Which Operating System and Manager is Right for You?

Your hardware platform can run one of two operating systems. For each operating system, you have a choice of managers. This chapter explains the operating system and manager choices.

- Operating Systems, on page 1
- Managers, on page 1

Operating Systems

You can use either ASA or Firepower Threat Defense (FTD) operating systems on your hardware platform:

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.
  
  You may want to use the ASA if you do not need the advanced capabilities of the FTD, or if you need an ASA-only feature that is not yet available on the FTD. Cisco provides ASA-to-FTD migration tools to help you convert your ASA to an FTD if you start with ASA and later reimage to FTD.

- FTD—FTD, also known as Firepower NGFW, is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the FTD takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

  We recommend using the FTD over the ASA because it contains most of the major functionality of the ASA, plus additional next generation firewall and IPS functionality.

To reimage between the ASA and the FTD, see Reimage the Cisco ASA or Firepower Threat Defense Device.

Managers

The FTD and ASA support multiple managers.
## FTD Managers

**Table 1: FTD Managers**

<table>
<thead>
<tr>
<th>Manager</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Device Manager (FDM)</td>
<td>FDM is a web-based, simplified, on-device manager. Because it is simplified, some FTD features are not supported using FDM. You should use FDM if you are only managing a small number of devices and don't need a multi-device manager.</td>
<td>Both FDM and CDO can discover the configuration on the device, so you can use FDM and CDO to manage the same device. FMC is not compatible with other managers.</td>
</tr>
<tr>
<td>Cisco Defense Orchestrator (CDO)</td>
<td>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some FTD features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience (similar to FDM). And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as ASAs, so you can use a single manager for all of your security devices.</td>
<td>Both FDM and CDO can discover the configuration on the device, so you can use FDM and CDO to manage the same device. FMC is not compatible with other managers.</td>
</tr>
<tr>
<td>Firepower Management Center (FMC)</td>
<td>FMC is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use FMC if you want a multi-device manager, and you require all features on the FTD. FMC also provides powerful analysis and monitoring of traffic and events.</td>
<td>FMC is not compatible with other managers because the FMC owns the FTD configuration, and you are not allowed to configure the FTD directly, bypassing the FMC.</td>
</tr>
<tr>
<td>FTD REST API</td>
<td>The FTD REST API lets you automate direct configuration of the FTD. This API is compatible with FDM and CDO use because they can both discover the configuration on the device. You cannot use this API if you are managing the FTD using FMC. The FTD REST API is not covered in this guide. For more information, see the FTD REST API guide.</td>
<td></td>
</tr>
<tr>
<td>FMC REST API</td>
<td>The FMC REST API lets you automate configuration of FMC policies that can then be applied to managed FTDs. This API does not manage an FTD directly. The FMC REST API is not covered in this guide. For more information, see the FMC REST API guide.</td>
<td></td>
</tr>
</tbody>
</table>
# ASA Managers

## Table 2: ASA Managers

<table>
<thead>
<tr>
<th>Manager</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Security Device Manager (ASDM)</td>
<td>ASDM is a Java-based, on-device manager that provides full ASA functionality. You should use ASDM if you prefer using a GUI over the CLI, and you only need to manage a small number of ASAs. ASDM can discover the configuration on the device, so you can also use the CLI, CDO, or CSM with ASDM. To get started with ASDM, see <a href="#">ASA and ASA FirePOWER Module Deployment with ASDM, on page 61</a>.</td>
</tr>
<tr>
<td>CLI</td>
<td>You should use the ASA CLI if you prefer CLIs over GUIs. The CLI is not covered in this guide. For more information, see the <a href="#">ASA configuration guides</a>.</td>
</tr>
<tr>
<td>Cisco Defense Orchestrator (CDO)</td>
<td>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some ASA features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience. And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as FTDs, so you can use a single manager for all of your security devices. CDO can discover the configuration on the device, so you can also use the CLI or ASDM. CDO is not covered in this guide. To get started with CDO, see the <a href="#">CDO home page</a>.</td>
</tr>
<tr>
<td>Cisco Security Manager (CSM)</td>
<td>CSM is a powerful, multi-device manager that runs on its own server hardware. You should use CSM if you need to manage large numbers of ASAs. CSM can discover the configuration on the device, so you can also use the CLI or ASDM. CSM does not support managing FTDs. CSM is not covered in this guide. For more information, see the <a href="#">CSM user guide</a>.</td>
</tr>
<tr>
<td>ASA REST API</td>
<td>The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced. The ASA REST API is not covered in this guide. For more information, see the <a href="#">ASA REST API guide</a>.</td>
</tr>
</tbody>
</table>
CHAPTER 2

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 ISA 3000 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

Privacy Collection Statement — The Firepower 1100 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 6
• Review the Network Deployment and Default Configuration, on page 7
• Cable the Device (6.5 and Later), on page 10
• Cable the Device (6.4 and Earlier), on page 11
• Power on the Device, on page 12
• (Optional) Change Management Network Settings at the CLI, on page 13
• Log Into FDM, on page 14
• Complete the Initial Configuration (6.5 and Later), on page 15
• Complete the Initial Configuration (6.4 and Earlier), on page 19
• Configure Licensing, on page 20
• Configure the Device in Firepower Device Manager (6.5 and Later), on page 26
• Configure the Device in Firepower Device Manager (6.4 and Earlier), on page 28
• Access the Firepower Threat Defense CLI, on page 31
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

- Power Off the Device, on page 32
- What's Next?, on page 33
<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Pre-Configuration</td>
</tr>
<tr>
<td>4</td>
<td>FTD CLI (Optional) Change Management Network Settings at the CLI, on page 13.</td>
</tr>
<tr>
<td>5</td>
<td>Firepower Device Manager Log Into FDM, on page 14.</td>
</tr>
</tbody>
</table>
| 6    | Firepower Device Manager • Complete the Initial Configuration (6.5 and Later), on page 15  
|      |               • Complete the Initial Configuration (6.4 and Earlier), on page 19. |
| 7    | Cisco Commerce Workspace Configure Licensing, on page 20: Obtain license features. |
| 8    | Smart Software Manager Configure Licensing, on page 20: Generate a license token. |
| 9    | Firepower Device Manager Configure Licensing, on page 20: Register the device with the Smart Licensing Server. |
| 10   | Firepower Device Manager • Configure the Device in Firepower Device Manager (6.5 and Later), on page 26  
|      |               • Configure the Device in Firepower Device Manager (6.4 and Earlier), on page 28. |

**Review the Network Deployment and Default Configuration**

The following figures show the suggested network deployment for the ISA 3000 for version 6.5 and later, and for version 6.4 and earlier. The default configuration changed in version 6.5.

