Getting Started

The following topics explain how to get started configuring the Firepower Threat Defense (FTD) .

Is This Guide for You?

This guide explains how to configure FTD using the Firepower Device Manager (FDM) web-based configuration interface included on the FTD devices.

The FDM lets you configure the basic features of the software that are most commonly used for small or mid-size networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many FTD devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that FTD allows, use the Firepower Management Center (FMC) to configure your devices instead of the integrated FDM.

You can use the FDM on the following devices.

Table 1: FDM Supported Models

Device Model	Minimum FTD Software Version
Firepower 2110, 2120, 2130, 2140	6.2.1
FTDv (FTDv)for VMware	6.2.2
FTDv for Kernel-based Virtual Machine (KVM) hypervisor	6.2.3
ASA 5508-X, 5516-X	6.1
ASA 5525-X, 5545-X, 5555-X	6.1
ASA 5506-X, 5506H-X, 5506W-X, 5512-X	6.1

Device Model	Minimum FTD Software Version
ASA 5515-X	6.1
ISA 3000 (Cisco 3000 Series Industrial Security Appliances)	6.2.3

New Features in FDM/FTD 6.2

Released: January 23, 2017

The following table lists the new features available in FTD 6.2 when configured using FDM.

Feature	Description
Cisco Defense Orchestrator (CDO) cloud management.	You can manage the device using the Cisco Defense Orchestrator cloud-based portal. Select **Device** > **System Settings** > **Cloud Management**. For more information on Cisco Defense Orchestrator, see http://www.cisco.com/go/cdo.
Drag and drop for access rules.	You can drag and drop access rules to move them in the rules table.
Upgrade FTD software through FDM.	You can install software upgrades through FDM. Select **Device** > **Updates**.

Feature	Description
Default configuration changes.	For new or reimaged devices, the default configuration includes significant changes, including: • (ASA 5506-X, 5506W-X, 5506H-X.) Except for the first data interface, and the Wi-Fi interface on an ASA 5506W-X, all other data interfaces on these device models are structured into the "inside" bridge group and enabled. There is a DHCP server on the inside bridge group. You can plug endpoints or switches into any bridged interface and endpoints get addresses on the 192.168.1.0/24 network. • The inside interface IP address is now 192.168.1.1, and a DHCP server is defined on the interface with the address pool 192.168.1.5-192.168.1.254. • HTTPS access is enabled on the inside interface, so you can open FDM through the inside interface at the default address, 192.168.1.1. For the ASA 5506-X models, you can do this through any inside bridge group member interface. • The management port hosts a DHCP server for the 192.168.45.0/24 network. You can plug a workstation directly into the management port, get an IP address, and open FDM to configure the device. • The OpenDNS public DNS servers are now the default DNS servers for the management interface. Previously, there were no default DNS servers. You can configure different DNS servers during device setup. • The default gateway for the management IP address is to use the data interfaces to route to the Internet. Thus, you do not need to wire the Management physical interface to a network.

Feature	Description
Management interface and access changes.	Several changes to how the management address, and access to FDM, works: • You can now open data interfaces to HTTPS (for FDM) and SSH (for CLI) connections. You do not need a separate management network, or to connect the Management/Diagnostic physical port to the inside network, to manage the device. Select **Device** > **System Settings** > **Management Access List**. • The system can obtain system database updates through the gateway for the outside interface. You do not need to have an explicit route from the management interface or network to the Internet. The default is to use internal routes through the data interfaces. However, you can set a specific gateway if you prefer to use a separate management network. Select **Device** > **System Settings** > **Management Interface**. • You can use FDM to configure the management interface to obtain its IP address through DHCP. Select **Device** > **System Settings** > **Management Interface**. • You can configure a DHCP server on the management address if you configure a static address. Select **Device** > **System Settings** > **Management Interface**.
Miscellaneous user interface changes.	The following are notable changes to the FDM user interface. • **Device** main menu item. In previous releases, this menu item was the host name of your device. Also, the page opened is called Device Summary instead of Device Dashboard. • You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface. • **Device** > **System Settings** > **Cloud Preferences** is now called **Device** > **System Settings** > **URL Filtering Preferences**. • The **System Settings** > **DHCP Server** page is now organized on two tabs, with the table of DHCP servers separated from the global parameters.
Site-to-site VPN connections.	You can configure site-to-site virtual private network (VPN) connections using preshared keys. You can configure IKEv1 and IKEv2 connections.

Feature	Description
Integrated Routing and Bridging support.	Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the FTD device bridges instead of routes. The FTD device is not a true bridge in that the FTD device continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. This feature lets you configure bridge groups and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the FTD device to assign to the bridge group. The BVI can be a named interface and can participate separately from member interfaces in some features, such as DHCP server, where you configure other features on bridge group member interfaces, such as NAT and access control rules. Select **Device** > **Interfaces** to configure a bridge group.

New Features in FDM/FTD 6.2.1

Released: May 15, 2017

The following table lists the new features available in FTD 6.2.1 when configured using FDM.

Note This release applies to Firepower 2100 series only.

Feature	Description
Remote access VPN configuration.	You can configure remote access SSL VPN for the AnyConnect client. Configure RA VPN from the **Device** > **Remote Access VPN** group. Configure RA VPN licenses from the **Device** > **Smart License** group.
Firepower 2100 series device configuration.	You can configure FTD on Firepower 2100 series devices using FDM.

New Features in FDM/FTD 6.2.2

Released: September 5, 2017

The following table lists the new features available in FTD 6.2.2 when configured using FDM.

Feature	Description
Remote access VPN configuration for ASA 5500-X series devices.	You can configure remote access SSL VPN for the AnyConnect client on ASA 5500-X series devices. Configure RA VPN from the **Device** > **Remote Access VPN** group. Configure RA VPN licenses from the **Device** > **Smart License** group.
FTDv for VMware device configuration.	You can configure FTD on FTDv for VMware devices using FDM. Other virtual platforms are not supported by FDM. **Note** You must install a new 6.2.2 image to get FDM support. You cannot upgrade an existing virtual machine from an older version and then switch to FDM.

New Features in FDM/FTD Version 6.2.3

Released: March 29, 2018

The following table lists the new features available in FTD 6.2.3 when configured using FDM.

Feature	Description
SSL/TLS Decryption	You can decrypt SSL/TLS connections so that you can inspect the contents of the connection. Without decryption, encrypted connections cannot be effectively inspected to identify intrusion and malware threats, or to enforce compliance with your URL and application usage polices. We added the **Policies** > **SSL Decryption** page and **Monitoring** > **SSL Decryption** dashboard. **Attention** Identity policies that implement active authentication automatically generate SSL decryption rules. If you upgrade from a release that does not support SSL decryption, the SSL decryption policy is automatically enabled if you have this type of rule. However, you must specify the certificate to use for Decrypt-Resign rules after completing the upgrade. Please edit the SSL decryption settings immediately after upgrade.
Security Intelligence Blacklisting	From the new **Policies** > **Security Intelligence** page you can configure a Security Intelligence policy, which you can use to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections will still be evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence. We also renamed the **Policies** dashboard to **Access And SI Rules**, and the dashboard now includes Security Intelligence rule-equivalents as well as access rules.

Feature	Description
Intrusion Rule Tuning	You can change the action for intrusion rules within the pre-defined intrusion policies you apply with your access control rules. You can configure each rule to drop or generate events (alert) matching traffic, or disable the rule. You can change the action for enabled rules only (those set to drop or alert); you cannot enable a rule that is disabled by default. To tune intrusion rules, choose **Policies** > **Intrusion**.
Automatic Network Analysis Policy (NAP) Assignment based on Intrusion Policy	In previous releases, the Balanced Security and Connectivity network analysis policy was always used for preprocessor settings, regardless of the intrusion policy assigned to a specific source/destination security zone and network object combination. Now, the system automatically generates NAP rules to assign the same-named NAP and intrusion policies to traffic based on those criteria. Note that if you use Layer 4 or 7 criteria to assign different intrusion policies to traffic that otherwise matches the same source/destination security zone and network object, you will not get perfectly matching NAP and intrusion policies. You cannot create custom network analysis policies.
Drill-down reports for the Threats, Attackers, and Targets dashboards	You can now click into the Threats, Attackers, and Targets dashboards to view more detail about the reported items. These dashboards are available on the Monitoring page. Because of these new reports, you will lose reporting data for these dashboards when upgrading from a pre-6.2.3 release.
Web Applications Dashboard	The new Web Applications dashboard shows the top web applications, such as Google, that are being used in the network. This dashboard augments the Applications dashboard, which provides protocol-oriented information, such as HTTP usage.
New Zones dashboard replaces the Ingress Zone and Egress Zone dashboards.	The new Zones dashboard shows the top security zone pairs for traffic entering and then exiting the device. This dashboard replaces the separate dashboards for Ingress and Egress zones.
New Malware Dashboard	The new Malware dashboard shows the top Malware action and disposition combinations. You can drill down to see information on the associated file types. You must configure file policies on access rules to see this information.
Self-signed internal certificates, and Internal CA certificates	You can now generate self-signed internal identity certificates. You can also upload or generate self-signed internal CA certificates for use with SSL decryption policies. Configure these features on the **Objects** > **Certificates** page.
Ability to edit DHCP server settings when editing interface properties	You can now edit settings for a DHCP server configured on an interface at the same time you edit the interface properties. This makes it easy to redefine the DHCP address pool if you need to change the interface IP address to a different subnet.

