



Cisco ISA 3000 Getting Started Guide

First Published: 2019-09-25

Last Modified: 2023-01-23

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

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 the Secure Firewall ASA or the Secure Firewall Threat Defense (formerly Firepower Threat Defense) operating system 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 threat defense, or if you need an ASA-only feature that is not yet available on the threat defense. Cisco provides ASA-to-threat defense migration tools to help you convert your ASA to the threat defense if you start with ASA and later reimage to threat defense.
- **Threat Defense**—The threat defense is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the threat defense takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

We recommend using the threat defense 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 threat defense, see the [Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#).

Managers

The threat defense and ASA support multiple managers.

Threat Defense Managers

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	<p>The management center 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 the management center if you want a multi-device manager, and you require all features on the threat defense. The management center also provides powerful analysis and monitoring of traffic and events.</p> <p>In 6.7 and later, the management center can manage the threat defenses from the outside (or other data) interface instead of from the standard Management interface. This feature is useful for remote branch deployments.</p> <p>Note The management center is not compatible with other managers because the management center owns the threat defense configuration, and you are not allowed to configure the threat defense directly, bypassing the management center.</p> <p>To get started with the management center, see Threat Defense Deployment with the Management Center, on page 35.</p>
Secure Firewall Device Manager (formerly Firepower Device Manager)	<p>The device manager is a web-based, simplified, on-device manager. Because it is simplified, some threat defense features are not supported using the device manager. You should use the device manager if you are only managing a small number of devices and don't need a multi-device manager.</p> <p>Note Both the device manager and CDO in FDM mode can discover the configuration on the firewall, so you can use the device manager and CDO to manage the same firewall. The management center is not compatible with other managers.</p> <p>To get started with the device manager, see Threat Defense Deployment with the Device Manager, on page 5.</p>
Cisco Defense Orchestrator (CDO)	<p>CDO offers two management modes:</p> <ul style="list-style-type: none"> • (7.2 and later) Cloud-delivered management center mode with all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use either Secure Cloud Analytics in the cloud or an on-prem management center. • (Existing CDO users only) Device manager mode with a simplified user experience. This mode is only available to users who are already using CDO to manage threat defenses in device manager mode. This mode is not covered in this guide. <p>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.</p> <p>CDO is not covered in this guide. To get started with CDO, see the CDO home page.</p>

Manager	Description
Secure Firewall Threat Defense REST API	<p>The threat defense REST API lets you automate direct configuration of the threat defense. This API is compatible with the device manager and CDO use because they can both discover the configuration on the firewall. You cannot use this API if you are managing the threat defense using the management center.</p> <p>The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.</p>
Secure Firewall Management Center REST API	<p>The management center REST API lets you automate configuration of management center policies that can then be applied to managed threat defenses. This API does not manage the threat defense directly.</p> <p>The management center REST API is not covered in this guide. For more information, see the Secure Firewall Management Center REST API Quick Start Guide.</p>

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	<p>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 firewall, so you can also use the CLI, CDO, or CSM with ASDM.</p> <p>To get started with ASDM, see ASA Deployment with ASDM, on page 71.</p>
CLI	<p>You should use the ASA CLI if you prefer CLIs over GUIs.</p> <p>The CLI is not covered in this guide. For more information, see the ASA configuration guides.</p>
CDO	<p>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 threat defenses, so you can use a single manager for all of your security devices. CDO can discover the configuration on the firewall, so you can also use the CLI or ASDM.</p> <p>CDO is not covered in this guide. To get started with CDO, see the CDO home page.</p>
Cisco Security Manager (CSM)	<p>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 firewall, so you can also use the CLI or ASDM. CSM does not support managing the threat defenses.</p> <p>CSM is not covered in this guide. For more information, see the CSM user guide.</p>

Manager	Description
ASA REST API	<p>The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced.</p> <p>The ASA REST API is not covered in this guide. For more information, see the Cisco ASA REST API Quick Start Guide.</p>



CHAPTER 2

Threat Defense Deployment with the Device Manager

Is This Chapter for You?

This chapter explains how to complete the initial set up and configuration of your threat defense device using the device manager web-based device setup wizard.

Device Manager 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 device manager devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that threat defense allows, use the management center instead.

The ISA 3000 hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

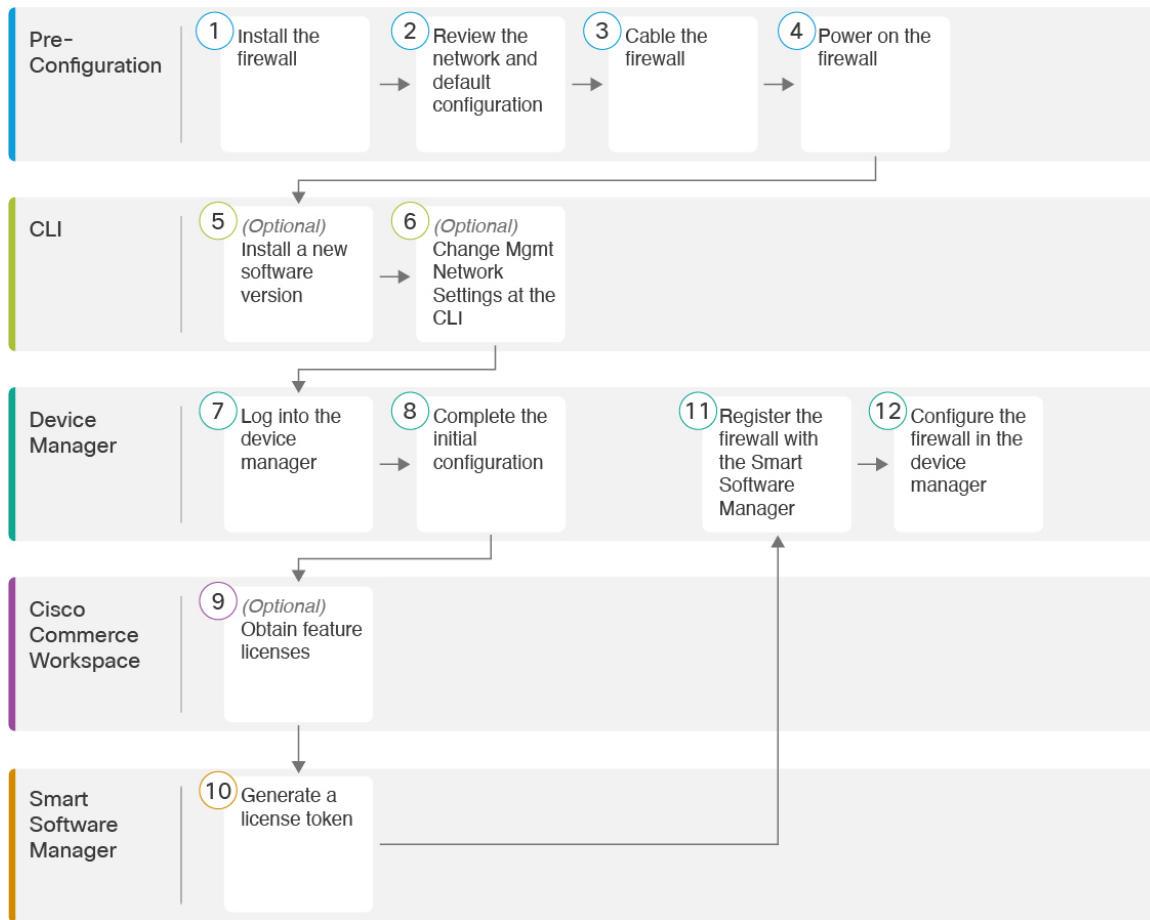
Privacy Collection Statement—The Firepower 1100 Series does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information 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 12](#)
- [Log Into the Device Manager, on page 14](#)
- [Complete the Initial Configuration \(6.5 and Later\), on page 14](#)
- [Complete the Initial Configuration \(6.4 and Earlier\), on page 19](#)
- [Configure Licensing, on page 20](#)
- [Configure the Device in the Device Manager \(6.5 and Later\), on page 26](#)
- [Configure the Firewall in the Device Manager \(6.4 and Earlier\), on page 28](#)
- [Access the Threat Defense CLI, on page 31](#)
- [Power Off the Firewall, on page 32](#)

