Firepower Threat Defense Deployment with FDM

Is This Chapter for You?

This chapter explains how to complete the initial set up and configuration of your Firepower Threat Defense (FTD) device using the Firepower Device Manager (FDM) web-based device setup wizard.

FDM lets you configure the basic features of the software that are most commonly used for small 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 FDM 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) instead.

Note

The Firepower 1010 hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Note

The Firepower 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 does not support the FXOS Firepower Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the FXOS troubleshooting guide for more information.

Note

Privacy Collection Statement—The Firepower 1010 Series does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- End-to-End Procedure, on page 2
- Review the Network Deployment and Default Configuration, on page 3
- Cable the Device, on page 6
- Power On the Device, on page 7
- (Optional) Change Management Network Settings at the CLI, on page 8
- Log Into FDM, on page 9
- Complete the Initial Configuration, on page 10
End-to-End Procedure

See the following tasks to deploy FTD with FDM on your chassis.

1. Review the network and default configuration
2. Cable the device
3. Power on the device
4. (Optional) Change Mgmt Network Settings at the CLI
5. Log into FDM
6. Complete the initial configuration
7. (Optional) Obtain feature licenses
8. Generate a license token
9. Register the device with the Smart Licensing Server
10. Configure the device in FDM

- Configure Licensing, on page 12
- Configure the Device in Firepower Device Manager, on page 18
- Access the FTD and FXOS CLI, on page 21
- View Hardware Information, on page 23
- Power Off the Device, on page 24
- What's Next?, on page 25
<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Pre-Configuration</td>
</tr>
<tr>
<td>3</td>
<td>Pre-Configuration</td>
</tr>
<tr>
<td>4</td>
<td>FTD CLI</td>
</tr>
<tr>
<td>5</td>
<td>Firepower Device Manager</td>
</tr>
<tr>
<td>6</td>
<td>Firepower Device Manager</td>
</tr>
<tr>
<td>7</td>
<td>Cisco Commerce Workspace</td>
</tr>
<tr>
<td>8</td>
<td>Smart Software Manager</td>
</tr>
<tr>
<td>9</td>
<td>Firepower Device Manager</td>
</tr>
<tr>
<td>10</td>
<td>Firepower Device Manager</td>
</tr>
</tbody>
</table>

### Review the Network Deployment and Default Configuration

You can manage the FTD using FDM from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface with its own network settings.

The following figure shows the recommended network deployment for the Firepower 1010. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the FTD performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so after you complete initial setup in FDM.
If you cannot use the default management IP address (for example, your management network does not include a DHCP server), 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. See (Optional) Change Management Network Settings at the CLI, on page 8.

If you need to change the inside IP address, you can do so after you complete initial setup in FDM. For example, you may need to change the inside IP address in the following circumstances:

- If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the FTD cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.

- If you add the FTD to an existing inside network, you will need to change the inside IP address to be on the existing network.

**Figure 1: Suggested Network Deployment**

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.
Default Configuration

The configuration for the Firepower device after initial setup includes the following:

- **inside**—IP address 192.168.1.1
  - (6.5 and later) **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
  - (6.4) **Software switch** (Integrated Routing and Bridging)—Ethernet 1/2 through 1/8 belong to bridge group interface (BVI) 1

- **outside**—Ethernet 1/1, IP address from DHCP or an address you specify during setup
  - **inside→outside** traffic flow

- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

---

**Note**

The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other types of management traffic (to-the-device and from-the-device), such as syslog or SNMP. The Diagnostic interface is not typically used. See the [FDM configuration guide](#) for more information.

- **DNS server for management**—OpenDNS: 208.67.222.222, 208.67.220.220, or servers you specify during setup. DNS servers obtained from DHCP are never used.

- **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup

- **Default routes**
  - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
  - **Management interface**—(6.6 and later) Obtained from management DHCP. If you do not receive a gateway, then the default route is over the backplane and through the data interfaces. (6.5 and earlier) Over the backplane and through the data interfaces

  Note that the FTD requires internet access for licensing and updates.

- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface

- **FDM access**—Management and inside hosts allowed

- **NAT**—Interface PAT for all traffic from inside to outside
Cable the Device

Inversion 6.5 and later, Ethernet 1/2 through 1/8 are configured as hardware switch ports; PoE+ is also available on Ethernet 1/7 and 1/8. In version 6.4, Ethernet 1/2 through 1/8 are configured as bridge group members (software switch ports); PoE+ is not available. The initial cabling is the same for both versions.

Note

For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Note

Manage the Firepower 1010 on either Management 1/1 or Ethernet 1/2 through 1/8. The default configuration also configures Ethernet 1/1 as outside.

Procedure

Step 1

Connect your management computer to one of the following interfaces:

- Ethernet 1/2 through 1/8—Connect your management computer directly to one of the inside switch ports (Ethernet 1/2 through 1/8). inside 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 (see Default Configuration).

- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1
obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the FTD so that you can connect to the IP address from your management computer.

If you need to change the Management 1/1 IP address from the default to configure a static IP address, you must also cable your management computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 8.

Step 2  Connect the outside network to the Ethernet 1/1 interface.
By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.

Step 3  Connect inside devices to the remaining switch ports, Ethernet 1/2 through 1/8.
Ethernet 1/7 and 1/8 are PoE+ ports.

---

**Power On the Device**

System power is controlled by the power cord; there is no power button.

**Before you begin**

It's important that you provide reliable power for your device (using an uninterruptable power supply (UPS), for example). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

**Procedure**

Step 1  Attach the power cord to the device, and connect it to an electrical outlet.
The power turns on automatically when you plug in the power cord.

Step 2  Check the Power LED on the back or top of the device; if it is solid green, the device is powered on.

Step 3  Check the Status LED on the back or top of the device; after it is solid green, the system has passed power-on diagnostics.
(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 CDO or FDM.

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 the FTD command reference.

Procedure

Step 1
Connect to the FTD console port. See Access the FTD and FXOS CLI, on page 21 for more information. Log in with the `admin` user and the default password, `Admin123`.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the FTD login for SSH.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]
Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]
firepower#
```

Step 2
Connect to the FTD CLI.

```
connect ftd
```

Example:

```
firepower# connect ftd
>
```

Step 3
The first time you log in to 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 outgoing 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 FDM on the Management interface if you are directly-connected to the Management network, but for remote management on Management, you need to enter the IP address of a gateway router on the Management network. Note that FDM management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the data-interfaces as a fallback method if DHCP doesn't provide a gateway.

- **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.

- **Manage the device locally?**—Enter yes to use CDO or 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' []:
For HTTP Proxy configuration, run 'configure network http-proxy'

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

> 

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

---

**Log Into FDM**

Log into FDM to configure your FTD.
**Before you begin**

- Use a current version of Firefox, Chrome, Safari, Edge, or Internet Explorer.

**Procedure**

**Step 1**
Enter the following URL in your browser.

- Inside (Ethernet1/2 through 1/8) — **https://192.168.1.1**. You can connect to the inside address on any inside switch port (Ethernet1/2 through 1/8).

- (6.6 and later) Management — **https://management_ip**. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.

- (6.5 and earlier) Management — **https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.

**Step 2**
Log in with the username **admin**, and the default password **Admin123**.

**What to do next**

- Run through the FDM setup wizard; see **Complete the Initial Configuration**, on page 10.

**Complete the Initial Configuration**

Use the setup wizard when you first log into FDM to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- An outside (Ethernet1/1) and an inside interface. Ethernet1/2 through 1/8 are switch ports on the inside VLAN1 interface (6.5 and later) or inside bridge group members on BVI1 (6.4).

- Security zones for the inside and outside interfaces.

- An access rule trusting all inside to outside traffic.

- An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.

- A DHCP server running on the inside interface.

**Note**

If you performed the (Optional) Change Management Network Settings at the CLI, on page 8 procedure, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.
Procedure

Step 1 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 Configure the following options for the outside and management interfaces and click Next.

Note 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.

a) Outside Interface—This is the data port that you connected to your gateway router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default 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. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

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.

b) 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.

Firewall Hostname—The hostname for the system's management address.

Step 3 Configure the system time settings and click Next.

a) Time Zone—Select the time zone for the system.

b) 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 4 (Optional) Configure the smart licenses for the system.

Your purchase of a Firepower Threat Defense device automatically includes a Base license. All additional licenses are optional.

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, and see Configure Licensing, on page 12.

To use the evaluation license, select Start 90 day evaluation period without registration.

Attention If you plan to onboard the device to CDO, we recommend using the evaluation license until you onboard the device. Any additional licenses you register with the Smart Software Manager will have to be unregistered before you can onboard to CDO, and then registered again; see Unregister a Smart-Licensed FTD.
Configure Licensing

The FTD uses Cisco Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally.

When you register the chassis, the License Authority issues an ID certificate for communication between the chassis and the License Authority. It also assigns the chassis to the appropriate virtual account.

The Base license is included automatically. Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

For complete information on licensing your system, see the FDM configuration guide.

**Before you begin**

- Have a master account on the Cisco Smart Software Manager.
  
  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

**Procedure**

**Step 1** Make sure your Smart Licensing account contains the available licenses you need.
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the **Cisco Commerce Workspace**. Search for the following license PIDs:

*Figure 3: License Search*

![Find Products and Solutions](image)

**Note** If a PID is not found, you can add the PID manually to your order.

- Threat, Malware, and URL license combination:
  - **Firepower 1010:**
    - L-FPR1010T-TMC=
  - **Firepower 1100:**
  - **Firepower 2100:**
  - **ASA 5508-X and 5516-X:**
  - **ISA 3000:**

When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

- **Firepower 1010:**
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y

- **Firepower 1100:**
- **Firepower 2100:**
- **ASA 5508-X and 5516-X:**
- **ISA 3000:**
  - **RA VPN**—See the **Cisco AnyConnect Ordering Guide**.

**Step 2** In the **Cisco Smart Software Manager**, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.
b) On the **General** tab, click **New Token**.

![Image of the General tab with New Token button highlighted]

- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the FTD.
Step 3 In FDM, click **Device**, and then in the **Smart License** summary, click **View Configuration**. You see the **Smart License** page.

Step 4 Click **Register Device**.

Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:
Step 5
Click Register Device.

You return to the Smart License page. While the device registers, you see the following message:

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

After the device successfully registers and you refresh the page, you see the following:

Step 6
Click the Enable/Disable control for each optional license as desired.
• **Enable** — Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.

• **Disable** — Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

• If you enabled the **RA VPN** license, select the type of license you want to use: **Plus**, **Apex**, **VPN Only**, or **Plus and Apex**.

<table>
<thead>
<tr>
<th>Type</th>
<th>Enable</th>
<th>Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN ONLY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PLUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APEX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APEX AND PLUS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:

**Device Summary**

**Smart License**

- **License Issue Out of Compliance**
  - Last sync: 10 Jul 2019 11:47 AM
  - Next sync: 10 Jul 2019 11:57 AM

There is no available license for the device. Licensed features continue to work. However, you must either purchase or free up additional licenses to be in compliance.

**Step 7**  Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.
Configure the Device in Firepower Device Manager

The following steps provide an overview of additional features you might want to configure. Please click the help button (?) on a page to get detailed information about each step.

**Procedure**

**Step 1**
If you want to convert a bridge group interface (6.4) or want to convert a switch port to a firewall interface (6.5 and later), choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon (-pencil) for each interface to set the mode and define the IP address and other settings.

The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publicly-accessible assets such as your web server. Click **Save** when you are finished.

*Figure 6: Edit Interface*

**Step 2**
If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.
The following example shows how to create a new dmz-zone for the dmz interface.

**Figure 7: Security Zone Object**

![Security Zone Object](Image)

**Step 3**  
If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device > System Settings > DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS lists supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.

**Figure 8: DHCP Server**

![DHCP Server](Image)

**Step 4**  
Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (:0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

**Note**  
The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device > System Settings > Management Interface**.
The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking Create New Network at the bottom of the Gateway drop-down list.

**Figure 2: Default Route**

---

### Step 5

Choose Policies and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following 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.

- **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.

- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting 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 blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.

- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.
• **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.

• **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.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

*Figure 10: Access Control Policy*

<table>
<thead>
<tr>
<th>Order</th>
<th>Title</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Inside_DMZ</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Step 6** Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

**Step 7** Click the **Deploy** button in the menu, then click the Deploy Now button (●), to deploy your changes to the device.

Changes are not active on the device until you deploy them.

---

**What to do next**

• You can choose to onboard the device to CDO. If so, you should register and license your device after you onboard; see **Onboard the Device to CDO**.

---

**Access the FTD and FXOS 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. You can access the CLI by connecting to the console port.

You can also access the FXOS CLI for troubleshooting purposes.
You can alternatively SSH to the Management interface of the FTD device. Unlike a console session, the SSH session defaults to the FTD CLI, from which you can connect to the FXOS CLI using the `connect fxos` command. You can later connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. This procedure describes console port access, which defaults to the FXOS CLI.

**Procedure**

**Step 1**
To log into the CLI, connect your management computer to the console port. The Firepower 1000 ships with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1010 hardware guide). The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the `admin` username and the password you set at initial setup (the default is `Admin123`).

*Example:*

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin': 1

firepower#
```