Feature	Description
The Cisco Success Network sends usage and statistics data to Cisco to improve the product and provide effective technical support	You can connect to the Cisco Success Network to send data to Cisco. By enabling Cisco Success Network, you are providing usage information and statistics to Cisco which are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. You can enable the connection when you register the device with the Cisco Smart Software Manager, or later at your choice. You can disable the connection at any time. Cisco Success Network is a cloud service. The **Device** > **System Settings** > **Cloud Management** page is renamed **Cloud Services**. You can configure Cisco Defense Orchestrator from the same page.
FTDv for Kernel-based Virtual Machine (KVM) hypervisor device configuration	You can configure FTD on FTDv for KVM devices using FDM. Previously, only VMware was supported. **Note** You must install a new 6.2.3 image to get FDM support. You cannot upgrade an existing virtual machine from an older version and then switch to FDM.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration	You can configure FTD on ISA 3000 devices using FDM. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000.
Optional deployment on update of the rules database or VDB	When you update the intrusion rules database or VDB, or configure an update schedule, you can prevent the immediate deployment of the update. Because the update restarts the inspection engines, there is a momentary traffic drop during the deployment. By not deploying automatically, you can choose to initiate the deployment at a time when traffic drops will be least disruptive. **Note** A VDB download can also restart Snort all by itself, and then again cause a restart on deployment. You cannot stop the restart on download.
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment	Before you start a deployment, FDM indicates whether the configuration updates require a Snort restart. Snort restarts result in the momentary dropping of traffic. Thus, you now know whether a deployment will not impact traffic and can be done immediately, or will impact traffic, so that you can deploy at a less disruptive time. In addition, in prior releases, Snort restarted on every deployment. Now, Snort restarts for the following reasons only: • you enable or disable SSL decryption policies • an updated rules database or VDB was downloaded • you changed the MTU on one or more physical interface (but not subinterface)

Feature	Description
CLI console in FDM	You can now open a CLI Console from FDM. The CLI Console mimics an SSH or console session, but allows a subset of commands only: **show**, **ping**, **traceroute**, and **packet-tracer**. Use the CLI Console for troubleshooting and device monitoring.
Support for blocking access to the management address	You can now remove all management access list entries for a protocol to prevent access to the management IP address. Previously, if you removed all entries, the system defaulted to allowing access from all client IP addresses. On upgrade to 6.2.3, if you previously had an empty management access list for a protocol (HTTPS or SSH), the system creates the default allow rule for all IP addresses. You can then delete these rules as needed. In addition, FDM will recognize changes you make to the management access list from the CLI, including if you disable SSH or HTTPS access. Ensure that you enable HTTPS access for at least one interface, or you will not be able to configure and manage the device.
Smart CLI and FlexConfig for configuring features using the device CLI	Smart CLI and FlexConfig allows you to configure features that are not yet directly supported through FDM policies and settings. FTD uses ASA configuration commands to implement some features. If you are a knowledgeable and expert user of ASA configuration commands, you can configure these features on the device using the following methods: • Smart CLI—(Preferred method.) A Smart CLI template is a pre-defined template for a particular feature. All of the commands needed for the feature are provided, and you simply need to select values for variables. The system validates your selection, so that you are more likely to configure a feature correctly. If a Smart CLI template exists for the feature you want, you must use this method. In this release, you can configure OSPFv2 using the Smart CLI. • FlexConfig—The FlexConfig policy is a collection of FlexConfig objects. The FlexConfig objects are more free-form than Smart CLI templates, and the system does no CLI, variable, or data validation. You must know ASA configuration commands and follow the ASA configuration guides to create a valid sequence of commands. **Caution** Cisco strongly recommends using Smart CLI and FlexConfig only if you are an advanced user with a strong ASA background and at your own risk. You may configure any commands that are not blacklisted. Enabling features through Smart CLI or FlexConfig may cause unintended results with other configured features.
FTD REST API, and an API Explorer	You can use a REST API to programmatically interact with a FTD device that you are managing locally through FDM. There is an API Explorer that you can use to view object models and test the various calls you can make from a client program. To open the API Explorer, log into FDM, and then change the path on the URL to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Logging Into the System

There are two interfaces to the FTD device:

FDM Web Interface

The FDM runs in your web browser. You use this interface to configure, manage, and monitor the system.

Command Line Interface (CLI, Console)

Use the CLI for troubleshooting. You can also use it for initial setup instead of the FDM.

The following topics explain how to log into these interfaces and manage your user account.

Logging Into the FDM

Use the FDM to configure, manage, and monitor the system. The features that you can configure through the browser are not configurable through the command-line interface (CLI); you must use the web interface to implement your security policies.

Use a current version of the following browsers: Firefox, Chrome, Safari, Edge, or Internet Explorer.

Note If you type in the wrong password and fail to log in on 3 consecutive attempts, your account is locked for 5 minutes. You must wait before trying to log in again.

Before you begin

You can log into the FDM using the **admin** username only. You cannot create additional users for the FDM access.

There can be up to 5 active logins at one time. This includes users logged into the device manager and active API sessions, which are represented by non-expired API tokens. If you exceed this limit, the oldest session, either the device manager login or API token, is expired to allow the new session. These limits do not apply to SSH sessions.

Procedure

Step 1 Using a browser, open the home page of the system, for example, https://ftd.example.com.

You can use any of the following addresses. You can use the IPv4 or IPv6 address or the DNS name, if you have configured one.

- The management address. By default (on most platforms), this is 192.168.45.45 on the Management interface.
- The address of a data interface that you have opened for HTTPS access. By default (on platforms), the “inside” interface allows HTTPS access, so you can connect to the default inside address 192.168.1.1. On device models where the inside interface is a bridge group, you can connect to this address through any bridge group member interface. See Default Configuration Prior to Initial Setup, on page 29 for details about your model's inside IP address.

Tip If your browser is not configured to recognize the server certificate, you will see a warning about an untrusted certificate. Accept the certificate as an exception, or in your trusted root certificate store.

Step 2 Enter the **admin** username and password, then click **Login**.

The default admin password is Admin123.

Your session will expire after 30 minutes of inactivity, and you will be prompted to log in again. You can log out by selecting **Log Out** from the user icon drop-down menu in the upper right of the page.

Logging Into the Command Line Interface (CLI)

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session.

To log into the CLI, do one of the following:

- Use the console cable included with the device to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your device for more information about the console cable.

Note On the Firepower device models, the CLI on the Console port is the Firepower eXtensible Operating System (FXOS).You can get to the FTD CLI using the **connect ftd** command. Use the FXOS CLI for chassis-level troubleshooting only. Use the FTD CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

- For the FTDv, open the virtual console.
- Use an SSH client to make a connection to the management IP address. You can also connect to the address on a data interface if you open the interface for SSH connections (see Configuring the Management Access List). SSH access to data interfaces is disabled by default. Log in using the **admin** username or another CLI user account. The default admin password is Admin123.

Tips

- After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see Cisco Firepower Threat Defense Command Reference at http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.
- You can create local user accounts that can log into the CLI using the **configure user add** command. However, these users can log into the CLI only. They cannot log into the FDM web interface.

Changing Your Password

You should periodically change your password. The following procedure explains how to change the password while logged into FDM.

Note If you are logged into the CLI, you can change your password using the **configure password** command. You can change the password for a different CLI user with the **configure user password** *username* command.

Procedure

Step 1 Select **Profile** from the user icon drop-down list in the upper right of the menu.

Step 2 Click the **Password** tab.

Step 3 Enter your current password.

Step 4 Enter your new password and then confirm it.

Step 5 Click **Change**.

Setting User Profile Preferences

You can set preferences for the user interface and change your password.

Procedure

Step 1 Select **Profile** from the user icon drop-down list in the upper right of the menu.

Step 2 On the **Profile** tab, configure the following and click **Save**.

- **Time Zone for Scheduling Tasks**—Select the time zone you want to use for scheduling tasks such as backups and updates. The browser time zone is used for dashboards and events, if you set a different zone.
- **Color Theme**—Select the color theme you want to use in the user interface.

Step 3 On the **Password** tab, you can enter a new password and click **Change**.