- [What's Next?, on page 34](#)

End-to-End Procedure

See the following tasks to deploy threat defense with device manager on your chassis.



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 7.
2	Pre-Configuration	<ul style="list-style-type: none"> • Cable the Device (6.5 and Later), on page 10. • Cable the Device (6.4 and Earlier), on page 11
3	Pre-Configuration	Power on the Device, on page 12.
4	Threat Defense CLI	(Optional) Change Management Network Settings at the CLI, on page 12.
5	Device Manager	Log Into the Device Manager, on page 14.

6	Device Manager	<ul style="list-style-type: none"> • Complete the Initial Configuration (6.5 and Later), on page 14 • 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	Device Manager	Configure Licensing , on page 20: Register the device with the Smart Licensing Server.
10	Device Manager	<ul style="list-style-type: none"> • Configure the Device in the Device Manager (6.5 and Later), on page 26 • Configure the Firewall in the 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 12.

Figure 1: 6.5 and Later: Suggested Network Deployment

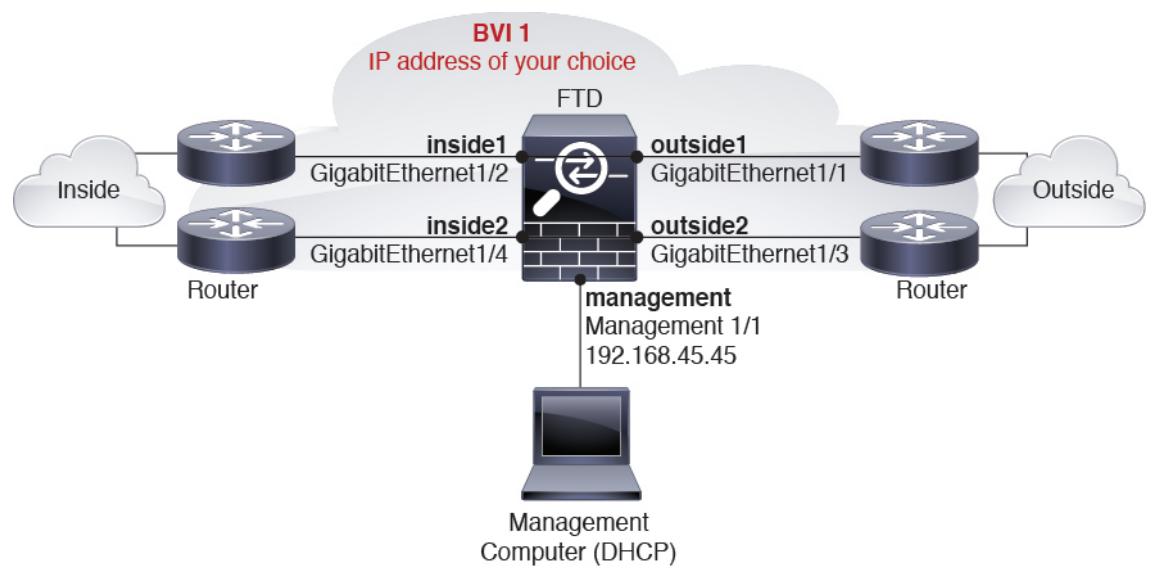
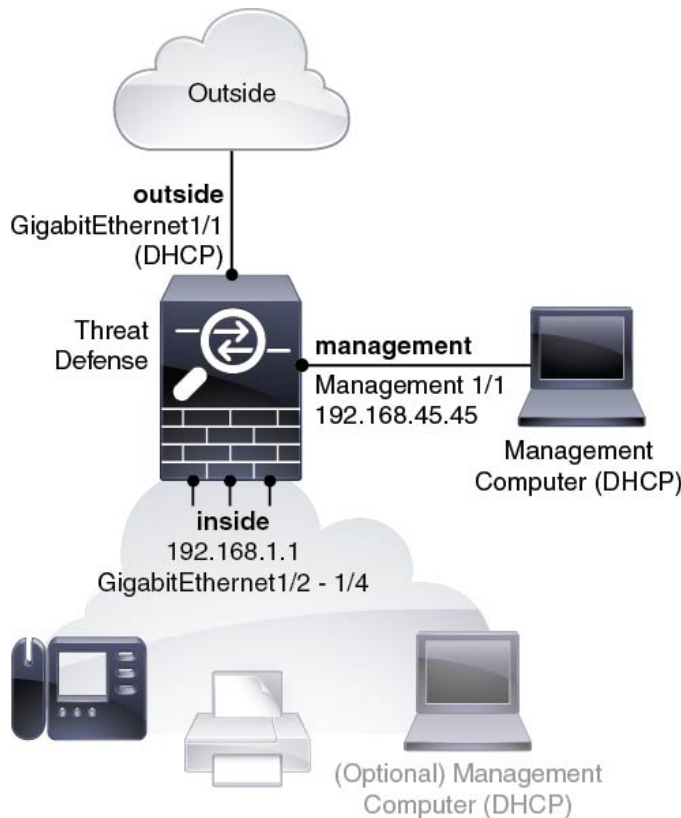


Figure 2: 6.4 and Earlier: Suggested Network Deployment



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 threat defense takes over the flows.