**Note**

If cannot use the default Management IP address (for example, you are adding your device to an existing network), 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 13.
Default Configuration (6.5 and Later)

The configuration for the ISA 3000, which is a special default configuration applied before shipping, includes the following:
• **BVI 1**—All member interfaces are in the same network (IP address not pre-configured; you must set to match your network): GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (outside2), GigabitEthernet 1/4 (inside2)

• **inside**→**outside** traffic flow. All interfaces can communicate with each other.

• **management**—Management 1/1 (management), IP address 192.168.45.45

  **Note** The Management 1/1 interface is shared between the Management logical interface and the Diagnostic logical interface; see the FDM configuration guide for more information.

• **DNS server for management**—OpenDNS: 208.67.222.222, 208.67.220.220

• **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org

• **Default routes**
  - **Management interface**—Through the Management interface to 192.168.45.1.
  - **Data interfaces**—None.

• **FDM access**—Management hosts allowed

• **Hardware bypass**—Enabled for the following interface pairs: GigabitEthernet 1/1 & 1/2; GigabitEthernet 1/3 & 1/4

  **Note** When the ISA 3000 loses power and goes into hardware bypass mode, only the above interface pairs can communicate; inside1 and inside2, and outside1 and outside2 can no longer communicate. Any existing connections between these interfaces will be lost. When the power comes back on, there is a brief connection interruption as the FTD takes over the flows.

### Default Configuration (6.4 and Earlier)

The configuration for the ISA 3000 after initial setup includes the following:

• **inside**—GigabitEthernet 1/2 through 1/4 belong to bridge group interface (BVI) 1, IP address 192.168.1.1

• **outside**—GigabitEthernet 1/1, IP address from DHCP or an address you specify during setup

• **inside**→**outside** traffic flow

• **management**—Management 1/1 (management), IP address 192.168.45.45

  **Note** The Management 1/1 interface is shared between the Management logical interface and the Diagnostic logical interface; 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

- **NTP**—Cisco NTP servers: 0.sourceforge.pool.ntp.org, 1.sourceforge.pool.ntp.org, 2.sourceforge.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**—Over the backplane and through the data interfaces. The FTD requires internet access for licensing and updates.

- **DHCP server** on inside interface, management interface

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

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

---

**Cable the Device (6.5 and Later)**

Manage the ISA 3000 on the Management 1/1 interface.
Procedure

Step 1  Connect GigabitEthernet 1/1 to an outside router, and GigabitEthernet 1/2 to an inside router. These interfaces form a hardware bypass pair.

Step 2  Connect GigabitEthernet 1/3 to a redundant outside router, and GigabitEthernet 1/4 to a redundant inside router. These interfaces form a hardware bypass pair. These interfaces provide a redundant network path if the other pair fails. All 4 of these data interfaces are on the same network of your choice. You will need to configure the BVI 1 IP address to be on the same network as the inside and outside routers.

Step 3  Connect Management 1/1 to your management PC (or network).

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 (cabling not shown). See (Optional) Change Management Network Settings at the CLI, on page 13.

Cable the Device (6.4 and Earlier)

Manage the ISA 3000 on either Management 1/1 or GigabitEthernet 1/2 through 1/4. The default configuration also configures GigabitEthernet1/1 as outside.
Procedure

Step 1 Connect your management computer to one of the following interfaces:

• GigabitEthernet 1/2 through 1/4—Connect your management computer directly to one of the inside ports (Ethernet 1/2 through 1/4). 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 (6.4 and Earlier), on page 9).

• Management 1/1—Connect your management computer directly to Management 1/1. 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 management network settings (see Default Configuration (6.4 and Earlier), on page 9).

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 (cabling not shown). See (Optional) Change Management Network Settings at the CLI, on page 13.

Step 2 Connect the outside network to the GigabitEthernet 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 ports, GigabitEthernet 1/2 through 1/8.

Power on the Device

System power is controlled by DC power; there is no power button.

Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). 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 plug to the ISA 3000 after wiring it to the DC power source.
Refer to “Connecting to DC Power” in the hardware installation guide for instructions on proper wiring of the power plug.

Step 2 Check the System LED on the front panel of the ISA 3000 device; if it is steady green, the device is powered on. If it is flashing green, the device is in Boot up phase and POST.
Refer to “Verifying Connections” in the hardware installation guide to verify that all devices are properly connected to the ISA 3000.

(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 configure later in 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 Firepower Threat Defense CLI, on page 31 for more information.

Log in with the admin user and the default password, Admin123.

Step 2
The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. 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 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 change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
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.
For HTTP Proxy configuration, run 'configure network http-proxy'
Manage the device locally? (yes/no) [yes]: yes

> 

Step 3 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.

• Management—https://192.168.45.45. If you changed the Management IP address at the CLI setup, then enter that address.

• (6.4 and earlier only) Inside—https://192.168.1.1. You can connect to the inside address on any inside BVI interfaces (Ethernet1/2 through 1/4). For 6.5 and later, the default configuration does not pre-configure management on data interfaces.

Step 2 Log in with the username admin, and the default password Admin123.
What to do next

- For 6.4 and earlier: Run through the FDM setup wizard; see Complete the Initial Configuration (6.4 and Earlier), on page 19. For 6.5 and later: The ISA 3000 does not support the setup wizard; a special default configuration is applied before shipping. To manually set up the FTD, see Complete the Initial Configuration (6.5 and Later), on page 15.

Complete the Initial Configuration (6.5 and Later)

This section describes how to configure the following important settings:

- **BVI 1 IP address**—You must set the BVI 1 IP address for traffic to flow between the bridge group member interfaces.

- **Default route for traffic originating on the device**—All interfaces are part of a bridge group, which use MAC address lookups for traffic forwarding. However, for traffic originating on the device, you need a default route. If you change the management gateway to the data interfaces, then this route is used for management interface traffic as well.