Creating Local User Accounts for the FTD CLI

You can create users for CLI access on FTD devices. These accounts do not allow access to the management application, but to the CLI only. The CLI is useful for troubleshooting and monitoring purposes.

You cannot create local user accounts on more than one device at a time. Each device has its own set of unique local user CLI accounts.

Procedure

Step 1 Log into the device CLI using an account with config privileges.

The admin user account has the required privileges, but any account with config privileges will work. You can use an SSH session or the Console port.

For certain device models, the Console port puts you into the FXOS CLI. Use the **connect ftd** command to get to the FTD CLI.

Step 2 Create the user account.

configure user add *username* {**basic** | **config**}

You can define the user with the following privilege levels:

- **config**—Gives the user configuration access. This gives the user full administrator rights to all commands.
- **basic**—Gives the user basic access. This does not allow the user to enter configuration commands.

Example:

The following example adds a user account named joecool with config access rights. The password is not shown as you type it.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Note Tell users they can change their passwords using the **configure password** command.

Step 3 (Optional.) Adjust the characteristics of the account to meet your security requirements.

You can use the following commands to change the default account behavior.

- **configure user aging** *username max_days warn_days*

  Sets an expiration date for the user's password. Specify the maximum number of days for the password to be valid followed by the number of days before expiration the user will be warned about the upcoming expiration. Both values are 1 to 9999, but the warning days must be less than the maximum days. When you create the account, there is no expiration date for the password.

- **configure user forcereset** *username*

  Forces the user to change the password on the next login.

- **configure user maxfailedlogins** *username number*

  Sets the maximum number of consecutive failed logins you will allow before locking the account, from 1 to 9999. Use the **configure user unlock** command to unlock accounts. The default for new accounts is 5 consecutive failed logins.

- **configure user minpasswdlen** *username number*

  Sets a minimum password length, which can be from 1 to 127.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  Enables or disables password strength checking, which requires a user to meet specific password criteria when changing their password. When a user's password expires or if the **configure user forcereset** command is used, this requirement is automatically enabled the next time the user logs in.

Step 4 Manage user accounts as necessary.

Users can get locked out of their accounts, or you might need to remove accounts or fix other issues. Use the following commands to manage the user accounts on the system.

- **configure user access** *username* {**basic** | **config**}

  Changes the privileges for a user account.

- **configure user delete** *username*

  Deletes the specified account.

- **configure user disable** *username*

  Disables the specified account without deleting it. The user cannot log in until you enable the account.

- **configure user enable** *username*

  Enables the specified account.

- **configure user password** *username*

  Changes the password for the specified user. Users should normally change their own password using the **configure password** command.

- **configure user unlock** *username*

  Unlocks a user account that was locked due to exceeding the maximum number of consecutive failed login attempts.

Setting Up the System

You must complete an initial configuration to make the system function correctly in your network. Successful deployment includes attaching cables correctly and configuring the addresses needed to insert the device into your network and connect it to the Internet or other upstream router. The following procedure explains the process.

Before you begin

Before you start the initial setup, the device includes some default settings. For details, see Default Configuration Prior to Initial Setup, on page 29.

Procedure

Step 1 Connect the Interfaces, on page 15

Step 2 Complete the Initial Configuration Using the Setup Wizard, on page 23

For details about the resulting configuration, see Configuration After Initial Setup, on page 31.

Step 3 Configure the Wireless Access Point (ASA 5506W-X), on page 26

Connect the Interfaces

The default configuration assumes that certain interfaces are used for the inside and outside networks. Initial configuration will be easier to complete if you connect network cables to the interfaces based on these expectations.

The default configuration for most models is designed to let you attach your management computer to the inside interface. Alternatively, you can also directly attach your workstation to the Management port. The interfaces are on different networks, so do not try to connect any of the inside interfaces and the Management port to the same network.

Do not connect any of the inside interfaces or the Management interface to a network that has an active DHCP server. This will conflict with the DHCP servers already running on the inside interface and Management interface. If you want to use a different DHCP server for the network, disable the unwanted DHCP server after initial setup.

The following topics show how to cable the system for this topology when using the inside interfaces to configure the device.

Cabling for ASA 5506-X, 5506W-X, and 5506H-X

Figure 1: ASA 5506W-X (with Wi-Fi), 5506-X (without Wi-Fi)

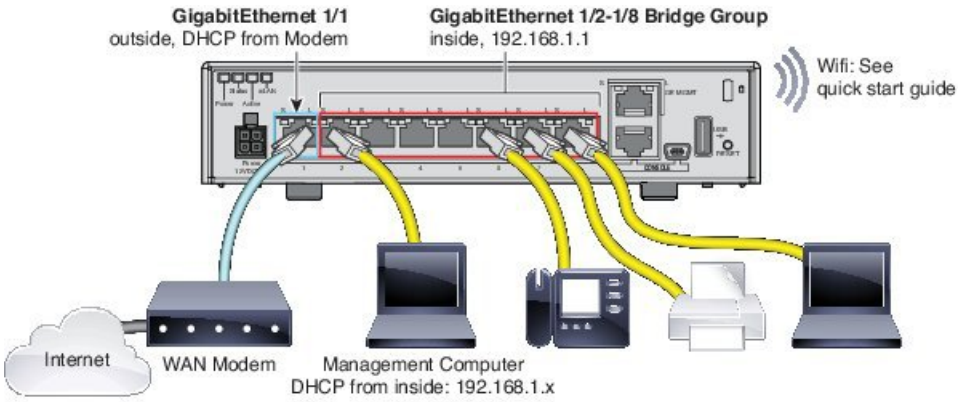
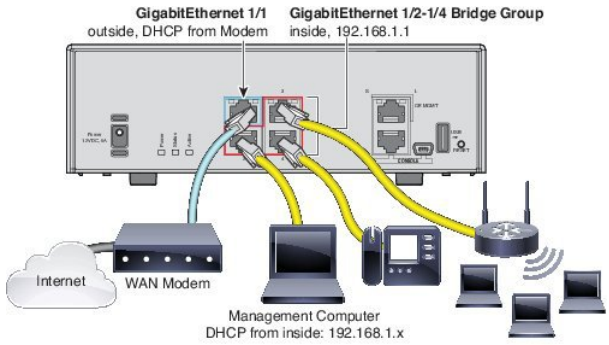


Figure 2: ASA 5506H-X



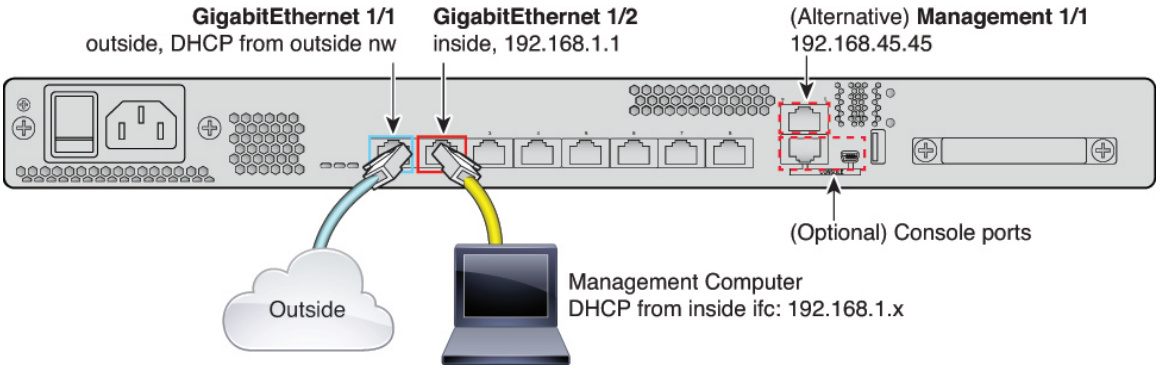
- Attach GigabitEthernet 1/1 to the ISP/WAN modem or other outside device. By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.
- Attach GigabitEthernet 1/2 (or another of the inside bridge group member ports) to your workstation, the one you will use to configure the device. Configure the workstation to obtain an IP address using DHCP. The workstation gets an address on the 192.168.1.0/24 network.

Note You have a couple of other options for connecting the management workstation. You can also directly connect it to the Management port. The workstation gets an address through DHCP on the 192.168.45.0/24 network. Another option is to leave your workstation attached to a switch, and attach that switch to one of the inside ports such as GigabitEthernet1/2. However, you must ensure that no other device on the switch's network is running a DHCP server, because it will conflict with the one running on the inside bridge group, 192.168.1.1.

- Optionally, attach other endpoints or switches to the other ports in the inside bridge group. You might want to wait until you complete the initial device setup before adding endpoints. If you add switches, ensure that there are no other DHCP servers running on those networks, as this conflicts with the DHCP server running on the inside bridge group.