Default Configuration (6.4 and Earlier)

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

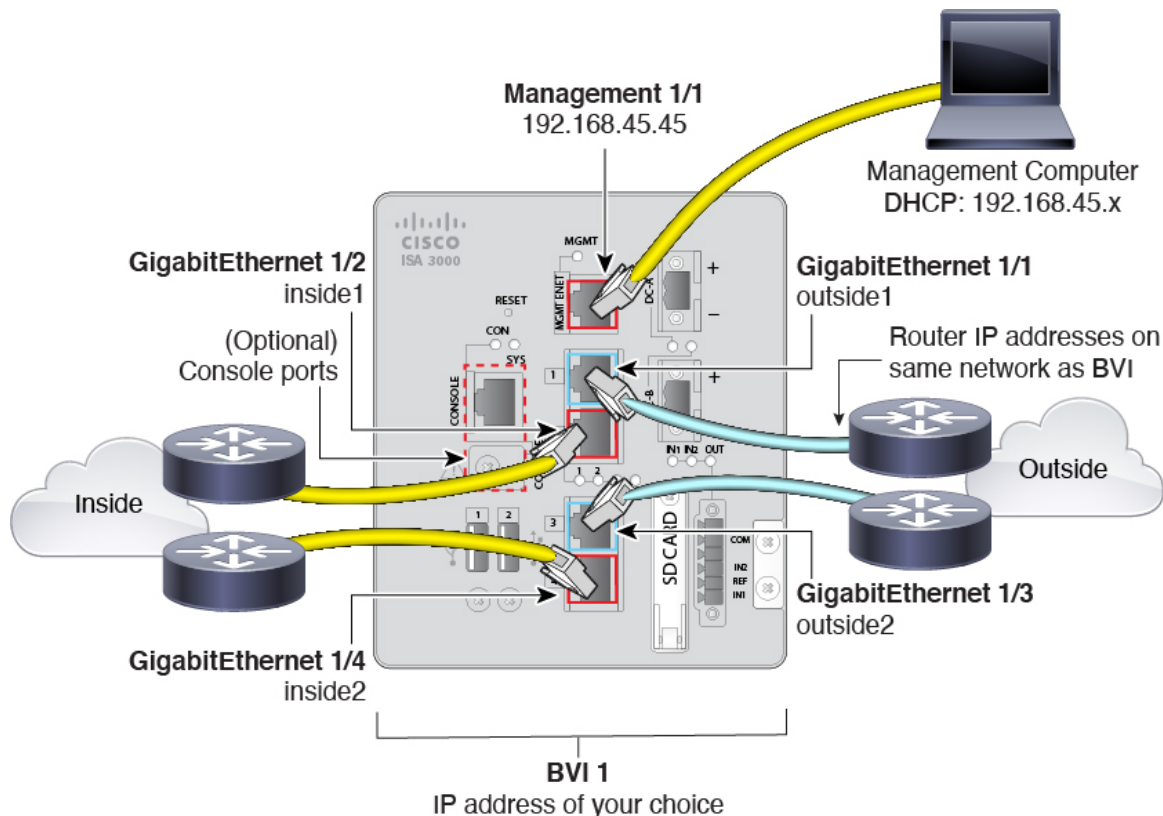
- **inside**—GigabitEthernet 1/2 through 1/4 belong to bridge group interface (BVI) 1, IP address 192.168.1.1
- **outside**—GigabitEthernet 1/1, IP address from DHCP or an address you specify during setup
- **inside**→**outside** traffic flow
- **management**—Management 1/1 (management), IP address 192.168.45.45



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.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup
- **Default routes**
 - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
 - **Management interface**—Over the backplane and through the data interfaces. The threat defense 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)

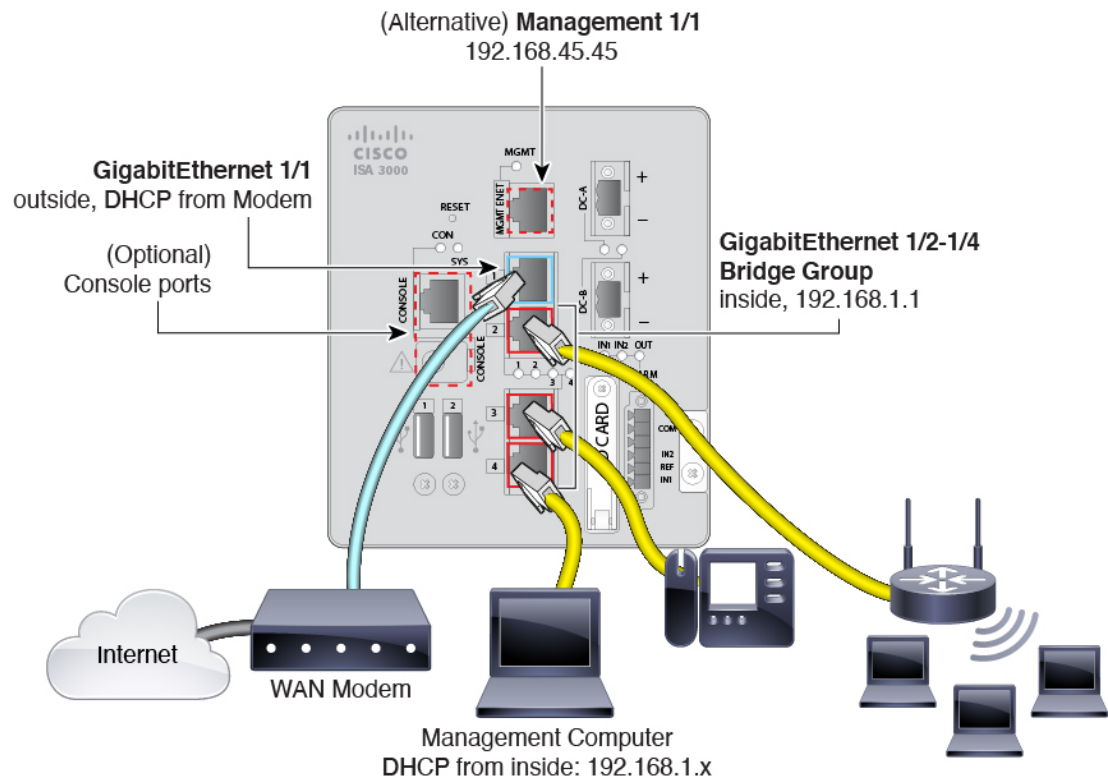


Manage the ISA 3000 on the Management 1/1 interface.