Procedure

**Step 1**

If you did not use the CLI setup script ((Optional) Change Management Network Settings at the CLI, on page 13), and this connection is your first connection, then you are prompted to:

- Read and accept the End User License Agreement.
- Change the admin password.
- Accept the 90-day evaluation license

**Step 2**

Set the BVI 1 IP address.

You must set the BVI 1 IP address for traffic to flow between the bridge group member interfaces.

a) On the **Device** page, click the link in the **Interfaces** summary, then click **Bridge Groups**.

b) Click the edit icon (-pencil) for the BVI1 bridge group.

c) Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **Static**—Choose this option if you want to assign an address that should not change. Type in the bridge group's IP address and the subnet mask. All attached endpoints will be on this network. Ensure that the address is not already used on the network.

  If you configured High Availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

- **DHCP**—Choose this option if the address should be obtained from the DHCP server on the network. This is not the typical option for bridge groups, but you can configure it if needed. You cannot use this option if you configure high availability. Change the following options if necessary:
Obtain Default Route Using DHCP—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.

d) Click the IPv6 Address tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the slider so it is enabled ( ). The link local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48.

- **Suppress RA**—Whether to suppress router advertisements. The FTD can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

  You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

- **Standby IP Address**—If you configure High Availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

e) Click OK.

**Step 3**

Set the default route for traffic originating on the device.

All interfaces are part of a bridge group, which use MAC address lookups for traffic forwarding. However, for traffic originating on the device, you need a default route. If you keep the management gateway as the data interfaces (the default), then this route is used for management interface traffic as well.

a) Click Device, then click the link in the Routing summary.

  The Static Routing page appears.

b) Click + or Create Static Route.

c) Configure the default route properties.
1. Enter a Name, for example, default.

2. Click either the IPv4 or IPv6 radio button.
   You need to create separate default routes for IPv4 and IPv6.

3. Click Gateway, and then click Create New Network to add the gateway IP address as a host object. Click OK to add the object.
4. For the **Interface**, choose BVI1.

5. Click the **Networks** icon, and choose **any-ipv4** for an IPv4 default route or **any-ipv6** for an IPv6 default route.

d) Click **OK**.
e) Click **OK**.

**Step 4**
If you did not set a new Management IP address and gateway using *(Optional) Change Management Network Settings at the CLI*, on page 13, then you can change the IP address and gateway on the **Device > System Settings > Management Interface** page. You will have to reconnect to the new address with your browser.

**Step 5**
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 Pending Changes window shows a comparison of the deployed version of the configuration with the pending changes. These changes are color-coded to indicate removed, added, or edited elements. See the legend in the window for an explanation of the colors.

**Step 6**
If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately.

The window will show that the deployment is in progress. You can close the window, or wait for deployment to complete. If you close the window while deployment is in progress, the job does not stop. You can see results in the task list or audit log. If you leave the window open, click the **Deployment History** link to view the results.
What to do next

- Although you can continue using the evaluation license, we recommend that you register and license your device; see Configure Licensing, on page 20.
- You can also choose to configure the device; see Configure the Device in Firepower Device Manager (6.5 and Later), on page 26.

Complete the Initial Configuration (6.4 and Earlier)

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 (GigabitEthernet1/1) and an inside interface. GigabitEthernet1/2 through 1/4 are inside bridge group members.
- 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 13 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. 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 20.

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

Step 5 Click Finish.

What to do next

• Although you can continue using the evaluation license, we recommend that you register and license your device; see Configure Licensing, on page 20.

• You can also choose to configure the device using FDM; see Configure the Device in Firepower Device Manager (6.4 and Earlier), on page 28.

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, but you should purchase the following optional feature licenses to be in compliance:

• 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.

In addition to the above licenses, you also need to buy a matching subscription to access updates for 1, 3, or 5 years.

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.

**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**.

![Cisco Software Central > Smart Software Licensing](image)

**Smart Software Licensing**

[Alerts | License Conversion | Reports | Email Notification | Satellites | Activity]

b) On the **General** tab, click **New Token**.
c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

- **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**.

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:

**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 (6.5 and Later)

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, choose Device, and then click the link in the Interfaces summary.

Click the edit icon (🚀) 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 5: Edit Interface

Step 2  Choose Policies and configure the security policies for the network.

By default, all traffic is allowed between all interfaces. If you add other security zones, you need rules to allow traffic to and from those zones. In addition, you can configure other policies to provide additional
services, and fine-tune 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 routable 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 6: 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 3** 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 4  
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.

---

**Configure the Device in Firepower Device Manager (6.4 and Earlier)**

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, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon (🛈) 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 7: 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 8: Security Zone Object*

---

### 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 9: DHCP Server*

---

### 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 10: 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 11: Access Control Policy*

**Add 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>

<table>
<thead>
<tr>
<th>Source/Destination</th>
<th>Applications</th>
<th>URLs</th>
<th>Users</th>
<th>Intrusion Policy</th>
<th>File Policy</th>
<th>Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOURCE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inside_zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DESTINATION</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmz_zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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.

---

**Access the Firepower Threat Defense 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 SSH to the management interface of the FTD device. You can also 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.
Procedure

Step 1  To log into the CLI, connect your management computer to the console port. See the hardware guide for your device for more information about the console cable. Use the following serial settings:

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

Step 2  Log into the FTD CLI using the admin username and the password you set at initial setup (the default is Admin123).

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.

Power Off the Device

It's important that you shut down your system properly using FDM. 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 ISA 3000 chassis does not have an external power switch.

Procedure

Step 1  Connect to the console port to access the FTD CLI, and then shut down the FTD.

shutdown

Example:

> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd...          [ OK ]
Clearing static routes
Unconfiguring default route      [ OK ]
Unconfiguring address on br1    [ OK ]
Unconfiguring IPv6              [ OK ]
 Downing interface              [ OK ]
Stopping xinetd:
Stopping nscd...               [ OK ]
Stopping system log daemon...   [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]

mdadm: Cannot get exclusive access to /dev/md0: Perhaps a running process, mounted filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
o /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]

**Step 2**

After the FTD shuts down, and the console shows that "It is safe to power off now", you can then unplug the power to physically remove power from the chassis if necessary.

Alternatively, you can reboot the system by typing y at the prompt.

---

**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.
CHAPTER 3

Firepower Threat Defense Deployment with FMC

Is This Chapter for You?