Cabling for ASA 5508-X and 5516-X

Figure 3: Cabling the ASA 5508-X or 5516-X



- Connect your management computer to either of the following interfaces:
  - GigabitEthernet 1/2—Connect your management computer directly to GigabitEthernet 1/2 for initial configuration, or connect GigabitEthernet 1/2 to your inside network. GigabitEthernet 1/2 has a default IP address (192.168.1.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings
  - Management 1/1—Connect your management computer directly to Management 1/1 for initial configuration, or connect Management 1/1 to your management network. Management 1/1 has a default IP address (192.168.45.45) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings.

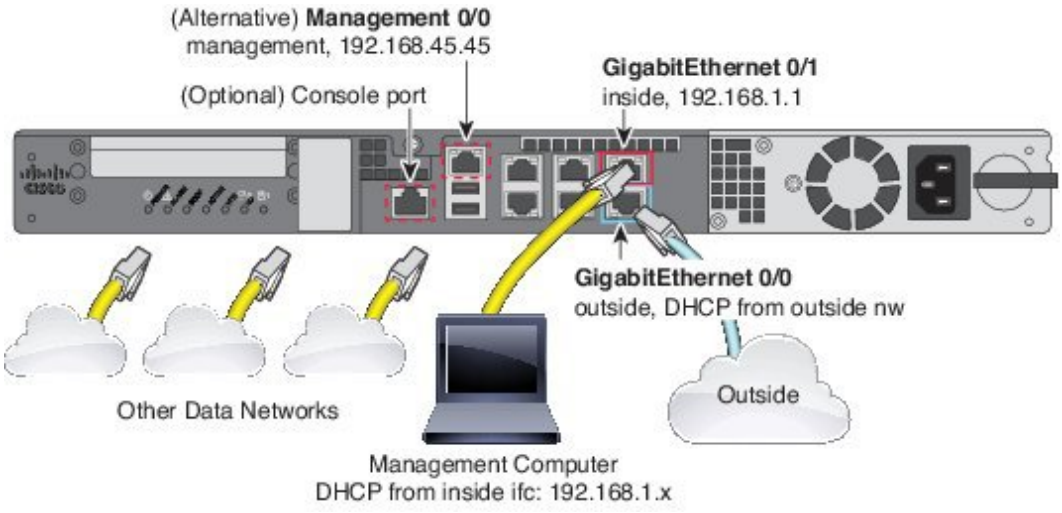
    If you need to change the Management 1/1 IP address from the default, you must also cable your management PC to the console port. See (Optional) Change Management Network Settings at the CLI, on page 22.

  You can later configure the FDM management access from other interfaces.
- Connect the outside network to the GigabitEthernet1/1 interface.

  By default, the IP address is obtained using IPv4 DHCP, but you can set a static address during initial configuration.
- Connect other networks to the remaining interfaces.

Cabling for ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X

Figure 4: Cabling the ASA 5500-X



- Connect your management computer to either of the following interfaces:
  - GigabitEthernet 0/1—Connect your management computer directly to GigabitEthernet 0/1 for initial configuration, or connect GigabitEthernet 0/1 to your inside network. GigabitEthernet 0/1 has a default IP address (192.168.1.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings

- Management 0/0—Connect your management computer directly to Management 0/0 for initial configuration, or connect Management 0/0 to your management network. Management 0/0 has a default IP address (192.168.45.45) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings.

  If you need to change the Management 0/0 IP address from the default, you must also cable your management computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 22.

You can later configure the FDM management access from other interfaces.

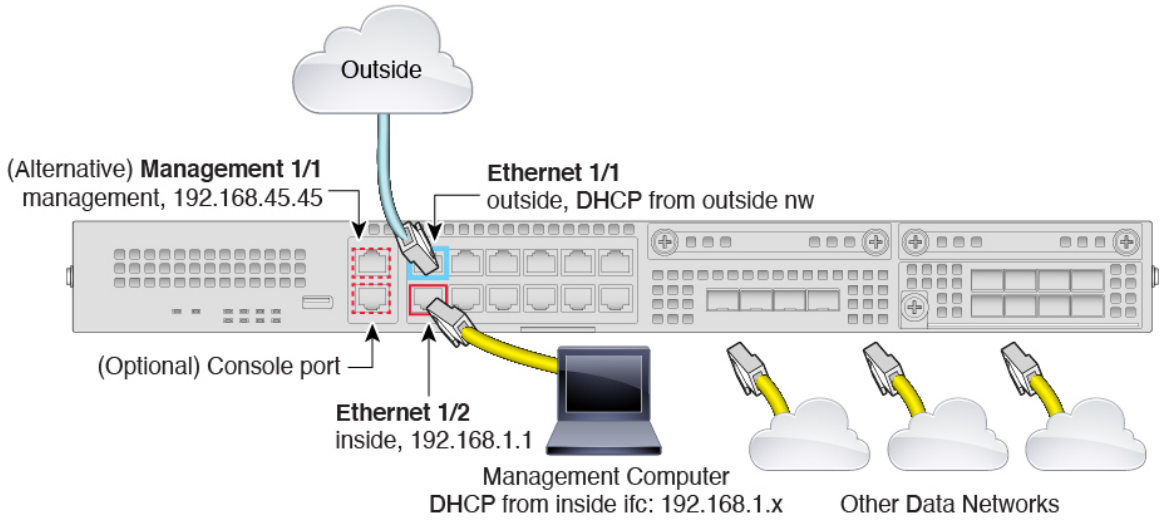
- Connect the outside network to the GigabitEthernet 0/0 interface.

  By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.

- Connect other networks to the remaining interfaces.

Cabling for the Firepower 2100

Figure 5: Cabling the Firepower 2100



- Connect your management computer to either of the following interfaces:

  - Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.1.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings

  - Management 1/1 (labeled MGMT)—Connect your management computer directly to Management 1/1 for initial configuration, or connect Management 1/1 to your management network. Management 1/1 has a default IP address (192.168.45.45) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings.

If you need to change the Management 1/1 IP address from the default, you must also cable your management computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 22.

You can later configure management access from other interfaces.

- Connect the outside network to the Ethernet1/1 interface (labeled WAN).

  By default, the IP address is obtained using IPv4 DHCP, but you can set a static address during initial configuration.

- Connect other networks to the remaining interfaces.

Virtual Cabling for the FTDv

To install the FTDv, see the quick start guide for your virtual platform at http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html. The FDM is supported on the following virtual platforms: VMware, KVM.

The FTDv default configuration puts the management interface and inside interface on the same subnet. You must have Internet connectivity on the management interface in order to use Smart Licensing and to obtain updates to system databases.

Thus, the default configuration is designed so that you can connect both the Management0/0 and GigabitEthernet0/1 (inside) to the same network on the virtual switch. The default management address uses the inside IP address as the gateway. Thus, the management interface routes through the inside interface, then through the outside interface, to get to the Internet.

You also have the option of attaching Management0/0 to a different subnet than the one used for the inside interface, as long as you use a network that has access to the Internet. Ensure that you configure the management interface IP address and gateway appropriately for the network.

Note that the management interface IP configuration is defined on **Device** > **System Settings** > **Management Interface**. It is not the same as the IP address for the Management0/0 (diagnostic) interface listed on **Device** > **Interfaces** > **View Configuration**.

How VMware Network Adapters and Interfaces Map to the FTD Physical Interfaces

You can configure up to 10 interfaces for a VMware FTDv device. You must configure a minimum of 4 interfaces.

Ensure that the Management0-0 source network is associated to a VM network that can access the Internet. This is required so that the system can contact the Cisco Smart Software Manager and also to download system database updates.

You assign the networks when you install the OVF. As long as you configure an interface, you can later change the virtual network through the VMware Client. However, if you need to add a new interface, the process is more cumbersome, as explained in Add Interfaces to the FTDv.