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 12.
-

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 12.

- 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 later configure in the GUI.



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

Procedure

Step 1 Connect to the threat defense console port. See [Access the Threat Defense CLI, on page 31](#) for more information.

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

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the [Cisco ASA and Firepower Threat Defense Device Reimage Guide](#) for instructions.

Step 2 The first time you log into the threat defense, 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 outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the device manager (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that the device manager 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 the device manager. A **no** answer means you intend to use the on-premises or cloud-delivered management center 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 the device manager on the new Management IP address.

Log Into the Device Manager

Log into the device manager to configure your threat defense.

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 device manager 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 14](#).

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 12](#)), 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 () 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 threat defense 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 threat defense 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.

The screenshot shows the 'Add Static Route' configuration window. The fields are as follows:

- Name:** default
- Description:** (empty text area)
- Protocol:** IPv4 (selected), IPv6 (unselected)
- Gateway:** gateway
- Interface:** bvi1 (BV11)
- Metric:** 1
- Networks:** + any-ipv4
- SLA Monitor:** Please select an SLA Monitor (dropdown menu)

Buttons: CANCEL, OK

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 **BVII**.
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 12](#), 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 the 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 the device manager 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 12](#) procedure, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.

Procedure

-
- Step 1** You are prompted to read and accept the End User License Agreement and change the admin password. You must complete these steps to continue.
- Step 2** Configure the following options for the outside and management interfaces and click **Next**.
- Note** Your settings are deployed to the device when you click **Next**. The interface will be named “outside” and it will be added to the “outside_zone” security zone. Ensure that your settings are correct.
- a) **Outside Interface**—This is the data port that you connected to your gateway router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.
- Configure IPv4**—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

b) **Management Interface**

DNS Servers—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

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

Step 3 Configure the system time settings and click **Next**.

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

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

Your purchase of the 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 the device manager; see [Configure the Firewall in the Device Manager \(6.4 and Earlier\), on page 28](#).

Configure Licensing

The threat defense 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:

- **Secure Firewall Threat Defense IPS**—Security Intelligence and Cisco Secure IPS

- **Secure Firewall Threat Defense Malware Defense**—Malware Defense
- **Secure Firewall Threat Defense URL Filtering**—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**.



- b) On the **General** tab, click **New Token**.

The screenshot shows the 'Product Instance Registration Tokens' section of the Cisco licensing configuration page. The 'New Token...' button is circled in red. Below the button is a table with columns for Token, Expiration Date, and Description.

Token	Expiration Date	Description
NWU1MzY1MzEtZjNmOS00MjF..	2018-Jul-06 14:20:13 (in 354 days)	FTD-5506

- c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

The screenshot shows the 'Create Registration Token' dialog box. The 'Description' field is empty, 'Expire After' is set to 30 days, and the 'Allow export-controlled functionality' checkbox is checked. The 'Create Token' button is highlighted in blue.

- **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 threat defense.

Figure 3: View Token

General Licenses Product Instances Event Log

Virtual Account

Description: [REDACTED]

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjhhYTIhZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[REDACTED]	Actions

Figure 4: Copy Token

Token [?] [X]

MjM3ZjhhYTIhZGQ4OS00Yjk2LTgzMGltMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEdscDU4cWI5NFNWRUtsa2wz%0AMDRhST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjhhYTIhZGQ4OS00Yjk2LT... 2017-Aug-16 19:41:53

Step 3 In device manager, click **Device**, and then in the **Smart License** summary, click **View Configuration**. You see the **Smart License** page.

Step 4 Click **Register Device**.

Device Summary

Smart License

LICENSE ISSUE
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left.

REGISTER DEVICE

Then follow the instructions on the **Smart License Registration** dialog box to paste in your token.:

Smart License Registration
✕

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.

↓
- 2 On your assigned virtual account, under “General tab”, click on “**New Token**” to create token.

↓
- 3 Copy the token and paste it here:


```
MGY2NzMwOGIiODJiZi00NzFiLWJiNjltYWwNzU0ODY2ZGVILTE1NiUz
Nzlv%0AODQ5Mzh8SUQ5Vm5XbzZiSmN5M3l6K3owZ3oyVmpmc3Vtal
JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A
```
- 4 Select Region

When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.

Region

SSE US Region
▼
i
- 5 Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enable Cisco Success Network

CANCEL
REGISTER DEVICE

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:

[Device Summary](#)

Smart License

✓

CONNECTED
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM

Next sync: 10 Jul 2019 11:49 AM

i

Step 6 Click the **Enable/Disable** control for each optional license as desired.

SUBSCRIPTION LICENSES INCLUDED

Threat ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware ENABLE

Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

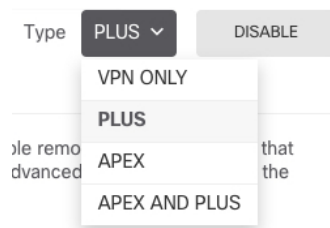
RA VPN License Type PLUS ▾ ENABLE

Disabled by user

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

- **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:

Device Summary

Smart License

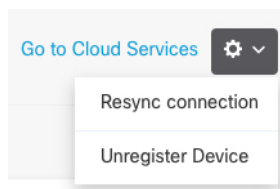
⚠ **LICENSE ISSUE**
OUT OF COMPLIANCE

Last sync: 10 Jul 2019 11:47 AM
Next sync: 10 Jul 2019 11:57 AM

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

GO TO LICENSE MANAGER
Need help?

