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
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
ASA 5515-X	6.1

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 the IPv4 or IPv6 address or the DNS name, if you have configured one. Use the management 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.
- Use an SSH client to make a connection to the management IP address. 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 14.

Procedure

Step 1 Connect the Interfaces, on page 6

Step 2 Complete the Initial Configuration Using the Setup Wizard, on page 10

For details about the resulting configuration, see Configuration After Initial Setup, on page 16.

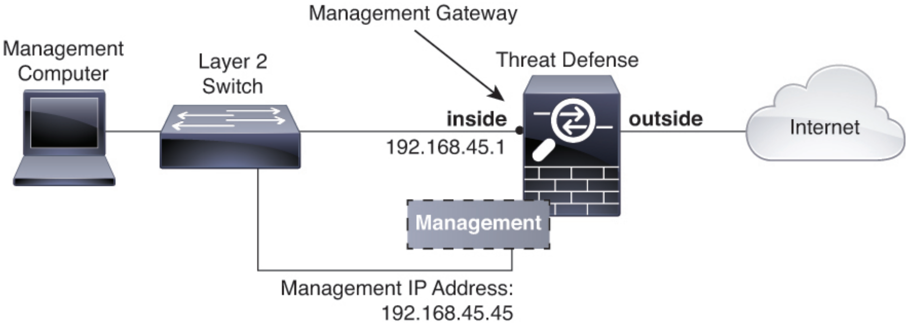
Step 3 Configure the Wireless Access Point (ASA 5506W-X), on page 11

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.

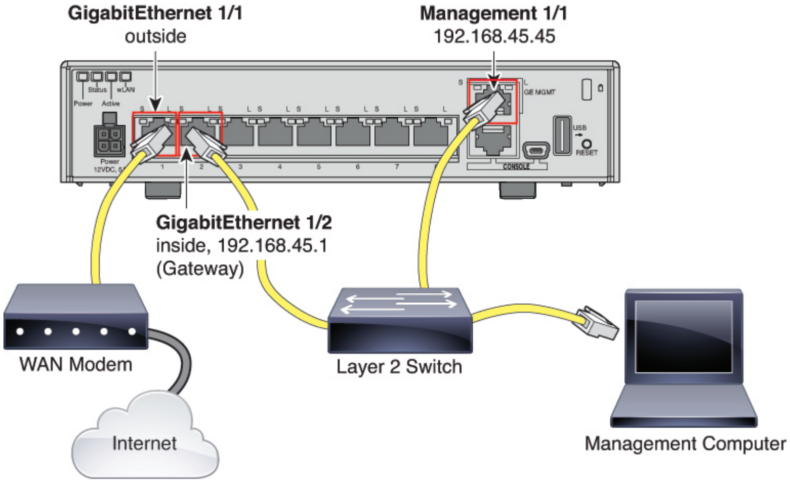
The default configuration also assumes that you will connect the management and inside interfaces to the same network using a switch. The inside interface is configured as a DHCP server, so you can attach your management workstation to the same switch and get an address through DHCP on the same network, so that you can open the FDM web interface.

The following diagram shows the expected network topology.



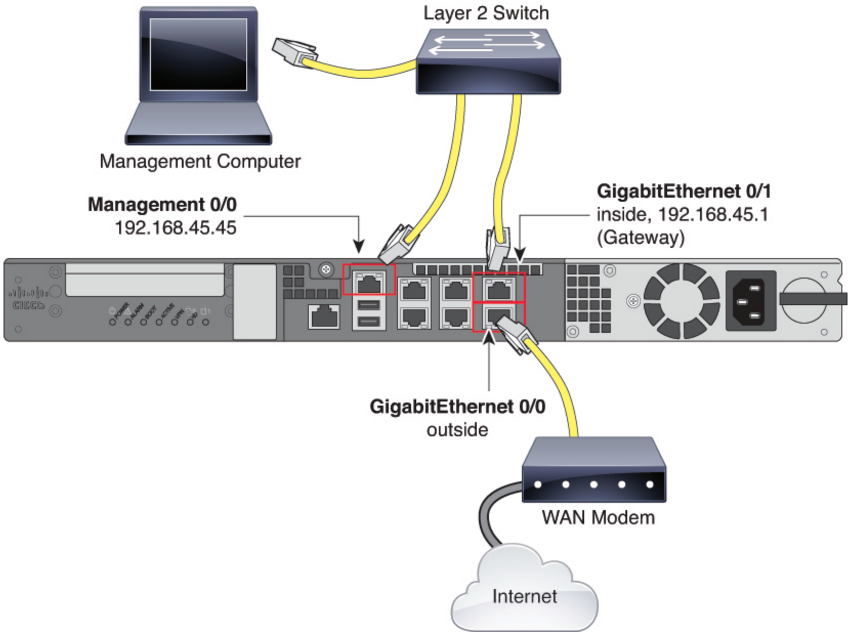
The following diagrams show how to cable the system for this topology. If you want to attach the management and inside networks to different networks using an inside router, see Routed Mode Deployment.

