

# Change the Management Interface IP Address on FTD Managed by FMC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

### [Configure](#)

#### [Configurations](#)

### [Verify](#)

### [Troubleshoot](#)

### [Related Information](#)

---

## Introduction

This document describes how to change the management IP for the Firewall Threat Defense device managed by the Secure Firewall Management Center.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

### Components Used

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

- Secure Firewall Management Center Virtual running version 7.2.5(1)
- Cisco Secure Firewall Threat Defense Virtual running version 7.2.4

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.

## Configure

### Configurations

Step 1. Navigate to the FMC GUI, and proceed to **Device > Device Management**.

## Step 2. Select **Device**, and find the **Management** section.

**Frepower**  
Cisco Firepower Threat Defense for VMware

**Device** Routing Interfaces Inline Sets DHCP VTEP

**General**

Name: Frepower  
Transfer Packets: Yes  
Mode: Routed  
Compliance Mode: None  
TLS Crypto Acceleration: Disabled

Device Configuration: [Import](#) [Export](#) [Download](#)

**License**

Performance Tier: FTDv50 - Tiered (Core 12 / 24 GB)  
Base: Yes  
Export-Controlled Features: No  
Malware: Yes  
Threat: Yes  
URL Filtering: Yes  
AnyConnect Apex: No  
AnyConnect Plus: No  
AnyConnect VPN Only: No

**System**

Model: Cisco Firepower Threat Defense for VMware  
Serial: 9A0HJUS0J27  
Time: 2024-04-12 00:57:32  
Time Zone: UTC (UTC+0:00)  
Version: 7.2.4  
Time Zone setting for Time based Rules: UTC (UTC+0:00)

**Inspection Engine**

Inspection Engine: Snort 3  
[Revert to Snort 2](#)

**Health**

Status: ●  
Policy: Initial\_Health\_Policy 2024-04-08 17:12:48  
Excluded: None

**Management**

Host: 192.168.10.42  
Status: ●  
Manager Access Interface: Management Interface

**Inventory Details**

CPU Type: CPU Xeon 4100/6100/8100 series 2700 MHz  
CPU Cores: 1 CPU (4 cores)  
Memory: 8192 MB RAM  
Storage: N/A  
Chassis URL: N/A  
Chassis Serial Number: N/A  
Chassis Module Number: N/A  
Chassis Module Serial Number: N/A

**Applied Policies**

Access Control Policy: Default  
Prefilter Policy: Default Prefilter Policy  
SSL Policy: Default DNS Policy  
DNS Policy: Default DNS Policy  
Identity Policy:  
NAT Policy:  
Platform Settings Policy:  
QoS Policy:  
FlexConfig Policy:

**Advanced Settings**

Application Bypass: No  
Bypass Threshold: 3000 ms  
Object Group Search: Enabled  
Interface Object Optimization: Disabled

## Step 3. Turn off **Management** by clicking the slider, and confirm the action by selecting **Yes**.

**Frepower**  
Cisco Firepower Threat Defense for VMware

**Device** Routing Interfaces Inline Sets DHCP VTEP

**General**

Name: Frepower  
Transfer Packets: Yes  
Mode: Routed  
Compliance Mode: None  
TLS Crypto Acceleration: Disabled

Device Configuration: [Import](#) [Export](#) [Download](#)

**Inspection Engine**

Inspection Engine: Snort 3  
[Revert to Snort 2](#)

**Inventory Details**

CPU Type: CPU Xeon 4100/6100/8100 series 2700 MHz  
CPU Cores: 1 CPU (4 cores)  
Memory: 8192 MB RAM  
Storage: N/A

**Applied Policies**

Access Control Policy: Default  
Prefilter Policy: Default Prefilter Policy  
DNS Policy: Default DNS Policy  
Identity Policy:

**License**

Performance Tier: FTDv50 - Tiered (Core 12 / 24 GB)  
Base: Yes  
Export-Controlled Features: No  
Malware: Yes  
Threat: Yes  
URL Filtering: Yes  
AnyConnect Apex: No  
AnyConnect Plus: No  
AnyConnect VPN Only: No

**System**

Model: Cisco Firepower Threat Defense for VMware  
Serial: 9A0HJUS0J27  
Time: 2024-04-12 01:14:15  
Time Zone: UTC (UTC+0:00)  
Version: 7.2.4  
Time Zone setting for Time based Rules: UTC (UTC+0:00)