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



Configure the Device in the 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

 A screenshot of the "Edit Physical Interface" configuration page. The page has a blue header with the title "Edit Physical Interface". Below the header, there are several fields:

- Interface Name:** A text input field containing "dmz".
- Status:** A toggle switch that is turned on (blue).
- Description:** A large text area that is currently empty.
- IPv4 Address:** A tabbed section with three tabs: "IPv4 Address" (selected), "IPv6 Address", and "Advanced Options".
- Type:** A dropdown menu set to "Static".
- IP Address and Subnet Mask:** Two input fields containing "192.168.6.1" and "24", separated by a slash. Below these fields is a small text note: "e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0".

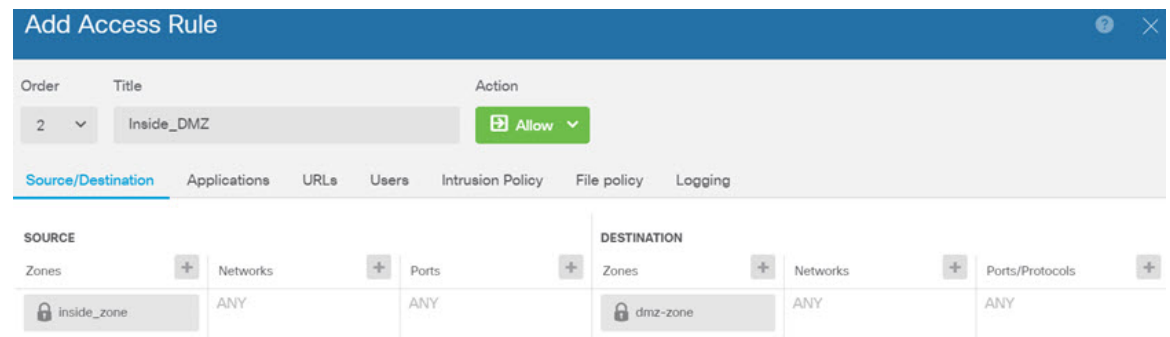
Step 2 Choose **Policies** and configure the security policies for the network.

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



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 Firewall in the 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

Edit Physical Interface

Interface Name: Status:

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask: /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

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 list 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

The screenshot shows the 'Add Static Route' configuration page. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A list containing a '+' icon and a network object 'any-ipv4'.

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.

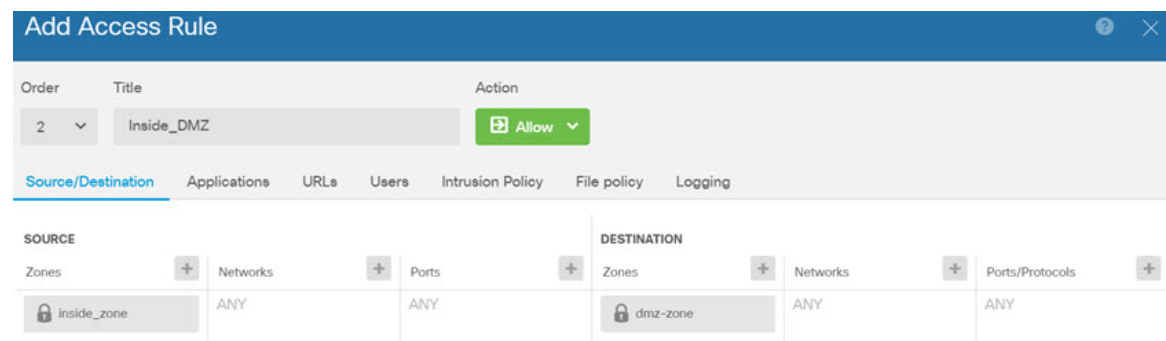
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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



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 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 threat defense 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., 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
- Step 2** Log in to the threat defense 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 Firewall

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

The ISA 3000 chassis does not have an external power switch. You can power off the firewall using device manager, or you can use the CLI.

Power Off the Firewall Using the Device Manager

You can shut down your system properly using the device manager.



Note Shutting down is supported in 7.0.2+/7.2+.

Procedure

- Step 1** Use the device manager to shut down the firewall.
- a) Click **Device**, then click the **System Settings > Reboot/Shutdown** link.
 - b) Click **Shut Down**.
- Step 2** Monitor the shutdown process. If you cannot monitor the device, wait approximately 3 minutes to ensure the system has shut down.
- Console—If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
```

To restart the device, you must Power cycle to the device.

Step 3 You can now unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

It's important that you shut down your system properly. Simply unplugging the power can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your system. The ISA 3000 chassis does not have an external power switch.



Note Shutting down is supported in 7.0.2+/7.2+.

Procedure

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

shutdown

Example:

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfid... [ 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.
```

```
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.

To restart the device, you must Power cycle to the device.
```

- Step 2** After the threat defense 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.
-

What's Next?

To continue configuring your threat defense, see the documents available for your software version at [Navigating the Cisco Firepower Documentation](#).

For information related to using the device manager, see [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#).



CHAPTER 3

Threat Defense Deployment with the Management Center

Is This Chapter for You?

This chapter explains how to complete the initial configuration of your threat defense and how to register the device to a management center. 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 management center, 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 management center, you can use the integrated device manager. Use the device manager web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

The Cisco ISA 3000 can run either the threat defense software or ASA software. Switching between threat defense and ASA requires you to reimagine the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

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.