This chapter explains how to complete the initial configuration of your Firepower Threat Defense (FTD) and how to register the device to a Firepower Management Center (FMC). In a typical deployment on a large network, multiple managed devices are installed on network segments, monitor traffic for analysis, and report to a managing FMC, which provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks.

For networks that include only a single device or just a few, where you do not need to use a high-powered multiple-device manager like the FMC, you can use the integrated Firepower Device Manager (FDM). Use the FDM web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

Note: The Cisco ISA 3000 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: Privacy Collection Statement—The ISA 3000 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.

- Before You Start, on page 36
- End-to-End Procedure, on page 36
- Review the Network Deployment, on page 37
- Cable the Device, on page 39
- Power on the Device, on page 41
- Complete the FTD Initial Configuration, on page 42
- Log Into the Firepower Management Center, on page 45
- Obtain Licenses for the Firepower Management Center, on page 45
- Register the FTD with the FMC, on page 46
- Configure a Basic Security Policy, on page 48
- Access the Firepower Threat Defense CLI, on page 58
- Power Off the Device, on page 59
Before You Start

Deploy and perform initial configuration of the FMC. See the FMC getting started guide.

Note

The Firepower device and the FMC both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup. Note that the FMC on 6.5 and later defaults to a DHCP client for the management interface; however, if there is no DHCP server, it will default to 192.168.45.45.

End-to-End Procedure

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

1. Review the network and deployment guidelines
2. Cable the device
3. Power on the device
4. Configure the device for management
5. Log into the FMC
6. Generate a license token for the FMC
7. Register the FMC with the Smart Licensing Server
8. Register the FTD with the FMC
9. Configure a basic security policy

Review the Network Deployment, on page 37.
Review the Network Deployment

By default, only the Management 1/1 interface is enabled and configured with an IP address (192.168.45.45). This interface also runs a DHCP server initially; after you select FMC as the manager during initial setup, the DHCP server is disabled. You can configure other interfaces after you connect the FTD to FMC.

See the following sample network deployments for ideas on how to place your FTD device in your network.

**Separate Management Network**

The FMC can only communicate with the FTD on the management interface. Both the FMC and FTD require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ISA 3000 where the FMC and management computer connect to the management network. The management network has a path to the internet for licensing and updates.
**Edge Network Deployment**

The FMC can only communicate with the FTD on the management interface. Moreover, both the FMC and FTD require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ISA 3000 where the ISA 3000 acts as the internet gateway for the FMC and FTD management.

In the following diagram, the ISA 3000 acts as the internet gateway for the management interface and the FMC by connecting Management 1/1 to an inside interface through a Layer 2 switch, and by connecting the FMC and management computer to the switch. (This direct connection is allowed because the management interface is separate from the other interfaces on the FTD.)
Cable the Device

To cable one of the recommended scenarios on the ISA 3000, see the following steps.

**Note**
The ISA 3000 and the FMC both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup. Note that the FMC on 6.5 and later defaults to a DHCP client for the management interface; however, if there is no DHCP server, it will default to 192.168.45.45.

**Note**
Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

**Procedure**

**Step 1**
Cable for a separate management network.
a) Cable the following to your management network:
   - Management 1/1 interface
   - Firepower Management Center
   - Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

c) Connect the inside interface (for example, GigabitEthernet 1/2) to your inside router.

d) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.

e) Connect other networks to the remaining interfaces.

**Step 2** Cable for an edge deployment.
a) Cable the following to a Layer 2 Ethernet switch:
   • Inside interface (for example, GigabitEthernet 1/2)
   • Management 1/1 interface
   • Firepower Management Center
   • Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.

d) Connect other networks to the remaining interfaces.

---

**Power on the Device**

System power is controlled by DC power; there is no power button.
Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). 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 plug to the ISA 3000 after wiring it to the DC power source.

Refer to “Connecting to DC Power” in the hardware installation guide for instructions on proper wiring of the power plug.

**Step 2**
Check the System LED on the front panel of the ISA 3000 device; if it is steady green, the device is powered on. If it is flashing green, the device is in Boot up phase and POST.

Refer to “Verifying Connections” in the hardware installation guide to verify that all devices are properly connected to the ISA 3000.

Complete the FTD Initial Configuration

Connect to the FTD CLI to perform initial setup, including setting the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. You will also configure FMC communication settings. You can only configure the Management interface settings; you must configure data interface settings in FMC.

Procedure

**Step 1**
Connect to the FTD CLI, either from the console port or using SSH to the Management interface. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

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

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

Note You cannot repeat the CLI setup wizard 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.

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**—The data-interfaces setting applies only to Firepower Device Manager management; you should set a gateway IP address for Management 1/1 when using FMC. In the edge deployment example shown in the network deployment section, the inside interface acts as the management gateway. In this case, you should set the gateway IP address to be the intended inside interface IP address; you must later use FMC to set the inside IP address.
• If your networking information has changed, you will need to reconnect—If you are connected with SSH 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 no to use FMC. A yes answer means you will use Firepower Device Manager instead. Note also that the DHCP server on Management 1/1 will be disabled if it wasn't already.

• Configure firewall mode?—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration.

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 change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
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]: no
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

Step 4

Identify the FMC that will manage this FTD.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}`—Specifies either the FQDN or IP address of the FMC. If the FMC is not directly addressable, use DONTRESOLVE and also specify the `nat_id`. At least one of the devices, either the FMC or the FTD, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you specify DONTRESOLVE in this command, then the FTD must have a reachable IP address or hostname.

- `reg_key`—Specifies a one-time registration key of your choice that you will also specify on the FMC when you register the FTD. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

- `nat_id`—Specifies a unique, one-time string of your choice that you will also specify on the FMC when you register the FTD when one side does not specify a reachable IP address or hostname. It is required if you set the FMC to DONTRESOLVE. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the FMC.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

What to do next

Register your device to a FMC.
Log Into the Firepower Management Center

Use the FMC to configure and monitor the FTD.

**Before you begin**
For information on supported browsers, refer to the release notes for the version you are using (see https://www.cisco.com/go/firepower-notes).

**Procedure**

**Step 1**
Using a supported browser, enter the following URL.
https://fmc_ip_address

**Step 2**
Enter your username and password.

**Step 3**
Click Log In.

Obtain Licenses for the Firepower Management Center

All licenses are supplied to the FTD by the FMC. You can optionally purchase the following feature 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.