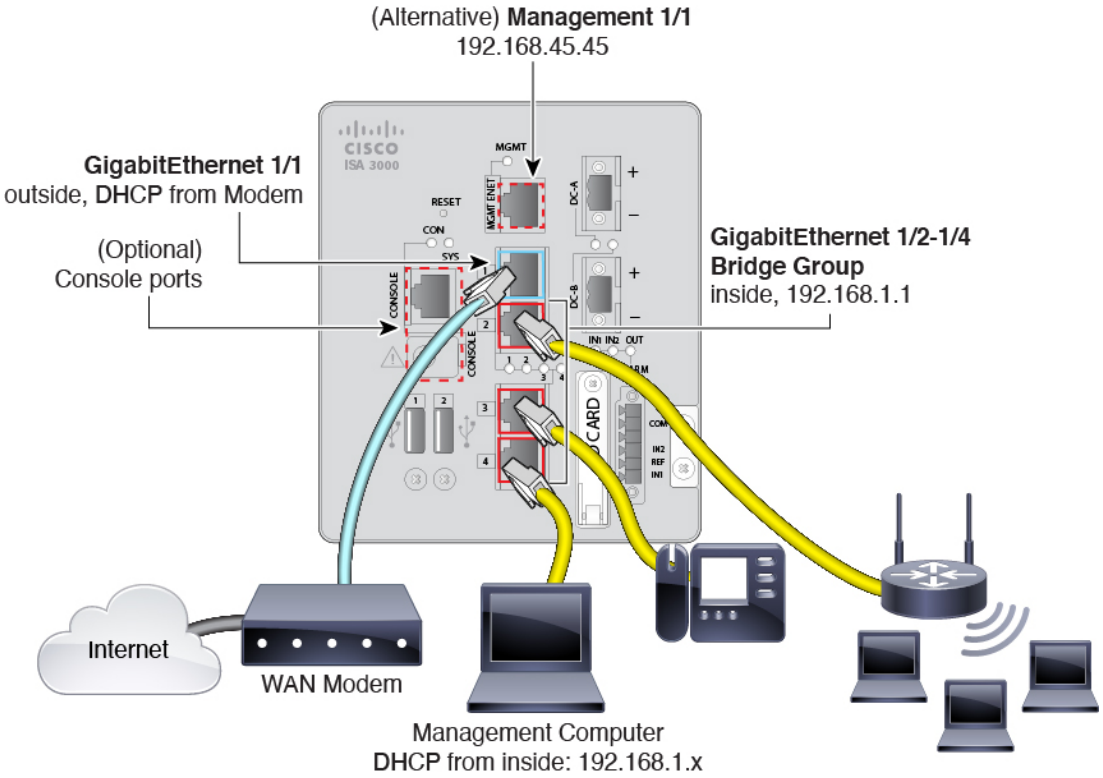
The following table explains how the VMware network adapter and source interface map to the FTDv physical interface names. For additional interfaces, the naming follows the same pattern, increasing the relevant numbers by one. All additional interfaces are data interfaces. For more information on assigning virtual networks to virtual machines, see the VMware online help.

Table 2: Source to Destination Network Mapping

Network Adapter	Source Network	Destination Network (Physical Interface Name)	Function
Network adapter 1	Management0-0	Diagnostic0/0	Management and diagnostic
Network adapter 2	GigabitEthernet0-0	GigabitEthernet0/0	Inside data
Network adapter 3	GigabitEthernet0-1	GigabitEthernet0/1	Outside data
Network adapter 4	GigabitEthernet0-2	GigabitEthernet0/2	Data traffic
Network adapter 5	GigabitEthernet0-3	GigabitEthernet0/3	Data traffic
Network adapter 6	GigabitEthernet0-4	GigabitEthernet0/4	Data traffic
Network adapter 7	GigabitEthernet0-5	GigabitEthernet0/5	Data traffic
Network adapter 8	GigabitEthernet0-6	GigabitEthernet0/6	Data traffic
Network adapter 9	GigabitEthernet0-7	GigabitEthernet0/7	Data traffic
Network adapter 10	GigabitEthernet0-8	GigabitEthernet0/8	Data traffic

Cabling for ISA 3000

Figure 6: ISA 3000



- Attach GigabitEthernet 1/1 to the ISP/WAN modem or other outside device. By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.
- Attach GigabitEthernet 1/2 (or another of the inside bridge group member ports) to your workstation, the one you will use to configure the device. Configure the workstation to obtain an IP address using DHCP. The workstation gets an address on the 192.168.1.0/24 network.

Note You have a couple of other options for connecting the management workstation. You can also directly connect it to the Management port. The workstation gets an address through DHCP on the 192.168.45.0/24 network. Another option is to leave your workstation attached to a switch, and attach that switch to one of the inside ports such as GigabitEthernet1/2. However, you must ensure that no other device on the switch's network is running a DHCP server, because it will conflict with the one running on the inside bridge group, 192.168.1.1.

- Optionally, attach other endpoints or switches to the other ports in the inside bridge group. You might want to wait until you complete the initial device setup before adding endpoints. If you add switches, ensure that there are no other DHCP servers running on those networks, as this conflicts with the DHCP server running on the inside bridge group.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.

Note You cannot repeat the CLI setup script unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See Cisco Secure Firewall Threat Defense Command Reference.

Procedure

Step 1 Connect to the FTD console port. See Logging Into the Command Line Interface (CLI), on page 11 for more information.

Step 2 Log in with the username **admin**.

The default admin password is Admin123.

Step 3 The first time you log into the FTD, you are prompted to accept the End User License Agreement (EULA). You are then presented with the CLI setup script.

Defaults or previously-entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the FDM (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that the FDM management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected. Note also that the DHCP server on Management will be disabled if you change the IP address.
- **Manage the device locally?**—Enter **yes** to use the FDM. A **no** answer means you intend to use the FMC to manage the device.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]
```

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
DHCP Server Disabled
The DHCP server has been disabled. You may re-enable with configure network ipv4
dhcp-server-enable

For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Step 4 Log into the FDM on the new Management IP address.

Complete the Initial Configuration Using the Setup Wizard

When you initially log into the FDM, you are taken through the device setup wizard to complete the initial system configuration.

Before you begin

Ensure that you connect a data interface to your gateway device, for example, a cable modem or router. For edge deployments, this would be your Internet-facing gateway. For data center deployments, this would be a back-bone router. Use the default “outside” interface for your model (see Connect the Interfaces, on page 15 and Default Configuration Prior to Initial Setup, on page 29).

Then, connect your management computer to the “inside” interface for your hardware model. Alternatively, you can connect to the Management interface. For the FTDv, simply ensure that you have connectivity to the management IP address.

(Except for the FTDv, which requires connectivity to the internet from the management IP address.) The Management interface does not need to be connected to a network. By default, the system obtains system licensing and database and other updates through the data interfaces, typically the outside interface, that connect to the internet. If you instead want to use a separate management network, you can connect the Management interface to a network and configure a separate management gateway after you complete initial setup.

To change the Management interface network settings if you cannot access the default IP address, see (Optional) Change Management Network Settings at the CLI, on page 22.

Procedure

Step 1 Log into the FDM.

a) Assuming you did not go through initial configuration in the CLI, open the FDM at **https://***ip-address*, where the address is one of the following.

- If you are connected to the inside interface: **https://192.168.1.1**.
- (Required for the FTDv) If you are connected to the Management interface: **https://192.168.45.45**.

b) Log in with the username **admin**. The default admin password is Admin123. .

Step 2 If this is the first time logging into the system, and you did not use the CLI setup wizard, you are prompted to read and accept the End User License Agreement and change the admin password.

You must complete these steps to continue.

Step 3 Configure the following options for the outside and management interfaces and click **Next**.

Caution Your settings are deployed to the device when you click **Next**. The interface will be named "outside" and it will be added to the "outside_zone" security zone. Ensure that your settings are correct.

Outside Interface

- **Configure IPv4**—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. Do not configure an IP address on the same subnet as the default inside address (see Default Configuration Prior to Initial Setup, on page 29), either statically or through DHCP.
- **Configure IPv6**—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

Management Interface

- **DNS Servers**—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields. Your ISP might require that you use specific DNS servers. If after completing the wizard, you find that DNS resolution is not working, see Troubleshooting DNS for the Management Interface.
- **Firewall Hostname**—The hostname for the system's management address.

Step 4 Configure the system time settings and click **Next**.

- **Time Zone**—Select the time zone for the system.
- **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

Step 5 Configure the smart licenses for the system.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, click the link to log into your Smart Software Manager account, generate a new token, and copy the token into the edit box.

If you do not want to register the device yet, select the evaluation mode option. The evaluation period last up to 90 days. To later register the device and obtain smart licenses, click **Device**, then click the link in the **Smart Licenses** group.

Step 6 Click **Finish**.

What to do next

- If you want to use features covered by optional licenses, such as category-based URL filtering, intrusion inspection, or malware prevention, enable the required licenses. See Enabling or Disabling Optional Licenses.
- Connect the other data interfaces to distinct networks and configure the interfaces. For information on configuring interfaces, see How to Add a Subnet and Interfaces.
- If you are managing the device through the inside interface, and you want to open CLI sessions through the inside interface, open the inside interface to SSH connections. See Configuring the Management Access List.
- Go through the use cases to learn how to use the product. See Best Practices: Use Cases for FTD.

What to Do if You Do Not Obtain an IP Address for the Outside Interface

The default device configuration includes a static IPv4 address for the inside interface. You cannot change this address through the initial device setup wizard, although you can change it afterwards.

The default inside IP address might conflict with other networks attached to the device. This is especially true if you use DHCP on the outside interface to obtain an address from your Internet Service Provider (ISP). Some ISPs use the same subnet as the inside network as the address pool. Because you cannot have two data interfaces with addresses on the same subnet, conflicting addresses from the ISP cannot be configured on the outside interface.

If there is a conflict between the inside static IP address and the DHCP-provided address on the outside interface, the connection diagram should show the outside interface as administratively UP, but with no IPv4 address.

The setup wizard will complete successfully in this case, and all the default NAT, access, and other policies and settings will be configured. Simply follow the procedure below to eliminate the conflict.

Before you begin

Verify that you have a healthy connection to the ISP. Although a subnet conflict will prevent you from getting an address on the outside interface, you will also fail to get one if you simply do not have a link to the ISP.

Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

Step 2 Mouse over the **Actions** column for the inside interface and click the edit icon ( ).

Step 3 On the **IPv4 Address** tab, enter a static address on a unique subnet, for example, 192.168.2.1/24 or 192.168.46.1/24. Note that the default management address is 192.168.45.45/24, so do not use that subnet.

You also have the option to use DHCP to obtain an address if you have a DHCP server already running on the inside network. However, you must first click **Delete** in the **DHCP SERVER IS DEFINED FOR THIS INTERFACE** group to remove the DHCP server from the interface.

Step 4 In the **DHCP SERVER IS DEFINED FOR THIS INTERFACE** area, click **Edit** and change the DHCP pool to a range on the new subnet, for example, 192.168.2.5-192.168.2.254.

Step 5 Click **OK** to save the interface changes.

Step 6 Click the **Deploy** button in the menu to deploy your changes.

Step 7 Click **Deploy Now**.

After deployment completes, the connection graphic should show that the outside interface now has an IP address. Use a client on the inside network to verify you have connectivity to the Internet or other upstream network.

Configure the Wireless Access Point (ASA 5506W-X)

The ASA 5506W-X includes a Cisco Aironet 702i wireless access point integrated into the device. The wireless access point is disabled by default. Connect to the access point web interface so that you can enable the wireless radios and configure the SSID and security settings.

The access point connects internally over the GigabitEthernet1/9 interface. All Wi-Fi clients belong to the GigabitEthernet1/9 network. Your security policy determines how the Wi-Fi network can access any networks on other interfaces. The access point does not contain any external interfaces or switch ports.

The following procedure explains how to configure the access point. The procedure assumes that you completed the device setup wizard. If you instead manually configured the device, you might need to adjust the steps based on your configuration.

For more information, see the following manuals:

- For details about using the wireless LAN controller, see the Cisco Wireless LAN Controller Software documentation.
- For details about the wireless access point hardware and software, see the Cisco Aironet 700 Series documentation.

Before you begin

If you are unable to reach the access point, and the FTD device has the suggested configuration, and other networking issues are not found, then you may want to restore the access point default configuration. You must access the FTD CLI (connect to the console port, or configure SSH access). From the FTD CLI, enter the following commands.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
```

```
Password: <press enter, by default, the password is blank>
firepower# hw-module module wlan recover configuration
```