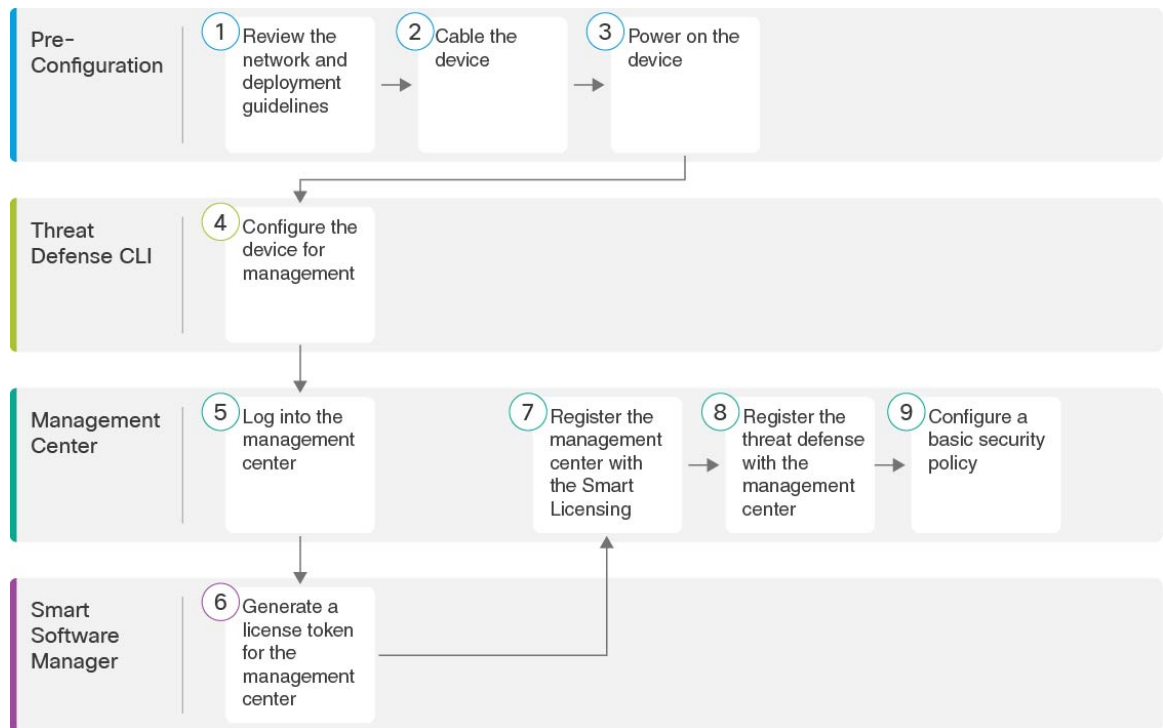
- [Before You Start, on page 36](#)
- [End-to-End Procedure, on page 36](#)
- [Review the Network Deployment, on page 37](#)
- [Cable the Device, on page 41](#)
- [Power on the Device, on page 45](#)
- [Complete the Threat Defense Initial Configuration Using the CLI, on page 46](#)
- [Log Into the Management Center, on page 51](#)
- [Obtain Licenses for the Management Center, on page 52](#)
- [Register the Threat Defense with the Management Center, on page 53](#)
- [Configure a Basic Security Policy, on page 56](#)
- [Access the Threat Defense CLI, on page 67](#)
- [Power Off the Firewall, on page 67](#)
- [What's Next?, on page 69](#)

Before You Start

Deploy and perform initial configuration of the management center. See the [Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide](#) or [Cisco Secure Firewall Management Center Virtual Getting Started Guide](#).

End-to-End Procedure

See the following tasks to deploy the threat defense with management center on your chassis.



1	Pre-Configuration	Review the Network Deployment, on page 37.
2	Pre-Configuration	Cable the Device, on page 41.
3	Pre-Configuration	Power on the Device, on page 45.
4	Threat Defense CLI	Complete the Threat Defense Initial Configuration Using the CLI, on page 46.
5	Management Center	Log Into the Management Center, on page 51.

6	Smart Software Manager	Obtain Licenses for the Management Center, on page 52 : Generate a license token for the management center.
7	Management Center	Obtain Licenses for the Management Center, on page 52 : Register the management center with the Smart Licensing server.
8	Management Center	Register the Threat Defense with the Management Center, on page 53 .
9	Management Center	Configure a Basic Security Policy, on page 56 .

Review the Network Deployment

You can manage the threat defense using management center from the Management 1/1 interface, or in 6.7 and later, a data interface. By default, 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 the management center as the manager during initial setup, the DHCP server is disabled. You can configure the Management interface and an management center access data interface during initial setup at the console port. You can configure other data interfaces after you connect the threat defense to the management center.



Note Management Center access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
- The interface must be in the global VRF only.
- You cannot use separate management and event-only interfaces.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

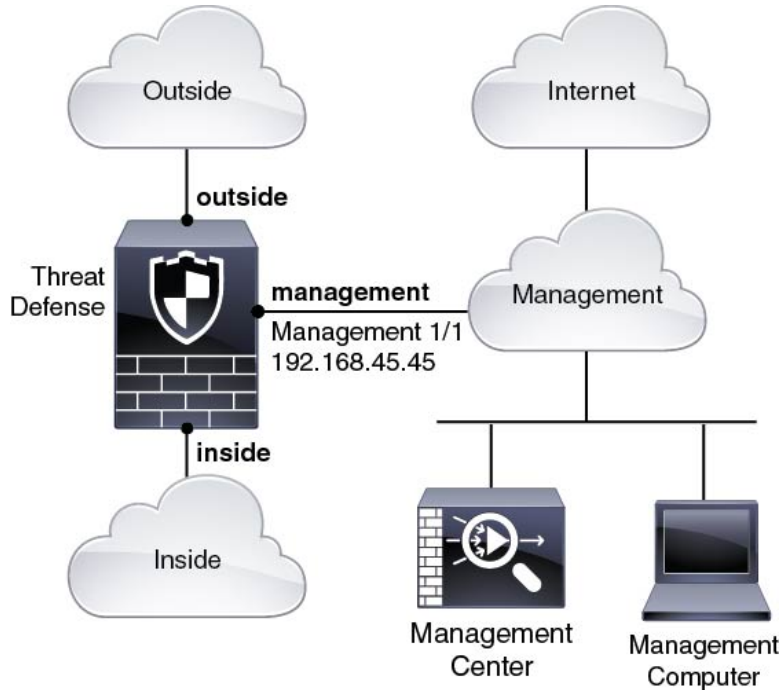
See the following sample network deployments for ideas on how to place your threat defense device in your network.

Separate Management Network

Both the management center and the threat defense require internet access from management for licensing and updates.

