the device or the FMC can establish the management connection. Depending on the initial setup:

- Either the device or the FMC can initiate.
- Only the device can initiate.
- Only the FMC can initiate.

Initiation always originates with eth0 on the FMC or with the lowest-numbered management interface on the device. Additional management interfaces are tried if the connection is not established. Multiple management interfaces on the FMC let you connect to discrete networks or segregate management and event traffic. However, the initiator does not choose the best interface based on the routing table.

The Internal Interface labeled as Management (Eth0) is a 1 Gigabit Ethernet embedded in the Device Chassis. Some models of FMC Chassis have an expansion slot that can carry a Network Module Expansion Card, which can be Copper or Fiber and up to 10 Gigabit, some Chassis embedded ports can support 10-Gigabit Ethernet SFP+ transceivers.

This figure shows the rear panel of the FMC 1000.

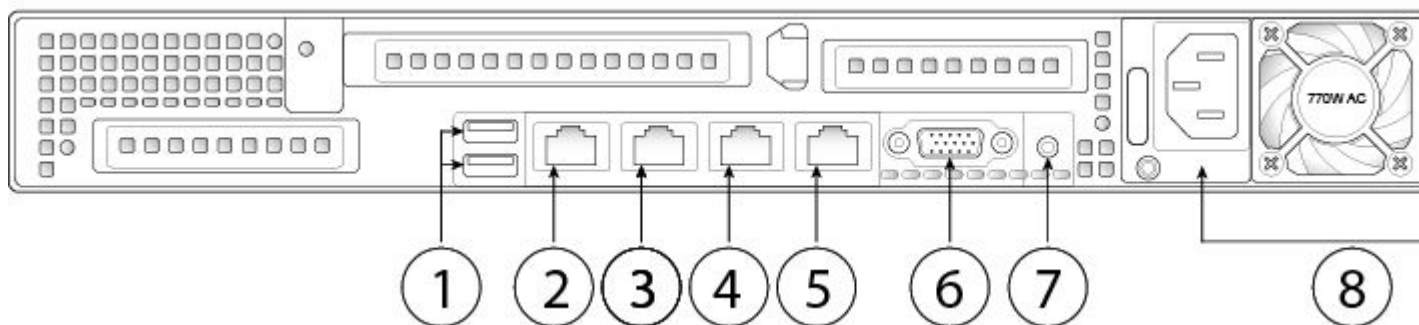


Figure 1. FMC 1000 Rear Panel

1	<p>2 USB keyboard ports</p> <p>You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.</p>	2	<p>CIMC interface (labeled "M")</p> <p>This interface is not supported.</p>
3	<p>Serial console port</p> <p>This port is disabled by default; use the VGA port and keyboard USB port instead.</p>	4	<p>eth0 management interface (labeled "1")</p> <p>Gigabit Ethernet 10/100/1000 Mbps interface, RJ-45</p> <p>eth0 is the default</p>

			management interface.
5	eth1 management interface (labeled "2") Gigabit Ethernet 10/100/1000 Mbps interface, RJ-45	6	VGA interface Enabled by default.
7	Unit identification button/LED	8	Two 770-W AC power supplies

This figure shows the rear panel of the FMC 2500 and 4500.

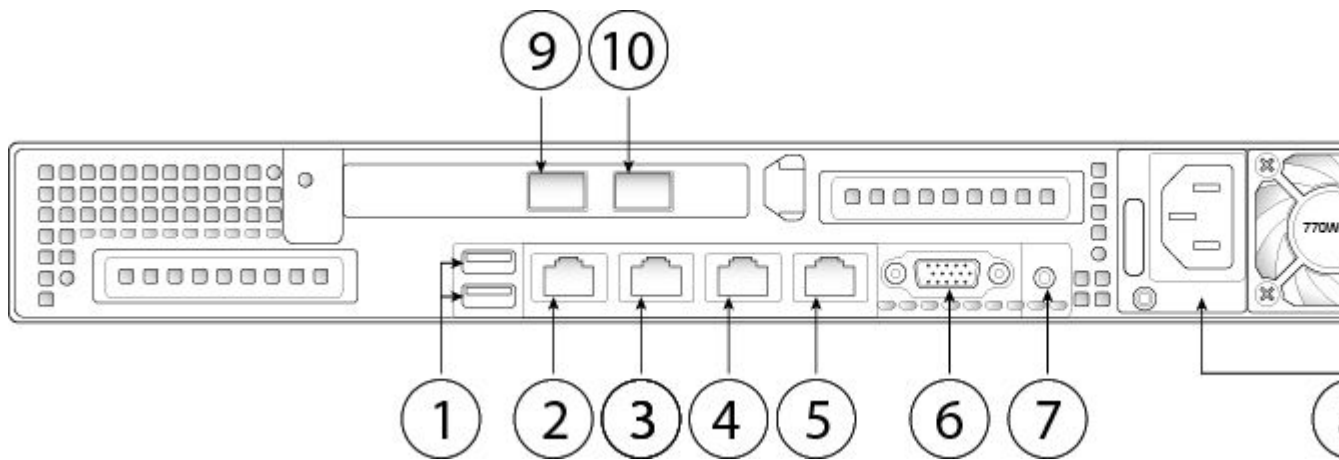


Figure 2. FMC 2500 and 4500 Rear Panel

2 USB keyboard ports 1 You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.	2 CIMC interface (labeled "M") This interface is not supported.
Serial console port 3 This port is disabled by default; use the VGA port and keyboard USB port instead.	4 eth0 management interface (labeled "1") Gigabit Ethernet 10/100/1000 Mbps interface, RJ-45 eth0 is the default management interface.
eth1 management interface (labeled "2") 5 Gigabit Ethernet 10/100/1000 Mbps	6 VGA interface Enabled by default.