If you need to troubleshoot the access point further, connect to the access point CLI using the **session wlan console** command.

Procedure

Step 1 Configure and enable the wireless interface, GigabitEthernet1/9.

a) Click **Device**, then click the link in the **Interfaces** group to open the list of interfaces.

b) Click the edit icon ( ) for the GigabitEthernet1/9 interface.

c) Configure the following options.

- **Interface Name**—Enter a name for the interface, for example, **wifi**.
- **Status**—Click the slider to enable the interface.
- **IPv4 Address**—Select **Static** for the address type, then enter an address and subnet mask. For example, 192.168.10.1/24.

d) Click **Save**.

Step 2 Add the Wi-Fi interface to the same security zone as the inside interfaces.

The device setup wizard puts the members of the **inside** bridge group in a security zone named **inside_zone**. The Wi-Fi interface needs to be in the same zone so that you can reach the access point web interface (made possible by the default Inside_Inside_Rule access rule).

a) Click **Objects** in the menu, then select **Security Zones** from the table of contents.

b) Click the edit icon ( ) for **inside_zone**.

c) Click + under **Interfaces** and select the **wifi** interface.

Step 3 Verify that there is an access control rule to allow traffic between interfaces in the **inside_zone** security zone.

The device setup wizard creates a rule to allow traffic to flow from the **inside_zone** to the **outside_zone**, which allows inside users to get to the Internet.

The wizard also create a rule to allow traffic to flow between the **inside_zone** and **inside_zone**, so that internal hosts can reach each other.

By adding the **wifi** interface to **inside_zone**, Wi-Fi users are also included in both of these rules, so that they can reach the Internet and other internal users.

If you did not complete the wizard, these rules might not exist. Because the default action is to block all traffic, you must create these rules. The following procedure explains how to create a rule to enable traffic between the interfaces in the **inside_zone** security zone.

a) Click **Policies** in the menu.

b) Click + above the **Access Control** table to add a rule.

c) Configure at least the following options in the rule.

- **Title**—Enter a name for the rule. For example, Inside_Inside.
- **Action**—Either Allow or Trust.

- **Source/Destination** > **Source Zones**—Select inside_zone.
- **Source/Destination** > **Destination Zones**—Select inside_zone.

d) Click **OK**.

Step 4 Configure the DHCP server on the wireless interface.

The DHCP server supplies IP addresses to devices that connect to the access point. It also supplies an address to the access point itself.

a) Click **Device**.
b) Click **System Settings** > **DHCP Server**.
c) Click the **DHCP Servers** tab.
d) Click **+** above the DHCP server table.
e) Configure the following DHCP server properties.

- **Enable DHCP Server**—Click the slider to enable the DHCP server.
- **Interface**—Select the **wifi** interface.
- **Address Pool**—Enter the address pool for DHCP clients. For example, if you used the example address for the wireless interface, the pool would be 192.168.10.2-192.168.10.254. The pool must be on the same subnet as the IP address for the interface, and it cannot include the address of the interface or the broadcast address.

f) Click **OK**.

Step 5 Click the Deploy button in the menu, then click the **Deploy Now** button, to deploy your changes to the device.

Wait until the deployment finishes before you continue.

Step 6 Configure the wireless access point.

The wireless access point obtains its address from the DHCP pool defined for the wireless interface. It should get the first address in the pool. If you used the example addresses, this is 192.168.10.2. (Try the next address in the pool if the first one does not work.)

a) Use a new browser window to go to the wireless access point IP address, for example, **http://192.168.10.2**.

The access point web interface should appear.

You must be on the inside network, or a network that can route to it, to open this address.

b) Log in with the username **cisco** and password **Cisco**.
c) On the left, click **Easy Setup** > **Network Configuration**.
d) In the **Radio Configuration** area, for each of the **Radio 2.4GHz** and **Radio 5GHz** sections, set at least the following parameters and click **Apply** for each section.

- **SSID**—The Service Set Identifier. This is the name of the wireless network. Users will see this name when selecting a wireless network for their Wi-Fi connection.
- **Broadcast SSID in Beacon**—Select this option.
- **Universal Admin Mode: Disable**.

- **Security**—Select whichever security option you want to use.

Step 7 While in the wireless access point web interface, enable the radios.

a) On the left, click **Summary**, and then on the main page under **Network Interfaces**, click the link for the 2.4 GHz radio.
b) Click the **Settings** tab.
c) For the **Enable Radio** setting, click the **Enable** radio button, and then click **Apply** at the bottom of the page.
d) Repeat the process for the 5 GHz radio.

Default Configuration Prior to Initial Setup

Before you initially configure the FTD device using the local manager (FDM), the device includes the following default configuration.

For many models, this configuration assumes that you open the device manager through the inside interface, typically by plugging your computer directly into the interface, and use the DHCP server defined on the inside interface to supply your computer with an IP address. Alternatively, you can plug your computer into the Management interface and use DHCP to obtain an address. However, some models have different default configurations and management requirements. See the table below for details.

Note You can pre-configure many of these settings using the CLI setup ((Optional) Change Management Network Settings at the CLI, on page 22) before you perform setup using the wizard.

Default Configuration Settings

Setting	Default	Can be changed during initial configuration?
Password for admin user.	Admin123	Yes. You must change the default password.
Management IP address.	FTDv192.168.45.45	No.
Management gateway.	The data interfaces on the device. Typically the outside interface becomes the route to the Internet. This gateway works for from-the-device traffic only. FTDv: 192.168.45.1	No.
DHCP server on the management interface.	Enabled with the address pool 192.168.45.46-192.168.45.254. FTDv: No DHCP server enabled.	No.
DNS servers for the management interface.	The OpenDNS public DNS servers, 208.67.220.220 and 208.67.222.222.	Yes

Setting	Default	Can be changed during initial configuration?
Inside interface IP address.	192.168.1.1/24 FTDv: 192.168.45.1/24	No.
DHCP server for inside clients.	Running on the inside interface with the address pool 192.168.1.5 - 192.168.1.254. FTDv: The address pool on the inside interface is 192.168.45.46 - 192.168.45.254.	No.
DHCP auto-configuration for inside clients. (Auto-configuration supplies clients with addresses for WINS and DNS servers.)	Enabled on outside interface.	Yes, but indirectly. If you configure a static IPv4 address for the outside interface, DHCP server auto-configuration is disabled.
Outside interface IP address.	Obtained through DHCP from Internet Service Provider (ISP) or upstream router.	Yes.