Cabling for ASA 5506-X, 5508-X, and 5516-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 to the layer 2 switch. The IP address is 192.168.45.1, which serves as the gateway for the inside network.
- Attach Management 1/1 to the layer 2 switch. The IP address is 192.168.45.45.
- Attach your workstation to the layer 2 switch and configure it to obtain an address using DHCP.

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



- Attach GigabitEthernet 0/0 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 0/1 to the layer 2 switch. The IP address is 192.168.45.1, which serves as the gateway for the inside network.
- Attach Management 0/0 to the layer 2 switch. The IP address is 192.168.45.45.
- Attach your workstation to the layer 2 switch and configure it to obtain an address using DHCP.

(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 3 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 6 and Default Configuration Prior to Initial Setup, on page 14).

The management interface must also be connected to a gateway through which the internet is accessible. System licensing and database updates require internet access.

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 8.

Procedure

Step 1 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 2 Select the outside interface and click **Next**.

This is the data port that you connected to your gateway modem or router.

Note You cannot select the interface that is configured as the inside interface in the default configuration. If you intend to use the default inside interface as the outside interface, you can skip the device configuration and manually configure your settings. Alternatively, you can select a different interface as a temporary outside interface to complete the setup, then manually edit the configuration to reflect the real outside interface.

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 14), 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. Click **Use OpenDNS** if you want to configure the OpenDNS public DNS servers. Clicking the button loads the appropriate IP addresses into the fields.
- **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 the name of the device in the menu, 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.
- If you connected other interfaces to networks, configure each of the connected interfaces. See How to Add a Subnet and Interfaces.
- Go through the use cases to learn how to use the product. See Best Practices: Use Cases for FTD.

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 the name of the device in the menu, 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 **inside** interface 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.

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 Configure 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. By adding the **wifi** interface to **inside_zone**, Wi-Fi users are also included in the rule that allows Internet access.

However, the default action is to block all traffic, so you must 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 the name of the device in the menu.
b) Click **System Settings** > **DHCP Server**.
c) Click + above the DHCP server table.
d) 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.

e) Click **Add**.

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.

This configuration assumes that you wire the management interface, inside interface, and your computer to the same switch, and use the DHCP server defined on the inside interface to supply your computer with an IP address. See the table below for the default inside and outside interfaces by device model.

Note You can pre-configure many of these settings using the CLI setup ((Optional) Change Management Network Settings at the CLI, on page 8) 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.	192.168.45.1	No.
Inside interface IP address.	192.168.45.1/24	No.
DHCP server for inside clients.	Running on the inside interface with the address pool 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 can select a different outside interface during initial configuration. However, you cannot select a different inside interface. To change the inside interface after configuration, edit the interface and DHCP settings.

FTD device	Outside Interface	Inside Interface
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet1/1	GigabitEthernet1/2
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

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.	192.168.45.1	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.
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.	192.168.45.1	Default.
DHCP server for inside clients.	Running on the inside interface with the address pool 192.168.45.46 - 192.168.45.254.	Default.
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.
Outside physical interface and IP address.	Whichever physical port you selected. The IP address is obtained by DHCP, or it is a static address as entered (IPv4, IPv6, or both).	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.

Setting	Configuration	Explicit, implied, or default configuration
Security zones.	**inside_zone**, containing the inside 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. The default action for any other traffic is to block it. This prevents any traffic initiated from outside to enter your network.	Implied.
NAT	An interface dynamic PAT rule translates the source address for any traffic destined to the outside interface to a unique port on the outside interface's IP address. **Note** This rule prevents connections to external IPv6 addresses. To bypass the PAT rule when using IPv6, edit it and select a network object for the internal IPv4 network as the source address.	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 the name of the device in the menu to get to the **Device Dashboard**.

For example, the following link would appear for a device named 5516-x-1.

5516-x-1

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 21.

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. 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.
- **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.

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 19.

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:

- **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.
- **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.

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 19.

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 20.

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 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

Any deployment restarts the inspection engines.

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 Dashboard includes a graphical view of your device and select settings for the management address. To open the Device Dashboard, click the name of your device in the menu.

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.

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** > **Device Management IP**.
- 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.