**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:
Register the FTD with the FMC

Before you begin

- Gather the following information that you set in the FTD initial configuration:
  - FTD management IP address or hostname, and NAT ID, if configured
  - FMC registration key

Procedure

Step 1  In FMC, choose **Devices > Device Management.**

Step 2  From the **Add** drop-down list, choose **Add Device**, and enter the following parameters.

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

- Threat, Malware, and URL license combination:
  - L-ISA3000T-TMC=

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:

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- RA VPN—See the [Cisco AnyConnect Ordering Guide](#).

Step 2  If you have not already done so, register the FMC with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the [FMC configuration guide](#) for detailed instructions.
• **Host**—Enter the IP address or hostname of the FTD you want to add. You can leave this field blank if you specified both the FMC IP address and a NAT ID in the FTD initial configuration.

• **Display Name**—Enter the name for the FTD as you want it to display in the FMC.

• **Registration Key**—Enter the same registration key that you specified in the FTD initial configuration.

• **Domain**—Assign the device to a leaf domain if you have a multidomain environment.

• **Group**—Assign it to a device group if you are using groups.

• **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see **Allow Traffic from Inside to Outside, on page 56**.

• **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use AMP malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering). **Note:** You can apply an AnyConnect

---

**New Policy**

- **Name**: ftd_ac_policy
- **Description**:
- **Select Base Policy**: None
- **Default Action**: **Block all traffic**

---

**Register the FTD with the FMC**
remote access VPN license after you add the device, from the System > Licenses > Smart Licenses page.

- **Unique NAT ID**—Specify the NAT ID if you specified it in the FTD initial configuration.
- **Transfer Packets**—Allow the device to transfer packets to the FMC. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC, but packet data is not sent.

**Step 3**

Click Register, and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the FTD fails to register, check the following items:

- **Ping**—Access the FTD CLI, and ping the FMC IP address using the following command:
  
  ```
  ping system ip_address
  ```

  If the ping is not successful, check your network settings using the `show network` command. If you need to change the FTD IP address, use the `configure network {ipv4 | ipv6} manual` command.

- **Registration key, NAT ID, and FMC IP address**—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the FTD using the `configure manager add` command.

For more troubleshooting information, see [https://cisco.com/go/fmc-reg-error](https://cisco.com/go/fmc-reg-error).

## Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- **Inside and outside interfaces**—Assign a static IP address to the inside interface, and use DHCP for the outside interface.

- **DHCP server**—Use a DHCP server on the inside interface for clients.

- **Default route**—Add a default route through the outside interface.

- **NAT**—Use interface PAT on the outside interface.

- **Access control**—Allow traffic from inside to outside.

To configure a basic security policy, complete the following tasks.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure Interfaces, on page 49.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the DHCP Server, on page 52.</td>
</tr>
<tr>
<td>3</td>
<td>Add the Default Route, on page 53.</td>
</tr>
</tbody>
</table>
Configure Interfaces

Enable FTD interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization’s networks. Some of these interfaces might be “demilitarized zones” (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

**Procedure**

**Step 1** Choose Devices > Device Management, and click the Edit (щей) for the device.

**Step 2** Click Interfaces.

**Step 3** Click the Edit (шей) for the interface that you want to use for inside.

The General tab appears.
a) Enter a **Name** up to 48 characters in length.
   For example, name the interface **inside**.

b) Check the **Enabled** check box.

c) Leave the **Mode** set to **None**.

d) From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**.

   For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

e) Click the **IPv4** and/or **IPv6** tab.

   - **IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

      For example, enter **192.168.1.1/24**
f) Click OK.

**Step 4**

Click the Edit (✍️) for the interface that you want to use for outside.

The General tab appears.

<table>
<thead>
<tr>
<th>General</th>
<th>IPv4</th>
<th>IPv6</th>
<th>Advanced</th>
<th>Hardware Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>outside</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Zone:</td>
<td>outside_zone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface ID:</td>
<td>GigabitEthernet0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU:</td>
<td>1500</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a) Enter a Name up to 48 characters in length.  
For example, name the interface outside.

b) Check the Enabled check box.

c) Leave the Mode set to None.

d) From the Security Zone drop-down list, choose an existing outside security zone or add a new one by clicking New.

For example, add a zone called outside_zone.

e) Click the IPv4 and/or IPv6 tab.

• IPv4—Choose Use DHCP, and configure the following optional parameters:
  • Obtain default route using DHCP—Obtains the default route from the DHCP server.
  • DHCP route metric—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.
Configure the DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTD.

**Procedure**

1. **Step 1** Choose Devices > Device Management, and click the Edit (.edit) for the device.
2. **Step 2** Choose DHCP > DHCP Server.
3. **Step 3** On the Server page, click Add, and configure the following options:

   - **Interface**—Choose the interface from the drop-down list.
   - **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
   - **Enable DHCP Server**—Enable the DHCP server on the selected interface.

4. **Step 4** Click OK.
5. **Step 5** Click Save.
Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the IPv4 Routes or IPv6 Routes table on the Devices > Device Management > Routing > Static Route page.

Procedure

Step 1  Choose Devices > Device Management, and click the Edit ( ) for the device.

Step 2  Choose Routing > Static Route, click Add Route, and set the following:

- **Type**—Click the IPv4 or IPv6 radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
- **Available Network**—Choose any-ipv4 for an IPv4 default route, or any-ipv6 for an IPv6 default route and click Add to move it to the Selected Network list.
- **Gateway** or IPv6 Gateway—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.
- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

Step 3  Click OK.
The route is added to the static route table.

---

**Step 4**  
Click **Save**.

---

**Configure NAT**

A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

**Procedure**

1. **Step 1**  
   Choose **Devices > NAT**, and click **New Policy > Threat Defense NAT**.

2. **Step 2**  
   Name the policy, select the device(s) that you want to use the policy, and click **Save**.
The policy is added the FMC. You still have to add rules to the policy.

**Step 3** Click Add Rule.

The Add NAT Rule dialog box appears.

**Step 4** Configure the basic rule options:

- **NAT Rule**—Choose Auto NAT Rule.
- **Type**—Choose Dynamic.

**Step 5** On the Interface Objects page, add the outside zone from the Available Interface Objects area to the Destination Interface Objects area.

**Step 6** On the Translation page, configure the following options:
• **Original Source**—Click **Add** to add a network object for all IPv4 traffic (0.0.0.0/0).

