

Configure FDM On-Box Management Service for The Secure Firewall 2100

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how to configure the Secure Firewall Device Management (FDM) On-Box management service for the Secure Firewall 2100 series with FTD installed.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall 2100, FTD software installation
- Cisco Secure Firewall Threat Defense (FTD) basic configuration and troubleshooting

Components Used

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

- Cisco Secure Firewall 2100 series
- Cisco FTD version 6.2.3


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

The main intention of this document is to guide you through the steps required to enable the FDM On-Box management for the Secure Firewall 2100 series.

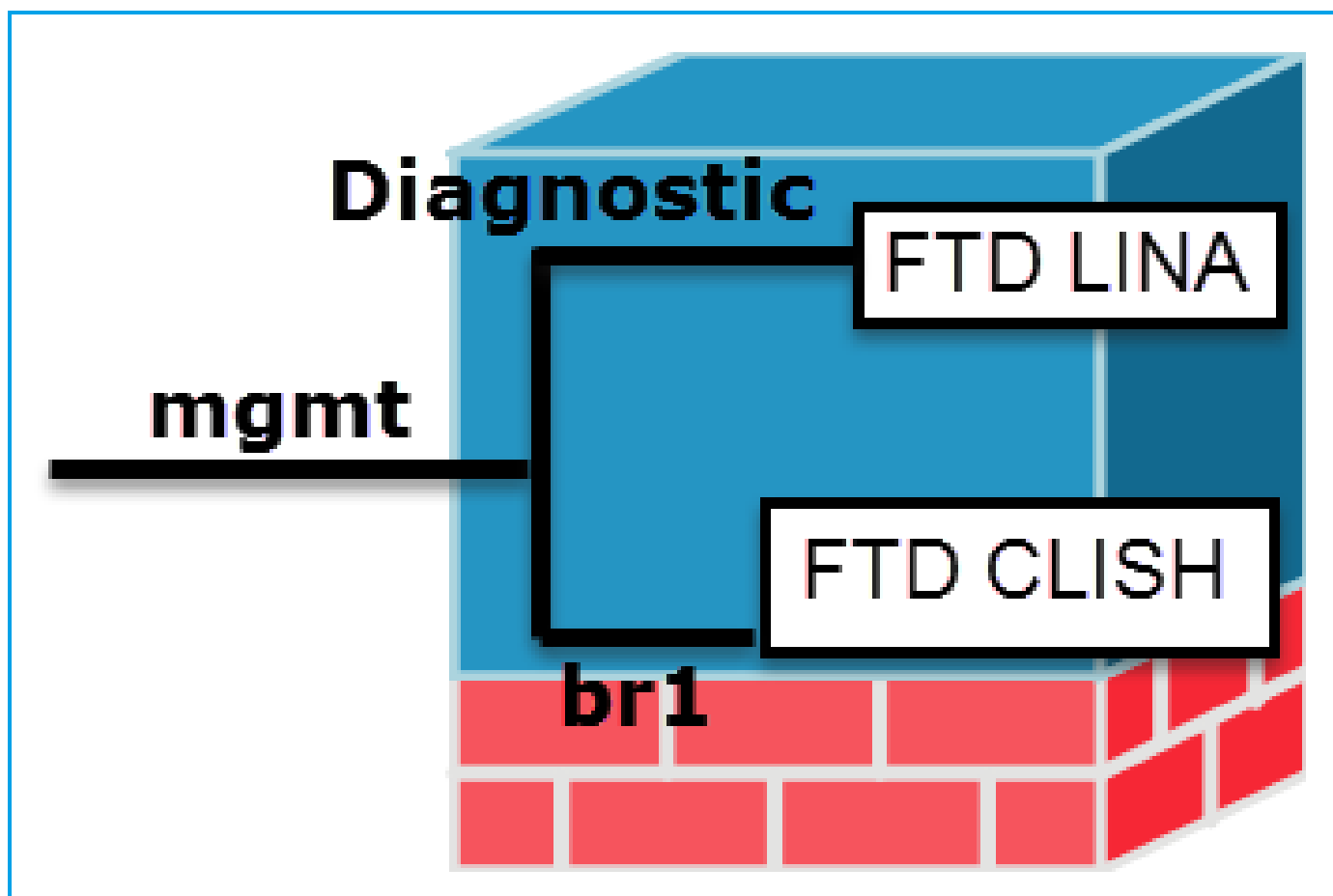
You have two options to manage the Secure Firewall Threat Defense (FTD) installed on a secure firewall 2100 series:

- The Secure Firewall Device Management (FDM) On-Box management
- The Cisco Secure Firewall Management Center (FMC)

 **Note:** An FTD installed on a Secure Firewall 2100 cannot be managed simultaneously by both FDM and FMC. Enabling FDM On-Box management on the Secure Firewall 2100 FTD prevents management via FMC, unless local management is disabled and reconfigured for FMC. Conversely, registering the FTD to an FMC automatically disables the FDM On-Box management service on the device.


 Use the Secure Firewall Migration Tool (FMT) to seamlessly migrate the configuration from a locally managed device using FDM to being managed by the FMC, as detailed in the [Migrating an FDM Managed device to Cisco Secure Firewall Threat Defense with the Migration tool](#)

The management interface is divided into 2 logical interfaces, br1 (management0 on 2100/4100/9300 appliances) and diagnostic:




	Management - br1/management0	Management - Diagnostic
Purpose	<ul style="list-style-type: none">• This interface is used in order to assign the FTD IP that is used for FTD/FMC communication.• Terminates the sftunnel between	<ul style="list-style-type: none">• Provides remote access (for example, SNMP) to ASA engine.• Used as a source for LINA-level syslogs, AAA, SNMP and so on messages.

	<p>FMC/FTD.</p> <ul style="list-style-type: none"> • Used as a source for rule-based syslogs. • Provides SSH and HTTPS access to the FTD box. 	
Mandatory	Yes, since it is used for FTD/FMC communication (the sftunnel terminates on it).	No, and it is not recommended to configure it. The recommendation is to use a data interface instead (check the note below).


 **Note:** The benefit of leaving the IP address off of the diagnostic interface is that you can place the management interface on the same network as any other data interface. If you configure the diagnostic interface, its IP address must be on the same network as the management IP address, and it counts as a regular interface that cannot be on the same network as any other data interfaces. Because the management interface requires internet access for updates, to put the management interface on the same network as an inside FTD interface means you can deploy the FTD with only a switch on the LAN and point the inside interface as the default gateway for the management interface (This just applies when the FTD is deployed in routed mode).

The FTD can be installed in a secure firewall 2100 appliance. The chassis runs its own operating system called Secure Firewall eXtensible Operating System (FXOS) to control basic operations of the device, while the FTD logical device is installed on a module/blade.

 **Note:** You can use the FXOS Graphic User Interface (GUI) called Secure Firewall Chassis Manager (FCM) or the FXOS Command Line Interface (CLI) to configure fchassis functions; however the GUI FCM is not available when the FTD is installed on the 2100 series, just the FXOS CLI.

Secure Firewall 21xx appliance:

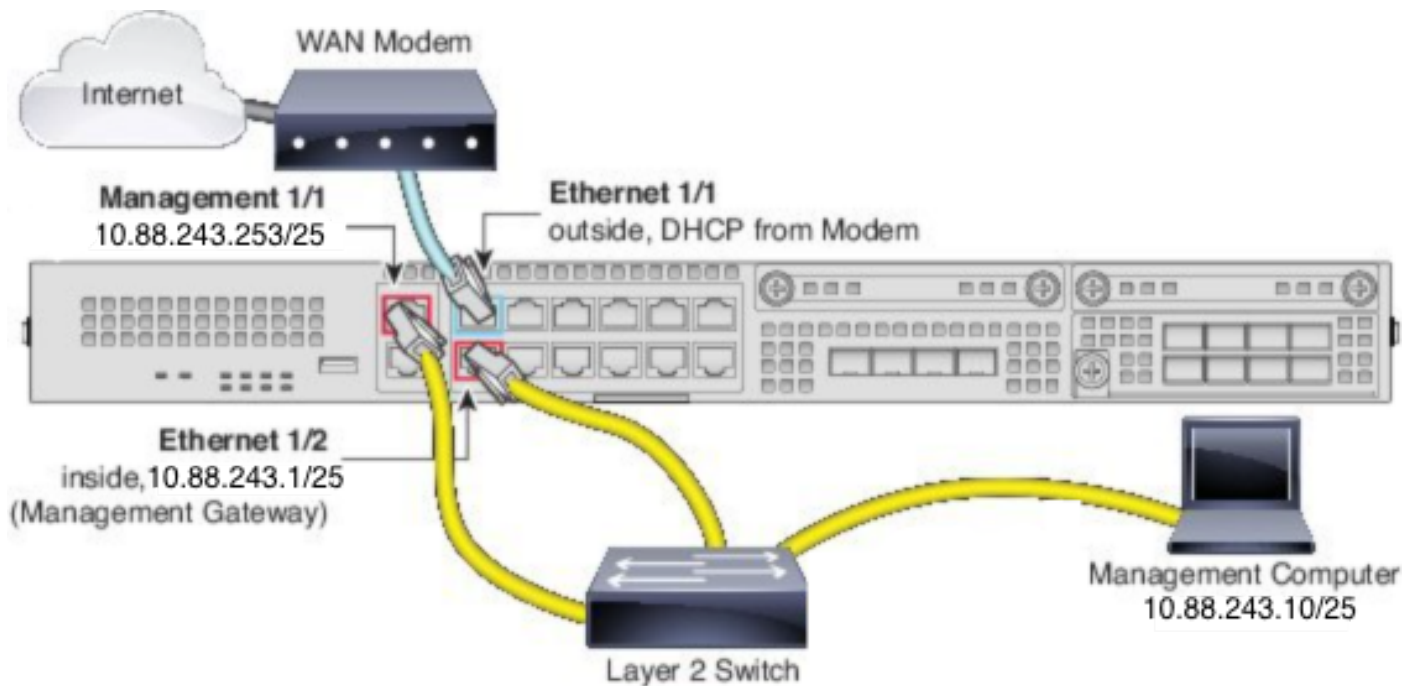



 **Note:** On the secure firewall 2100 series, the management interface is shared between the chassis FXOS and the FTD logical device.

Configure

Network Diagram

The default configuration assumes that certain secure firewall 2100 interfaces are used for the inside and outside networks. Initial configuration is easier to complete if you connect network cables to the interfaces based on these expectations. To cable the secure firewall 2100 series, see the next image.



 **Note:** The image shows a simple topology that uses a Layer 2 switch. Other topologies can be used and your deployment can vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Configurations

In order to enable the FDM On-Box management on the secure firewall 2100 series proceed as follows.