Default Interfaces by Device Model

You cannot select different inside and outside interfaces during initial configuration. To change the interface assignments after configuration, edit the interface and DHCP settings. You must remove an interface from the bridge group before you can configure it as a non-switched interface.

FTD device	Outside Interface	Inside Interface
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet1/1	BVI1, which contains all other data interfaces except the outside interface, and for the 5506W-X, the wireless interface GigabitEthernet1/9.
ASA 5508-X ASA 5516-X	GigabitEthernet1/1	GigabitEthernet1/2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet0/0	GigabitEthernet0/1
Firepower 2100 series	Ethernet1/1	Ethernet1/2
FTDv	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1	BVI1, which contains all other data interfaces except the outside interface.

Configuration After Initial Setup

After you complete the setup wizard, the device configuration will include the following settings. The table shows whether a particular setting is something you explicitly chose or whether it was defined for you based on your other selections. Validate any "implied" configurations and edit them if they do not serve your needs.

Setting	Configuration	Explicit, implied, or default configuration
Password for admin user.	Whatever you entered.	Explicit.
Management IP address.	FTDv: 192.168.45.45	Default.
Management gateway.	The data interfaces on the device. Typically the outside interface becomes the route to the Internet. The management gateway works for from-the-device traffic only. FTDv: 192.168.45.1	Default.
DHCP server on management interface.	Enabled with the address pool 192.168.45.46-192.168.45.254. FTDv: No DHCP server enabled.	Default.
DNS servers for the management interface.	The OpenDNS public DNS servers, 208.67.220.220, 208.67.222.222, or whatever you entered. DNS servers obtained from DHCP are never used.	Explicit.
Management hostname.	**firepower** or whatever you entered.	Explicit.
Management access through data interfaces.	A data interface management access list rule allows HTTPS access through the inside interface. SSH connections are not allowed. Both IPv4 and IPv6 connections are allowed. FTDv: No data interfaces have default management access rules.	Implied.
System time.	The time zone and NTP servers you selected.	Explicit.
Smart license.	Either registered with a base license, or the evaluation period activated, whichever you selected. Subscription licenses are not enabled. Go to the smart licensing page to enable them.	Explicit.
Inside interface IP address.	192.168.1.1/24 FTDv: 192.168.45.1/24	Default.
DHCP server for inside clients.	Running on the inside interface with the address pool 192.168.1.5 - 192.168.1.254. FTDv: The address pool on the inside interface is 192.168.45.46 - 192.168.45.254.	Default.

Setting	Configuration	Explicit, implied, or default configuration
DHCP auto-configuration for inside clients. (Auto-configuration supplies clients with addresses for WINS and DNS servers.)	Enabled on outside interface if you use DHCP to obtain the outside interface IPv4 address. If you use static addressing, DHCP auto-configuration is disabled.	Explicit, but indirectly.
Data interface configuration.	• ASA 5506-X, ISA 3000—All data interfaces (such as GigabitEthernet1/2) except the outside interface are enabled and part of the inside bridge group. You can plug end points or switches into these ports and obtain addresses from the DHCP server for the inside interface. These interfaces are named inside_1, inside_2, and so forth. • All other models—The outside and inside interfaces are the only ones configured and enabled. All other data interfaces are disabled.	Default.
Outside physical interface and IP address.	The default outside port based on the device model. See Default Configuration Prior to Initial Setup, on page 29. The IP address is obtained by DHCP, or it is a static address as entered (IPv4, IPv6, or both).	Interface is Default. Addressing is Explicit.
Static routes.	If you configure a static IPv4 or IPv6 address for the outside interface, a static default route is configured for IPv4/IPv6 as appropriate, pointing to the gateway you defined for that address type. If you select DHCP, the default route is obtained from the DHCP server. Network objects are also created for the gateway and the "any" address, that is, 0.0.0.0/0 for IPv4, ::/0 for IPv6.	Implied.
Security zones.	**inside_zone**, containing the inside interface. For models that have an inside bridge group, the zone contains all members of the inside bridge group interface. **outside_zone**, containing the outside interface. (You can edit these zones to add other interfaces, or create your own zones.)	Implied.
Access control policy.	A rule trusting all traffic from the inside_zone to the outside_zone. This allows without inspection all traffic from users inside your network to get outside, and all return traffic for those connections. For models that have an inside bridge group, a second rule trusting all traffic between the interfaces in the inside_zone. This allows without inspection all traffic between users on your inside network. The default action for any other traffic is to block it. This prevents any traffic initiated from outside to enter your network.	Implied.

Setting	Configuration	Explicit, implied, or default configuration
NAT	(Models that do not have an inside bridge group.) An interface dynamic PAT rule translates the source address for any IPv4 traffic destined to the outside interface to a unique port on the outside interface's IP address. (Models that have an inside bridge group.) For each member of the inside bridge group, an interface dynamic PAT rule translates the source address for any IPv4 traffic destined to the outside interface to a unique port on the outside interface's IP address. These appear in the NAT rule table and you can edit them later if desired. There are additional hidden PAT rules to enable HTTPS access through the inside interfaces, and routing through the data interfaces for the management address. These do not appear in the NAT table, but you will see them if you use the **show nat** command in the CLI.	Implied.

Configuration Basics

The following topics explain the basic methods for configuring the device.

Configuring the Device

When you initially log into FDM, you are guided through a setup wizard to help you configure basic settings. Once you complete the wizard, use the following method to configure other features and to manage the device configuration.

If you have trouble distinguishing items visually, select a different color scheme in the user profile. Select **Profile** from the user icon drop-down menu in the upper right of the page.

Procedure

Step 1 Click **Device** to get to the **Device Summary**.

The dashboard shows a visual status for the device, including enabled interfaces and whether key settings are configured (colored green) or still need to be configured. For more information, see Viewing Interface and Management Status, on page 37.

Above the status image is a summary of the device model, software version, VDB (System and Vulnerability Database) version, and the last time intrusion rules were updated.

Below the image are groups for the various features you can configure, with summaries of the configurations in each group, and actions you can take to manage the system configuration.

Step 2 Click the links in each group to configure the settings or perform the actions.

Following is a summary of the groups:

- **Interface**—You should have at least two data interfaces configured in addition to the management interface. See Interfaces.
- **Routing**—The routing configuration. You must define a default route. Other routes might be necessary depending on your configuration. See Routing.
- **Updates**—Geolocation, intrusion rule, and vulnerability database updates, and system software upgrades. Set up a regular update schedule to ensure that you have the latest database updates if you use those features. You can also go to this page if you need to download an update before the regularly schedule update occurs. See Updating System Databases and Feeds.
- **System Settings**—This group includes a variety of settings. Some are basic settings that you would configure when you initially set up the device and then rarely change. See System Settings.
- **Smart License**—Shows the current state of the system licenses. You must install the appropriate licenses to use the system. Some features require additional licenses. See Licensing the System.
- **Backup and Restore**—Back up the system configuration or restore a previous backup. See Backing Up and Restoring the System.
- **Troubleshoot**—Generate a troubleshooting file at the request of the Cisco Technical Assistance Center. See Creating a Troubleshooting File.
- **Site-to-Site VPN**—The site-to-site virtual private network (VPN) connections between this device and remote devices. See Managing Site-to-Site VPNs.
- **Remote Access VPN**—The remote access virtual private network (VPN) configuration that allows outside clients to connect to your inside network. See Configuring Remote Access VPN.
- **Advanced Configuration**—Use FlexConfig and Smart CLI to configure features that you otherwise cannot configure using FDM. See Advanced Configuration.

Step 3 Click the **Deploy** button in the menu to deploy your changes.

Changes are not active on the device until you deploy them. See Deploying Your Changes, on page 35.

What to do next

Click **Policies** in the main menu and configure the security policy for the system. You can also click **Objects** to configure the objects needed in those policies.

Configuring Security Policies

Use the security policies to implement your organization's acceptable use policy and to protect your network from intrusions and other threats.

Procedure

Step 1 Click **Policies**.

The Security Policies page shows the general flow of a connection through the system, and the order in which security policies are applied.

Step 2 Click the name of a policy and configure it.

You might not need to configure each policy type, although you must always have an access control policy. Following is a summary of the policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it. See Configuring SSL Decryption Policies.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address. See Configuring Identity Policies.
- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to selected IP addresses or URLs. By blocking known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence block lists update dynamically. Using feeds, you do not need to edit the policy to add or remove items in the block lists. See Configuring Security Intelligence.
- **NAT** (Network Address Translation)—Use the NAT policy to convert internal IP addresses to externally routeable addresses. See Configure NAT.
- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering. See Configuring the Access Control Policy.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules. See Intrusion Policies.