![New Network Object](image)

- **Name**: all-ipv4
- **Description**: 
- **Network**: [Network] 0.0.0.0/0
- **Allow Overides**: [Check Box]

**Note**: You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

• **Translated Source**—Choose **Destination Interface IP**.

**Step 7** Click **Save** to add the rule.

The rule is saved to the **Rules** table.

**Step 8** Click **Save** on the NAT page to save your changes.

---

### Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

See the **FMC configuration guide** to configure more advanced security settings and rules.
Procedure

**Step 1** Choose **Policy > Access Policy > Access Policy**, and click the **Edit** (руш) for the access control policy assigned to the FTD.

**Step 2** Click **Add Rule**, and set the following parameters:

- **Name**—Name this rule, for example, **inside_to_outside**.
- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.
- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.

Leave the other settings as is.

**Step 3** Click **Add**.

The rule is added to the **Rules** table.

**Step 4** Click **Save**.

**Deploy the Configuration**

Deploy the configuration changes to the FTD; none of your changes are active on the device until you deploy them.
Access the Firepower Threat Defense 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 SSH to the management interface of the FTD device. You can also 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.

Procedure

Step 1  To log into the CLI, connect your management computer to the console port. See the hardware guide for your device for more information about the console cable. Use the following serial settings:

- 9600 baud
- 8 data bits
Power Off the Device

It's important that you shut down your system properly using FDM. 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 ISA 3000 chassis does not have an external power switch.

Procedure

Step 1
Connect to the console port to access the FTD CLI, and then shut down the FTD.

shutdown

Example:

> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nscd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus.
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0: Perhaps a running process, mounted filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
Acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]

Step 2

After the FTD shuts down, and the console shows that "It is safe to power off now", you can then unplug the power to physically remove power from the chassis if necessary.

Alternatively, you can reboot the system by typing y at the prompt.

What's Next?

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

For information related to using FMC, see the Firepower Management Center Configuration Guide.
ASA and ASA FirePOWER Module Deployment with ASDM

Is This Chapter for You?

The Cisco ISA 3000 is a powerful, rack-mountable, hardened firewall. This chapter describes how to deploy the ISA 3000 ASA in your network with the ASA FirePOWER module and how to perform initial configuration. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

- Failover
- CLI configuration

This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

Note

The ISA 3000 hardware can run either ASA software or FTD software. Switching between ASA and FTD requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Note

Privacy Collection Statement—The ISA 3000 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.

- About the ASA, on page 62
- End-to-End Procedure, on page 62
- Review the Network Deployment and Default Configuration, on page 64
- Cable the Device, on page 67
- Power on the Device, on page 68
- (Optional) Change the IP Address, on page 68
- Log Into ASDM, on page 69
- (Optional) Configure ASA Licensing, on page 70
- Configure the ASA, on page 71
About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device, and with the included ASA FirePOWER module, next-generation firewall services including Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the ASA using one of the following managers:

- ASDM (Covered in this guide)—A single device manager included on the device.
- CLI
- Cisco Security Manager—A multi-device manager on a separate server.

You can manage the ASA FirePOWER module using one of the following managers:

- ASDM (Covered in this guide)—A single device manager included on the device.
- Firepower Management Center (FMC)—A full-featured, multidevice manager on a separate server.

You can also access the FirePOWER CLI for troubleshooting purposes.

End-to-End Procedure

See the following tasks to deploy and configure the ASA on your chassis.
Pre-Configuration 1. Review the network and default configuration, on page 64.

Pre-Configuration 2. Cable the device, on page 67.

Pre-Configuration 3. Power on the device, on page 68.

Pre-Configuration 4. (Optional) Change the IP address, on page 68.

ASA CLI 5. Log into ASDM, on page 69.

ASDM 6. (Optional) View the serial number, on page 69.

ASDM 7. (Optional) Obtain feature licenses, on page 69.

ASDM 8. (Optional) Obtain the activation key, on page 69.

ASDM 9. (Optional) Apply the activation key to the device, on page 69.

ASDM 10. Configure the ASA, on page 69.

ASDM 11. Configure the ASA FirePOWER Module, on page 69.
Review the Network Deployment and Default Configuration

The following figure shows the recommended network deployment for the ISA 3000 with the ASA FirePOWER module. The ASA FirePOWER module needs internet access from the Management 1/1 interface for database updates, so be sure the management network can reach the internet.

Note

If you cannot use the default Management IP address for ASDM access, you can set the Management IP address at the ASA CLI. See (Optional) Change the IP Address, on page 68.

Figure 17: ISA 3000 Network

---

ASA and ASA FirePOWER Module Deployment with ASDM

<table>
<thead>
<tr>
<th></th>
<th>ASDM</th>
<th>(Optional) Configure ASA Licensing, on page 70: View the serial number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Cisco Commerce Workspace</td>
<td>(Optional) Configure ASA Licensing, on page 70: Obtain feature licenses.</td>
</tr>
<tr>
<td>8</td>
<td>Smart Software Manager</td>
<td>(Optional) Configure ASA Licensing, on page 70: Obtain the activation key.</td>
</tr>
<tr>
<td>9</td>
<td>ASDM</td>
<td>(Optional) Configure ASA Licensing, on page 70: Apply the activation key to the device.</td>
</tr>
<tr>
<td>10</td>
<td>ASDM</td>
<td>Configure the ASA, on page 71.</td>
</tr>
<tr>
<td>11</td>
<td>ASDM</td>
<td>Configure the ASA FirePOWER Module, on page 74.</td>
</tr>
</tbody>
</table>
ISA 3000 Default Configuration

The default factory configuration for the ISA 3000 configures the following:

- **Transparent firewall mode**—A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

- **1 Bridge Virtual Interface**—All member interfaces are in the same network (IP address *not pre-configured; you must set to match your network*): GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (outside2), GigabitEthernet 1/4 (inside2)

- All **inside and outside** interfaces can communicate with each other.

- **Management 1/1 interface**—192.168.1.1/24 for ASDM access.

- **DHCP** for clients on management.

- **ASDM access**—Management hosts allowed.

- **Hardware bypass** is enabled for the following interface pairs: GigabitEthernet 1/1 & 1/2; GigabitEthernet 1/3 & 1/4

  **Note** When the ISA 3000 loses power and goes into hardware bypass mode, only the above interface pairs can communicate; inside1 and inside2, and outside1 and outside2 can no longer communicate. Any existing connections between these interfaces will be lost. When the power comes back on, there is a brief connection interruption as the ASA takes over the flows.