**Health**

Status: ●  
Policy: Initial\_Health\_Policy 2024-04-08 17:12:48  
Excluded: None

**Management**

Host: 192.168.10.42  
Status: ●  
Manager Access Interface: Management Interface

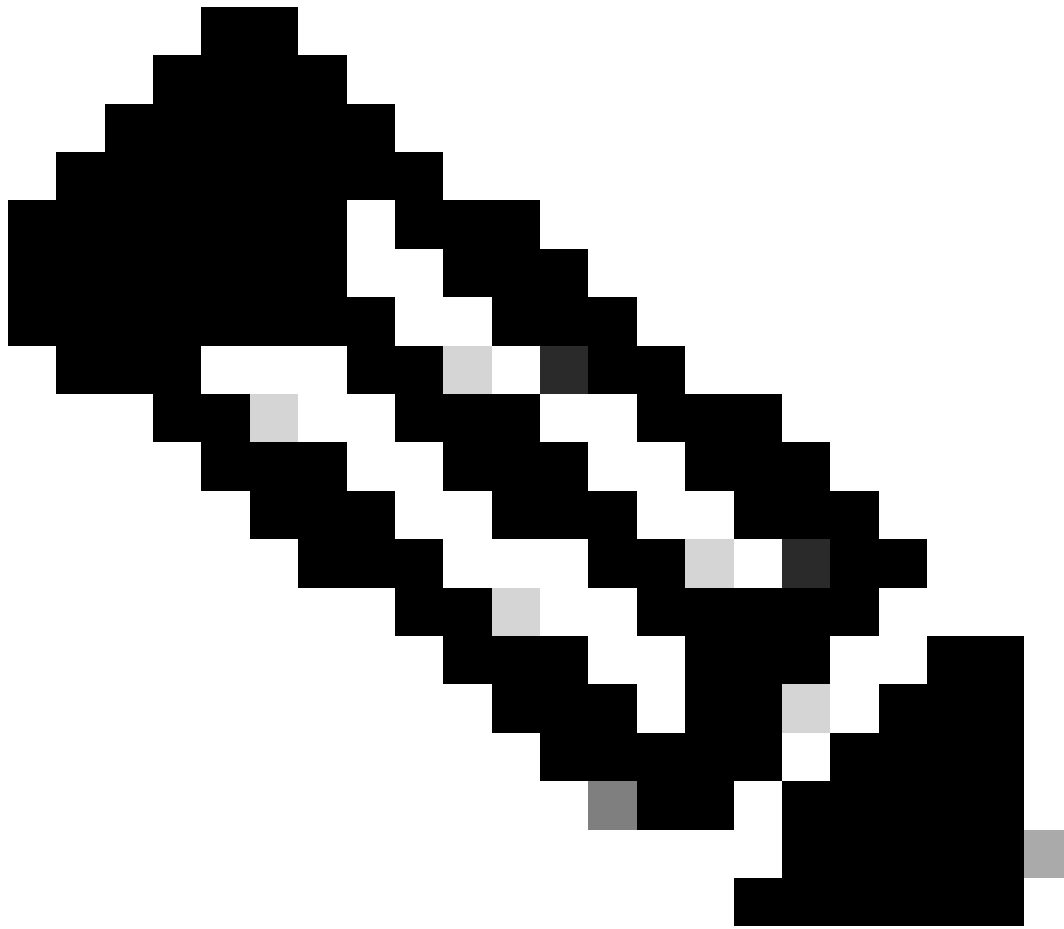
**Advanced Settings**

Application Bypass: No  
Bypass Threshold: 3000 ms  
Object Group Search: Enabled  
Interface Object Optimization: Disabled

**Disable Management**

Managing this device will not be possible if its Management IP is disabled. Do you want to proceed? You can enable it later.

[No](#) [Yes](#)