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

Figure 12: Separate Management Network



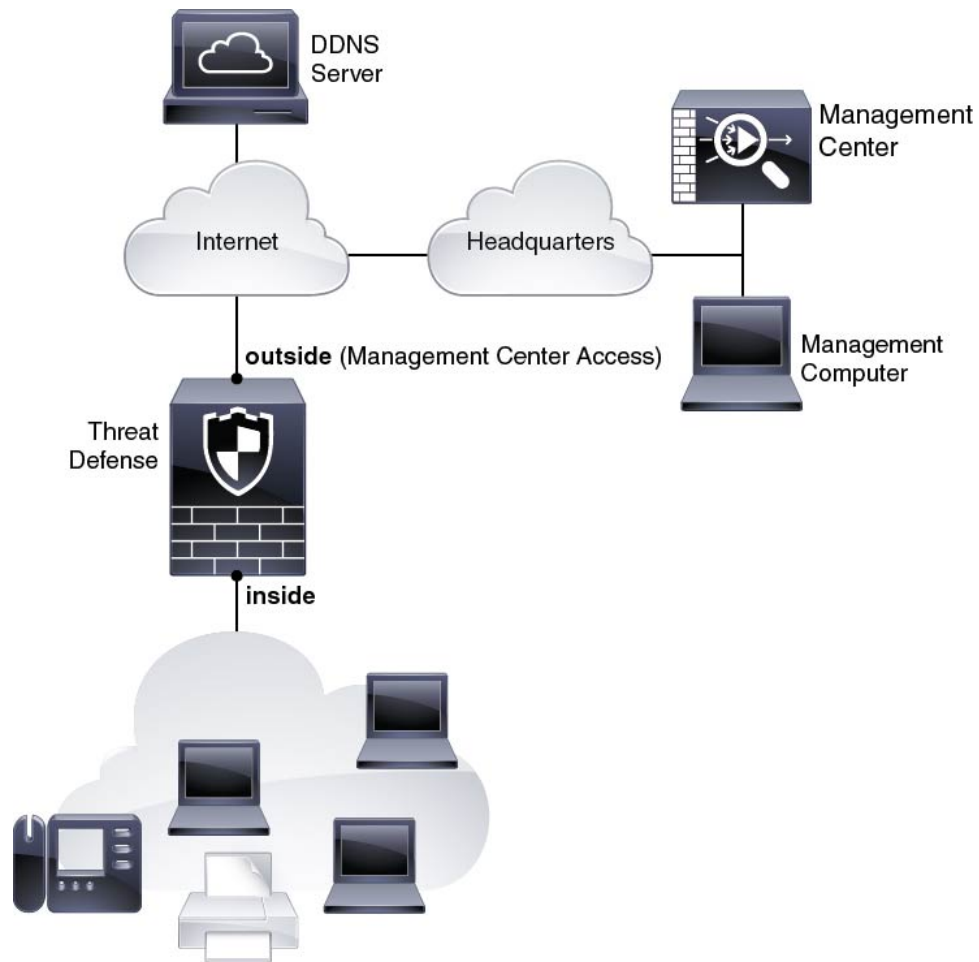
6.7 and Later Remote Management Deployment



Note For a remote branch setup, we recommend that you use the [standalone document](#) specific to that deployment.

The following figure shows the recommended network deployment for the ISA 3000 using the outside interface for management. This scenario is ideal for managing branch offices from a central headquarters. You can perform initial setup of the threat defense at headquarters and then send a pre-configured device to a branch location.

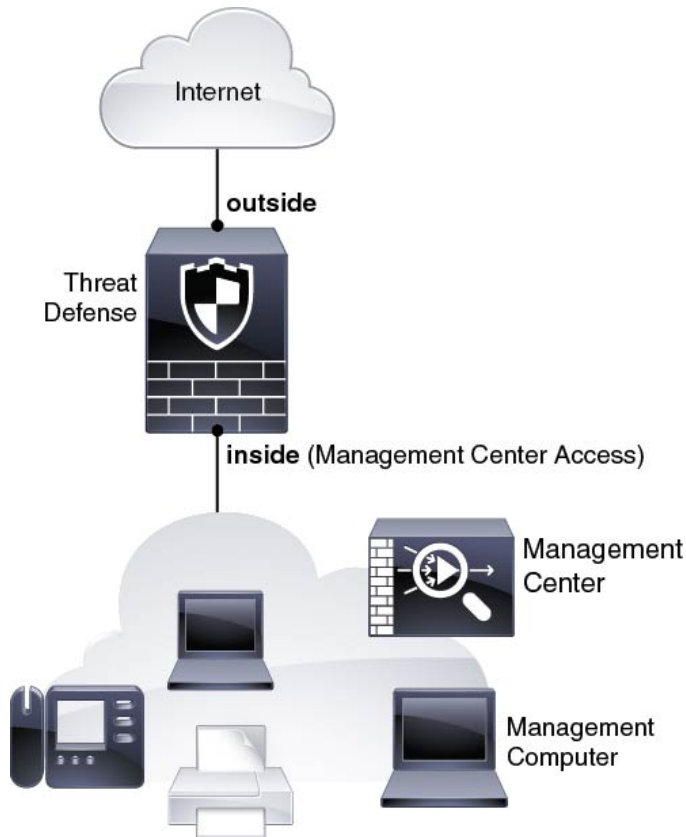
Either the threat defense or management center needs a public IP address or hostname. If the threat defense receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the outside interface. DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. If the threat defense receives a private IP address, then the management center needs to have a public IP address or hostname.

Figure 13: Remote Management Deployment

6.7 and Later Inside Management Deployment

The following figure shows the recommended network deployment for the ISA 3000 using the inside interface for management.