- **ASA FirePOWER module**—All traffic is sent to the module in Inline Tap Monitor-Only Mode. This mode sends a duplicate stream of traffic to the ASA Firepower module for monitoring purposes only.

- **Precision Time Protocol**—PTP traffic is not sent to the FirePOWER module.

The configuration consists of the following commands:

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown

interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown

interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown

interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
```
no shutdown
te interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
    sfr fail-open monitor-only
service-policy global_policy global
Manage the ISA 3000 and the ASA FirePOWER module on the Management 1/1 interface.

Procedure

Step 1
Connect GigabitEthernet 1/1 to an outside router, and GigabitEthernet 1/2 to an inside router. These interfaces form a hardware bypass pair.

Step 2
Connect GigabitEthernet 1/3 to a redundant outside router, and GigabitEthernet 1/4 to a redundant inside router. These interfaces form a hardware bypass pair. These interfaces provide a redundant network path if the other pair fails. All 4 of these data interfaces are on the same network of your choice. You will need to configure the BVI 1 IP address to be on the same network as the inside and outside routers.

Step 3
Connect Management 1/1 to your management computer (or network). You will need to configure the FirePOWER module IP address to be on the same network so your computer can manage both the ASA and the FirePOWER module.

Step 4
(Optional) Connect the management computer to the console port.
Power on the Device

System power is controlled by DC power; there is no power button.

Procedure

Step 1  Attach the power plug to the ISA 3000 after wiring it to the DC power source.
Refer to “Connecting to DC Power” in the hardware installation guide for instructions on proper wiring of
the power plug.

Step 2  Check the System LED on the front panel of the ISA 3000 device; if it is steady green, the device is powered
on. If it is flashing green, the device is in Boot up phase and POST.
Refer to “Verifying Connections” in the hardware installation guide to verify that all devices are properly
connected to the ISA 3000.

(Optional) Change the IP Address

If you cannot use the default IP address for ASDM access, you can set the IP address at the ASA CLI.

Note  This procedure restores the default configuration and also sets your chosen IP address, so if you made any
changes to the ASA configuration that you want to preserve, do not use this procedure.

Procedure

Step 1  Connect to the ASA console port, and enter global configuration mode. See Access the ASA CLI, on page
76 for more information.

Step 2  Restore the default configuration with your chosen IP address.

configure factory-default [ip_address [mask]]

Example:

ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload. Verify there is a valid image on disk0:/ or the system will not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

Step 3  Save the default configuration to flash memory.
write memory

Log Into ASDM

Launch ASDM so you can configure the ASA.

Before you begin

• See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Procedure

Step 1  Enter the following URL in your browser.

• https://192.168.1.1—Management interface IP address.

Note  Be sure to specify https://, and not http:// or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

The Cisco ASDM web page appears. You may see browser security warnings because the ASA does not have a certificate installed; you can safely ignore these warnings and visit the web page.

Step 2  Click one of these available options: Install ASDM Launcher or Run ASDM.
Step 3  Follow the onscreen instructions to launch ASDM according to the option you chose.

The Cisco ASDM-IDM Launcher appears.

Step 4  Leave the username and password fields empty, and click OK.
The main ASDM window appears.

(Optional) Configure ASA Licensing

The ISA 3000 includes the Base or Security Plus license, depending on the version you ordered. The Security Plus license provides more firewall connections, VPN connections, failover capability, and VLANs.

It also comes pre-installed with the Strong Encryption (3DES/AES) license if you qualify for its use; this license is not available for some countries depending on United States export control policy. The Strong Encryption license allows traffic with strong encryption, such as VPN traffic.

This procedure describes how to obtain and activate additional licenses. You do not need to follow this procedure unless you obtain new licenses.

If you need to manually request the Strong Encryption license (which is free), see https://www.cisco.com/go/license.

You can optionally purchase an AnyConnect Plus or Apex license, which allows AnyConnect VPN client connections.

To install additional ASA licenses, perform the following steps.

Procedure

Step 1
Obtain the serial number for your ASA in ASDM by choosing Configuration > Device Management > Licensing > Activation Key.

Note: The serial number used for licensing is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing. To view the licensing serial number, enter the `show version | grep Serial` command or see the ASDM Configuration > Device Management > Licensing Activation Key page.

Step 2
See http://www.cisco.com/go/ccw to purchase the Security Plus license using the following PID:

L-ISA3000SEC+-K9=

For AnyConnect License PIDs, see the Cisco AnyConnect Ordering Guide and the AnyConnect Licensing Frequently Asked Questions (FAQ).

After you order a license, you will then receive an email with a Product Authorization Key (PAK) so you can obtain the license activation key. For the AnyConnect licenses, you receive a multi-use PAK that you can apply to multiple ASAs that use the same pool of user sessions. The PAK email can take several days in some cases.

Step 3
Obtain the activation key from the following licensing website: https://www.cisco.com/go/license

Enter the following information, when prompted:

- Product Authorization Keys
- The serial number of your ASA
- Your e-mail address
An activation key is automatically generated and sent to the e-mail address that you provide. This key includes all features you have registered so far for permanent licenses.

**Step 4**

On the ASDM Configuration > Device Management > Licensing > Activation Key pane, enter the **New Activation Key**.

The key is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal. For example:

ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490

**Step 5**

Click **Update Activation Key**.

---

**Configure the ASA**

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards. You must set the BVI 1 IP address to match your network.

**Procedure**

**Step 1**

Choose **Wizards > Startup Wizard**, and click the **Modify existing configuration** radio button.
Step 2

The **Startup Wizard** walks you through configuring:

- The enable password
- Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces.
- Static routes
- The DHCP server
- And more...

Step 3

Configure the ASA FirePOWER module management IP address.

a) Configure additional ASA settings as desired, or skip screens until you reach the **ASA FirePOWER Basic Configuration** screen.
b) Set the following values to work with the default configuration:

- **IP Address** — 192.168.1.2. If you changed the ASA default IP address according to *(Optional) Change the IP Address, on page 68*, then use an available IP address on the same network. Be sure not to use an IP address in the DHCP server range (if you used the `configure factory-default` command, do not use any address higher than the ASA address you specified).

- **Subnet Mask** — 255.255.255.0

- **Gateway** — Your management router IP address.

c) Click **I accept the agreement**, and click **Next** or **Finish** to complete the wizard.

d) Quit ASDM, and then relaunch. You should see **ASA FirePOWER** tabs on the **Home** page.

---

**Step 4** *(Optional)* From the **Wizards** menu, run other wizards.

**Step 5** To continue configuring your ASA, see the documents available for your software version at **Navigating the Cisco ASA Series Documentation**.
Configure the ASA FirePOWER Module

Use ASDM to install licenses, configure the module security policy, and send traffic to the module.

\[\text{Note} \quad \text{You can alternatively use the Firepower Management Center to manage the ASA FirePOWER module. See the ASA FirePOWER Module Quick Start Guide for more information.}\]

1. Configure FirePOWER Licensing, on page 74.
2. Configure the FirePOWER Security Policy, on page 75.
3. Change the ASA FirePOWER Module to Inline Mode, on page 75.

Configure FirePOWER Licensing

The ASA FirePOWER module uses a separate licensing mechanism from the ASA. No licenses are pre-installed, but the box includes a PAK on a printout that lets you obtain a license activation key for the following licenses:

- **Control and Protection**—Control is also known as “Application Visibility and Control (AVC)” or “Apps”. Protection is also known as “IPS”. In addition to the activation key for these licenses, you also need “right-to-use” subscriptions for automated updates for these features.
  
  The Control (AVC) updates are included with a Cisco support contract.

  The Protection (IPS) updates require you to purchase the IPS subscription from [http://www.cisco.com/go/ccw](http://www.cisco.com/go/ccw). This subscription includes entitlement to Rule, Engine, Vulnerability, and Geolocation updates. **Note:** This right-to-use subscription does not generate or require a PAK/license activation key for the ASA FirePOWER module; it just provides the right to use the updates.

Other licenses that you can purchase include the following:

- **Advanced Malware Protection (AMP)**
- **URL Filtering**

These licenses generate a PAK/license activation key for the ASA FirePOWER module, which you should receive in your email. See the Cisco Firepower System Feature Licenses for more information.

To install ASA FirePOWER licenses, perform the following steps.

**Procedure**

1. **Step 1** Obtain the License Key for your chassis by choosing Configuration > ASA FirePOWER Configuration > Licenses and clicking Add New License.

   The License Key is near the top; for example, 72:78:DA:6E:D9:93:35.
Step 2  Click Get License to launch the licensing portal. Alternatively, in your browser go to https://www.cisco.com/go/license.

Step 3  Enter the PAKs separated by commas in the Get New Licenses field, and click Fulfill.

Step 4  Provide the License Key and email address and other fields.

Step 5  Copy the resulting license activation key from either the website display or from the zip file attached to the licensing email that the system automatically delivers.

Step 6  Return to the ASDM Configuration > ASA FirePOWER Configuration > Licenses > Add New License screen.

Step 7  Paste the license activation key into the License box.

Step 8  Click Verify License to ensure that you copied the text correctly, and then click Submit License after verification.

Step 9  Click Return to License Page.

Configure the FirePOWER Security Policy

Configure the security policy for traffic that you send from the ASA to the FirePOWER module.

Procedure

Choose Configuration > ASA FirePOWER Configuration to configure the ASA FirePOWER security policy.

Use the ASA FirePOWER pages in ASDM for information to learn about the ASA FirePOWER security policy. You can click Help in any page, or choose Help > ASA FirePOWER Help Topics, to learn more about how to configure policies.

See also the ASA FirePOWER module configuration guide.

Change the ASA FirePOWER Module to Inline Mode

The default ISA 3000 configuration sends all traffic to the ASA FirePOWER module in Inline Tap Monitor-Only Mode. This mode sends a duplicate stream of traffic to the module for monitoring purposes only. If you want to change the mode to inline mode, where the module policy affects traffic, and/or to change the traffic sent to the module, perform the following steps.

Procedure

Step 1  Choose Configuration > Firewall > Service Policy Rules.

Step 2  Under Global; Policy: global_policy, select sfrclass, and click Edit.
Step 3  (Optional) Click the ACL tab to change the traffic to send to the module.
By default, the ASA sends all incoming traffic to the module.

Step 4  Click the Rule Actions tab, and then click the ASA FirePOWER Inspection tab.

Step 5  Uncheck the Enable Monitor Only check box to set it to inline mode.

Step 6  (Optional) In the If ASA FirePOWER Card Fails area, click one of the following:

- Permit traffic—(Default) Sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
- Close traffic—Sets the ASA to block all traffic if the module is unavailable.

Step 7  Click OK and then Apply.

Access the ASA CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting to the console port. You can later configure SSH access to the ASA on any interface; SSH access is disabled by default. See the ASA general operations configuration guide for more information.
You can also connect to the ASA FirePOWER module internal console port from the ASA CLI. For details about the FirePOWER CLI, see the "Classic Device Command Reference" in the FMC configuration guide.

Procedure

**Step 1**  
Connect your management computer to the console port, either the RJ-45 port or the mini-USB port. Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:
- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the ASA CLI. There are no user credentials required for console access by default.

**Step 2**  
Access privileged EXEC mode.

```
enable
```

You are prompted to change the password the first time you enter the `enable` command.

**Example:**

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged EXEC mode, enter the `disable`, `exit`, or `quit` command.

**Step 3**  
Access global configuration mode.

```
configure terminal
```

**Example:**

```
ciscoasa# configure terminal
ciscoasa(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the `exit`, `quit`, or `end` command.

**Step 4**  
(Optional) Access the ASA FirePOWER module console.

```
session sfr
```

Log in with the `admin` username and the password. The default password is Admin123. The first time you log in, you are prompted for a new password and for Management interface network settings. You can alternatively set the network settings using ASDM.
Exit the FirePOWER CLI by typing Ctrl-Shift-6, X.

**Example:**

ciscoasa# session sfr
Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

FP3 login: admin
Password: ********
Last login: Wed Mar 13 05:16:08 UTC 2019 on ttyS1

Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.0 (build 42)
Cisco ASA5555 v6.2.0 (build 362)

>  

**What's Next?**

- To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.
- See the online help or the ASA FirePOWER module local management configuration guide or the FMC configuration guide for your version.