Step 3 Click the **Deploy** button in the menu to deploy your changes.

Changes are not active on the device until you deploy them. See Deploying Your Changes, on page 35.

Deploying Your Changes

When you update a policy or setting, the change is not immediately applied to the device. There is a two step process for making configuration changes:

1. Make your changes.

2. Deploy your changes.

This process gives you the opportunity to make a group of related changes without forcing you to run a device in a "partially configured" manner. In most cases, the deployment includes just your changes. However, if necessary, the system will reapply the entire configuration, which might be disruptive to your network. In addition, some changes require inspection engines to restart, with traffic dropping during the restart. Thus, consider deploying changes when potential disruptions will have the least impact.

Note If the deployment job fails, the system must roll back any partial changes to the previous configuration. Rollback includes clearing the data plane configuration and redeploying the previous version. This will disrupt traffic until the rollback completes.

After you complete the changes you want to make, use the following procedure to deploy them to the device.

Caution The FTD device drops traffic when the inspection engines are busy because of a software resource issue, or down because a configuration requires the engines to restart during configuration deployment. For detailed information on changes that require a restart, see Configuration Changes that Restart Inspection Engines, on page 36.

Procedure

Step 1 Click the **Deploy Changes** icon in the upper right of the web page.

The icon is highlighted with a dot when there are undeployed changes.

The Deployment Summary page opens. The window shows a list of previous deployments with summary information on the changes ("modified objects"), when the deployment was initiated and completed, and the status of each deployment.

If the deployment requires that inspection engines be restarted, the page includes a message that provides detail on what changed that requires a restart. If momentary traffic loss at this time would be unacceptable, close the dialog box and wait until a better time to deploy changes.

If the icon is not highlighted, you can still click it to see the results of previous deployment jobs.

Step 2 Click **Deploy Now**.

Configuration Changes that Restart Inspection Engines

Any of the following configurations or actions restart inspection engines when you deploy configuration changes.

Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires inspection engines to restart, which interrupts traffic inspection and drops traffic.

Deployment

Some changes require that inspection engines be restarted, which will result in momentary traffic loss. Following are the changes that require inspection engine restart:

- SSL decryption policy is enabled or disabled.
- The MTU changed on one or more physical interfaces (but not subinterfaces).
- You add or remove a file policy on an access control rule.
- The rule database was updated.
- The VDB was updated.

In addition, some packets might be dropped during deployment if the Snort process is busy, with the total CPU utilization exceeding 60%. You can check the current CPU utilization for Snort using the **show asp inspect-dp snort** command.

System Database Updates

If you download an update to the Rules database or VDB, you must deploy the update for it to become active. This deployment might restart inspection engines. When you manually download an update, or schedule an update, you can indicate whether the system should automatically deploy changes after the download is complete. If you do not have the system automatically deploy the update, the update is applied the next time you deploy changes, at which time inspection engines might restart.

System Updates

Installing a system update or patch that does not reboot the system and includes a binary change requires inspection engines to restart. Binary changes can include changes to inspection engines, a preprocessor, the vulnerability database (VDB), or a shared object rule. Note also that a patch that does not include a binary change can sometimes require a Snort restart.

Viewing Interface and Management Status

The Device Summary includes a graphical view of your device and select settings for the management address. To open the Device Summary, click **Device**.

Elements on this graphic change color based on the status of the element. Mousing over elements sometimes provides additional information. Use this graphic to monitor the following items.

Note The interface portion of the graphic, including interface status information, is also available on the **Interfaces** page and the **Monitoring** > **System** dashboard.

Interface Status

Mouse over a port to see its IP addresses, and enabled and link statuses. The IP addresses can be statically assigned or obtained using DHCP. Mousing over a Bridge Virtual Interface (BVI) also shows the list of member interfaces.

Interface ports use the following color coding:

- Green—The interface is configured, enabled, and the link is up.
- Gray—The interface is not enabled.
- Orange/Red—The interface is configured and enabled, but the link is down. If the interface is wired, this is an error condition that needs correction. If the interface is not wired, this is the expected status.

Inside, Outside Network Connections

The graphic indicates which port is connected to the outside (or upstream) and inside networks, under the following conditions.

- Inside Network—The port for the inside network is shown for the interface named "inside" only. If there are additional inside networks, they are not shown. If you do not name any interface "inside," no port is marked as the inside port.
- Outside Network—The port for the outside network is shown for the interface named "outside" only. As with the inside network, this name is required, or no port is marked as the outside port.

Management Setting Status

The graphic shows whether the gateway, DNS servers, NTP servers, and Smart Licensing are configured for the management address, and whether those settings are functioning correctly.

Green indicates that the feature is configured and functioning correctly, gray indicates that it is not configured or not functioning correctly. For example, the DNS box is gray if the servers cannot be reached. Mouse over the elements to see more information.

If you find problems, correct them as follows:

- Management port and gateway—Select **System Settings** > **Management Interface**.
- DNS servers—Select **System Settings** > **DNS Server**.
- NTP servers—Select **System Settings** > **NTP**. Also see Troubleshooting NTP.
- Smart License—Click the **View Configuration** link in the Smart License group.

Viewing System Task Status

System tasks include actions that occur without your direct involvement, such as retrieving and applying various database updates. You can view a list of these tasks and their status to verify that these system tasks are completing successfully.

Procedure

Step 1 Click the **Task List** button in the main menu.

The task list opens, displaying the status and details of system tasks.

Step 2 Evaluate the task status.

If you find a persistent problem, you might need to fix the device configuration. For example, a persistent failure to obtain database updates could indicate that there is no path to the Internet for the device's management IP address. You might need to contact the Cisco Technical Assistance Center (TAC) for some issues as indicted in the task descriptions.

You can do the following with the task list:

- Click the **Success** or **Failures** buttons to filter the list based on these statuses.
- Click the delete icon () for a task to remove it from the list.
- Click **Remove All Completed Tasks** to empty the list of all tasks that are not in progress.

Using the CLI Console to Monitor and Test the Configuration

FTD devices include a command line interface (CLI) that you can use for monitoring and troubleshooting. Although you can open an SSH session to get access to all of the system commands, you can also open a CLI Console in the FDM to use read-only commands, such as the various **show** commands and **ping**, **traceroute**, and **packet-tracer**.

You can keep the CLI Console open as you move from page to page, configure, and deploy features. For example, after deploying a new static route, you could use **ping** in the CLI Console to verify that the target network is reachable.

The CLI Console uses the base FTD CLI. You cannot enter the diagnostic CLI, expert mode, or FXOS CLI (on models that use FXOS) using the CLI Console. Use SSH if you need to enter those other CLI modes.

For detailed information on commands, see Cisco Firepower Threat Defense Command Reference, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Notes:

- Although **ping** is supported in CLI Console, the **ping system** command is not supported.
- The system can process at most 2 concurrent commands. Thus, if another user is issuing commands (for example, using the REST API), you might need to wait for other commands to complete before entering a command. If this is a persistent problem, use an SSH session instead of the CLI Console.
- Commands return information based on the deployed configuration. If you make a configuration change in the FDM, but do not deploy it, you will not see the results of your change in the command output. For example, if you create a new static route but do not deploy it, that route will not appear in **show route** output.

Procedure

Step 1 Click the **CLI Console** button in the upper right of the web page.

Step 2 Type the commands at the prompt and press **Enter**.

Some commands take longer to produce output than others, please be patient. If you get a message that the command execution timed out, please try again. You will also get a time out error if you enter a command that requires interactive responses, such as **show perfstats**. If the problem persists, you might need to use an SSH client instead of the CLI Console.

Following are some tips on how to use the window.

- Press the **Tab** key to automatically complete a command after partially typing it. Also, Tab will list out the parameters available at that point in the command. Tab works down to three levels of keyword. After three levels, you need to use the command reference for more information.
- You can stop command execution by pressing Ctrl+C.
- To move the window, click and hold anywhere in the header, then drag the window to the desired location.
- Click the **Expand** () or **Collapse** () button to make the window bigger or smaller.
- Click the **Undock Into Separate Window** () button to detach the window from the web page into its own browser window. To dock it again, click the **Dock to Main Window** () button.
- Click and drag to highlight text, then press Ctrl+C to copy output to the clipboard.
- Click the **Clear CLI** () button to erase all output.
- Click the **Copy Last Output** () button to copy the output from the last command you entered to the clipboard.

Step 3 When you are finished, simply close the console window. Do not use the **exit** command.

Although the credentials you use to log into the FDM validate your access to the CLI, you are never actually logged into the CLI when using the console.