	interface, RJ-45		
7	Unit identification button/LED	8	Two 770-W AC power supplies
9	eth2 management interface Note: Use only Cisco-supported SFP+ transceivers.	10	eth3 management interface Note: Use only Cisco-supported SFP+ transceivers.

This figure shows the rear panel of the FMC 1600, 2600, and 4600.

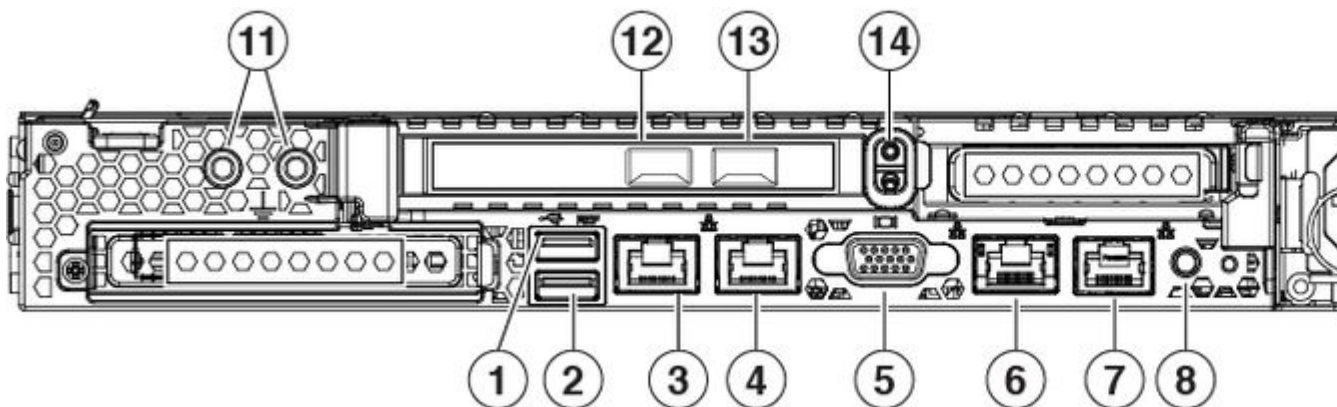


Figure 3. FMC 1600, 2600, and 4600 Rear Panel

1	USB 3.0 Type A (USB 1) You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.	2	USB 3.0 Type A (USB 2) You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.
3	eth0 management interface (labeled 1) Supports 100/1000/10000 Mbps depending on link partner capability.	4	eth1 management interface (labeled 2) Gigabit Ethernet 100/1000/10000 Mbps interface, RJ-45, LAN2
5	VGA video port (DB-15 connector)	6	CIMC interface (labeled M) Note: CIMC is

			supported only for LOM access. CIMC is not supported on any other interfaces.
7	Serial console port (RJ-45 connector) Disabled by default; use the VGA port and keyboard USB port instead. For more information on the serial port, see the "Set up Serial Access" topic in the Cisco Firepower Management Center Getting Started Guide for Models 1600, 2600, and 4600 .	8	Unit identification button
9	770-W AC power supply (PSU 1)	10	770-W AC power supply (PSU 2)
11	Threaded holes for dual-hole grounding lug	12	eth2 management interface (Optional) 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the FMC.
13	eth3 management interface (Optional) 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the FMC.	14	Riser handle Not supported

Related Documentation

For detailed hardware installation instructions, see the [Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide](#).

For a complete list of the Cisco Secure Firewall series documentation and where to find it, see the [documentation roadmap](#).

Pre-Configuration

Install the Secure Firewall Management Center for Versions 6.5 and Later

For detailed installation instructions, read the [Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide](#) up to the step [Connect Cables Turn On Power Verify Status for Versions 6.5 and Later](#). Please connect the cable on the interface required based on the Rear Diagrams.

Secure Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later

Complete the Management Center Initial setup using the CLI detailed in the document [Management Center Initial Setup Using the CLI for Versions 6.5 and Later](#) all the 8 steps.