1. Console access into the 2100 chassis and connect to the FTD application.

```
firepower# connect ftd
>
```

2. Configure the FTD management IP address.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

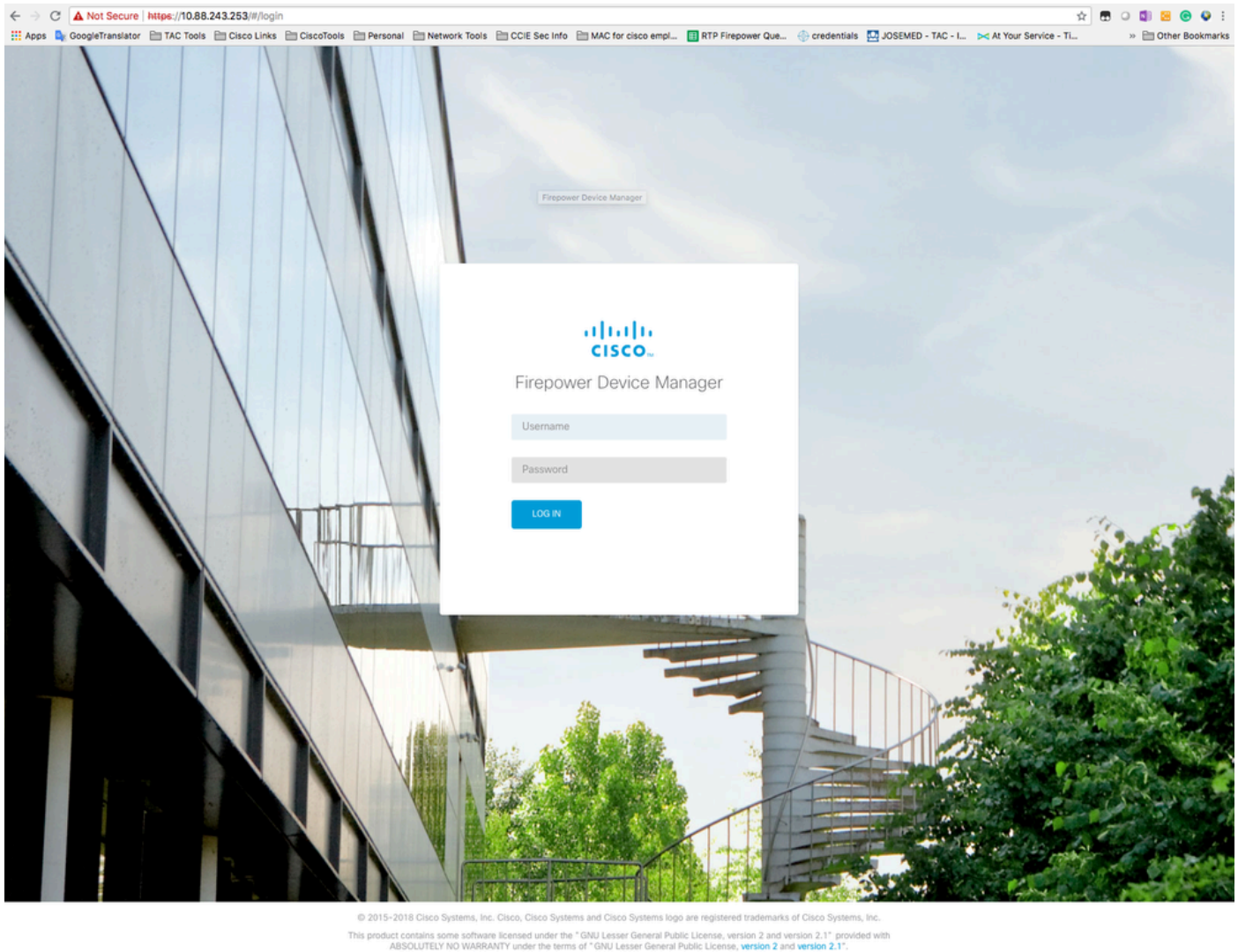
3. Configure the management type as local.

```
>configure manager local
```

4. Configure from which IP addresses/subnets the On-Box management access to the FTD can be allowed.

```
>configure https-access-list 0.0.0.0/0
```

5. Open a browser and https into the IP address you configured to manage the FTD. This can open the FDM (On-Box) manager.



6. Log in and use the default secure firewall credentials, username admin, and password Admin123.

Device

?
User

Device Setup

1 Configure Internet Connection
2 Configure Time Settings
3 Smart License Registration

Connection Diagram

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1	Default Action
Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Block all other traffic The default action blocks all other traffic.

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP

Configure IPv6

Using DHCP

Management Interface

Configure DNS Servers

Primary DNS IP Address

10.67.222.222

NEXT

Don't have internet connection?
[Skip device setup](#)

Verify

1. Verify the network settings you configured for the FTD with the next command.

```
> show network
===== [ System Information ] =====
Hostname                : firepower
DNS Servers             : 10.67.222.222
                        : 10.67.220.220
Management port        : 8305
IPv4 Default route
  Gateway               : 10.88.243.129

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 00:2C:C8:41:09:80
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.88.243.253
Netmask                : 255.255.255.128
Broadcast              : 10.88.243.255
```

```
-----[ IPv6 ]-----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                  : Disabled
Authentication         : Disabled
```

2. Verify the management type you configured for the FTD with the next command.

```
> show managers
Managed locally.
```

Related Information

- [Cisco Secure Firewall Device Manager](#)
- [Cisco Secure Firewall Threat Defense for the 2100 Series Using Secure Firewall Management Center Quick Start Guide](#)
- [Configure Secure Firewall Threat Defense \(FTD\) Management Interface](#)
- [Reimage the Secure Firewall 2100 Series](#)
- [Migrating an FDM Managed device to Cisco Secure Firewall Threat Defense with the Migration tool](#)