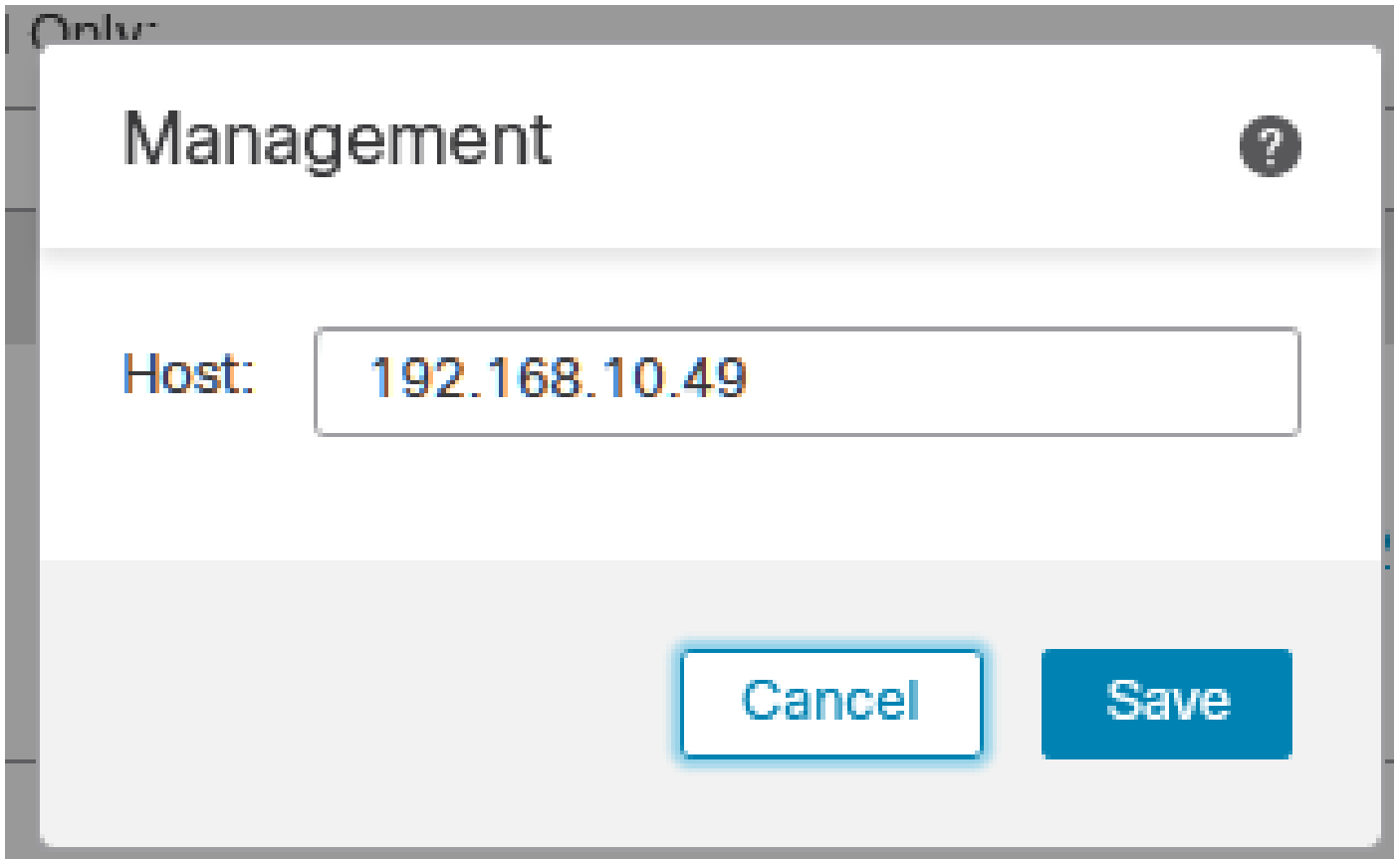


**Note:** Turning off **Management** halts the connection between the management center and the device but retains the device within the management center.

---

Step 4. With **Management** disabled, edit the management connection by selecting **Edit**.

Step 5. In the **Management** dialog box, change the IP address in the remote **Host** address field, and then select **Save**.



Step 6. Connect to the FTD console to modify the Management IP address.



**Warning:** Altering the Management IP address can result in the loss of SSH connectivity to the device if the session is established through the management IP address. Therefore, it is recommended to perform this change via Console access as suggested by Cisco.

---

Step 7. In Clish mode, modify the Management IP address with the command:

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```



**Note:** This configuration is applied to the management interface by default.

---

Step 8. Return to the FMC GUI, and reactivate **Management** by toggling the Slider to the **On** position.



Step 9. Be aware that reestablishing the **Management** connection can require some time; successful reconnection is indicated as demonstrated in this image:

Management 	
Host:	192.168.10.49
Status:	
Manager Access Interface:	<a href="#">Management Interface</a>

## Verify

Use this section in order to confirm that your configuration works properly.

You can verify the Management connectivity through the FTD CLI. This is achieved by connecting to the CLI, on Clish mode running this command:

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
```

```
-----OUTPUT OMITTED-----
```

```
*****
```

```
**RPC STATUS**192.168.10.40*****
'last_changed' => 'Fri Apr 12 01:09:19 2024',
'active' => 1,
'ipv6' => 'IPv6 is not configured for management',
'uuid_gw' => '',
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',
'name' => '192.168.10.40',
'ip' => '192.168.10.40'
```

Check routes:

No peers to check

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

- To verify the management connection status at the FTD CLI, run the command **show sftunnel status brief**. Observe the output for a connection that is down, indicated by the absence of connected to details for the peer channel and missing heartbeat information.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40
```

```
Registration: Completed.
```

```
Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC
```

```
Last disconnect time : Fri Apr 19 21:14:23 2024 UTC
```

```
Last disconnect reason : Both control and event channel connections with peer went down
```

A healthy connection between the devices is confirmed when the **sftunnel-status-brief** command at the FTD CLI produces an output that includes peer channel connected to information and heartbeat data.

```
> sftunnel-status-brief
```

```
PEER:192.168.10.40
```

```
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'
```

```
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'
```

```
Registration: Completed.
```

```
IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC
```

```
Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC
```

```
Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC
```

```
Last disconnect time : Fri Apr 19 21:12:57 2024 UTC
```

```
Last disconnect reason : Process shutdown due to stop request from PM
```

- To check network connectivity, ping the management center from the Management interface, and enter **ping system fmc\_ip** at the FTD CLI.

## Related Information

- [Device Management Basics](#)
- [Cisco Technical Support & Downloads](#)