Change the Management Interface using Console CLI

Procedure

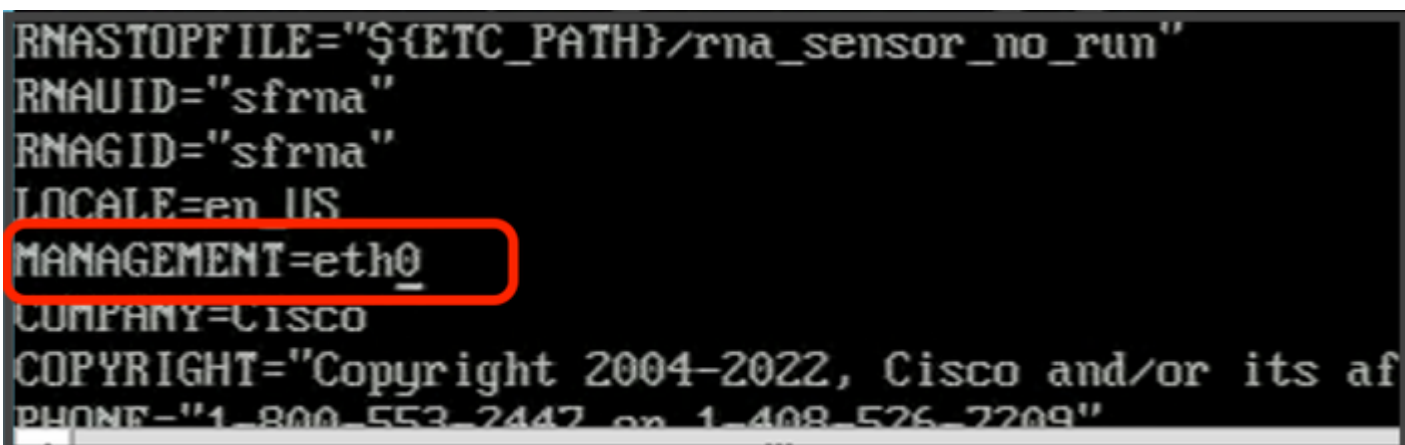
1. Log into the management center virtual at the console using admin as the username and the password for the **admin** account that you defined on the Initial Setup. Note that the password is case-sensitive.
2. Use the **expert** command to enter into Linux shell mode.
3. Edit the **ims.conf** file using **vi** editor with the command **sudo vi /etc/sf/ims.conf**:



```
>  
> expert  
admin@firepower:~$ sudo vi /etc/sf/ims.conf
```

Figure 4

4. Use the arrow keys on your keyboard and find the line **MANAGEMENT=eth0**:



```
RNASTOPFILE="$ {ETC_PATH}/rna_sensor_no_run"  
RNAUID="sfrna"  
RNAGID="sfrna"  
LOCALE=en_US  
MANAGEMENT=eth0  
COMPANY=CISCO  
COPYRIGHT="Copyright 2004-2022, Cisco and/or its af  
PHONE-"1-800-553-2447 or 1-408-526-7209"
```

Figure 5

5. Enter into **INSERT** mode to edit by typing the key **"I"**, the bottom line at the screen can confirm with the message **INSERT** that we are in edit mode, and replace **eth0** with the interface designed, use the previous Tables as reference:

```
RNAUID="sfrna"  
RNAGID="sfrna"  
LOCALE=en US  
MANAGEMENT=eth1  
COMPANY=Cisco  
-- INSERT --
```

Figure 6

6. Hit the **Esc** key on the Keyboard to exit INSERT mode and use the colon key ":" to enter in command mode, type "wq!" to save the changes and exit the file:

```
MODEL_CLASS="Defense Center"  
CSMVERSION=7.0.5  
CSMBUILD=11  
:wq! _
```

Figure 7

7. Disable the eth0 interface with the command **sudo ip link set eth0 down**:

```
admin@firepower:~$ sudo ip link set eth0 down
```

Figure 8

8. Run the Network Configuration Wizard to re-enter the **IP address, Network Mask and Gateway address** with the commando **sudo usr/local/sf/bin/configure-network**, this command can create the interface and assign a default route:

```
admin@firepower:~$ sudo /usr/local/sf/bin/configure-network
Do you wish to configure IPv4? (y or n) y
Management IP address? [192.168.45.45] 192.168.45.45
Management netmask? [255.255.255.0] 255.255.255.0
Management default gateway? [192.168.45.1] 192.168.45.1

Management IP address?          192.168.45.45
Management netmask?             255.255.255.0
Management default gateway?     192.168.45.1

Are these settings correct? (y or n) y
```

Figure 9

9. Exit the Linux shell mode with the **exit** command.

Verify

To verify if the interface selected was enabled, use this procedure:

1. Run from Linux Shell mode the command **sudo route -n** to confirm the default route table for the new Management Interface:

```
admin@firepower:~$ sudo route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.45.1   0.0.0.0         UG    0      0      0 eth1
192.168.45.0    0.0.0.0         255.255.255.0   U      0      0      0 eth1
admin@firepower:~$ _
```

Figure 10

Troubleshoot

If the new interface is not populated on the routing table, validate this:

1. Confirm that you disabled **eth0** interface with **sudo ifconfig** command.
2. If the interface is still enabled, run the step 7 again.
3. Run the configure network script again on step 8 to generate the interface configuration and the default route.