**Step 2**
Access the FTD CLI.

`connect ftd`

*Example:*

```
firepower# connect ftd
>
```

After logging in, for information on the commands available in the CLI, enter `help` or `?`. For usage information, see the *Cisco Firepower Threat Defense Command Reference*.

**Step 3**
To exit the FTD CLI, enter the `exit` or `logout` command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter `?`.

*Example:*
View Hardware Information

Use the command-line interface (CLI) to view information about your hardware, including the device model, hardware version, serial number, and chassis components including power supplies and network modules. You can access the CLI by connecting to the console port; see Access the FTD and FXOS CLI, on page 21.

Procedure

Step 1  To display the hardware model of the device, use the `show model` command.

`> show model`

Example:

`> show model`
Cisco Firepower 1010 Threat Defense

Step 2  To display the chassis serial number, use the `show serial-number` command.

`> show serial-number`

Example:

`> show serial-number`
JMX1943408S

This information is also shown in `show version system`, `show running-config`, and `show inventory` output.

Step 3  To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the `show inventory` command.

`> show inventory`

a) From the FTD CLI:

Example:

`> show inventory`
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010 , VID: V00 , SN: JMX1943408S

b) From the FXOS CLI:

Example:

`firepower /chassis # show inventory`
Chassis PID Vendor Serial (SN) HW Revision
Power Off the Device

It's important that you shut down your system properly. Simply unplugging the power can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your Firepower system.

The Firepower 1010 chassis does not have an external power switch. You can power off the device using FDM, or you can use the FXOS CLI.

Power Off the Device Using FDM

You can shut down your system properly using FDM.

**Procedure**

**Step 1**
(6.5 and later) Use FDM to shut down the device.

**Note** For 6.4 and earlier, enter the `shutdown` command at the FDM CLI.

a) Click **Device**, then click the **System Settings > Reboot/Shutdown** link.
b) Click **Shut Down**.

**Step 2**
Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

**Step 3**
After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

Power Off the Device at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the FTD and FXOS CLI, on page 21.

**Procedure**

**Step 1**
In the FXOS CLI, connect to local-mgmt:

`firepower # connect local-mgmt`

**Step 2**
Issue the shutdown command:

`firepower(local-mgmt) # shutdown`

**Example:**
firepower(local-mgmt)# shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok

**Step 3** Monitor the system prompts as the device shuts down.

**Step 4** Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

**Step 5** After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

---

**What's Next?**

To continue configuring your FTD device, see the documents available for your software version at *Navigating the Cisco Firepower Documentation*.

For information related to using FDM, see *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*. 