Figure 14: Inside Management Deployment



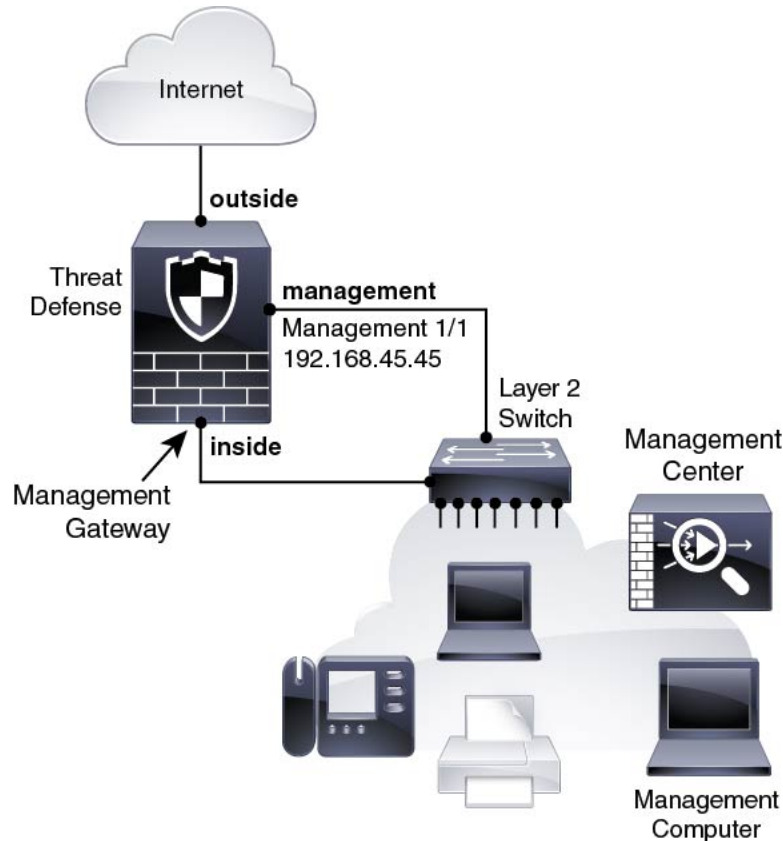
6.6 and Earlier Edge Network Deployment

The management center can only communicate with the threat defense on the management interface in 6.6 and earlier. Moreover, both the management center and threat defense 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 management center and threat defense management. You can also use this scenario in 6.7 and later for a High Availability deployment, for example.

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

Figure 15: Edge Network Deployment



Cable the Device

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



Note The ISA 3000 and the management center 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 management center 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.

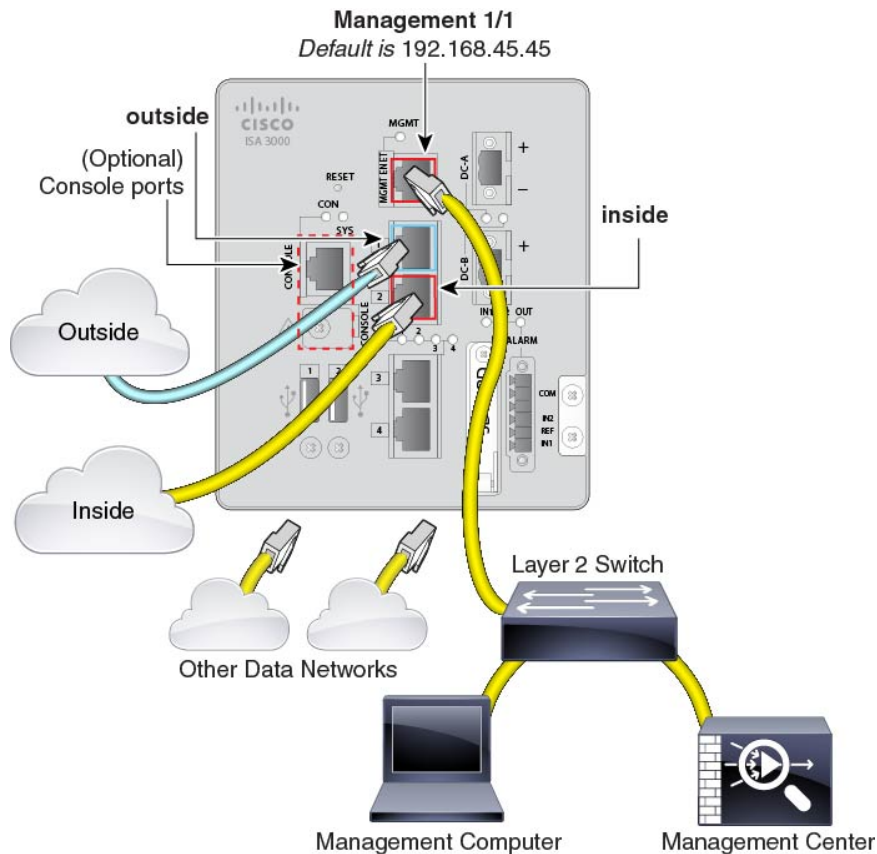


Note Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Procedure

Step 1 Cable for a separate management network.

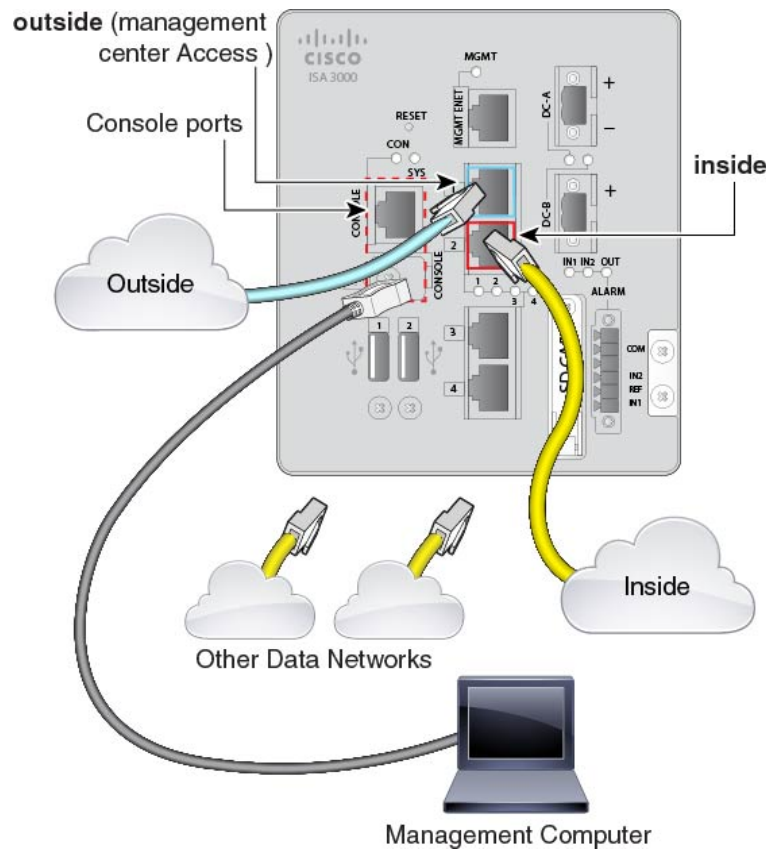
Figure 16: Cabling a Separate Management Network



- Cable the following to your management network:
 - Management 1/1 interface
 - Management Center
 - Management computer
- 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.
- Connect the inside interface (for example, GigabitEthernet 1/2) to your inside router.
- Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- Connect other networks to the remaining interfaces.

Step 2 (6.7 and later) Cable for a remote management deployment:

Figure 17: Cabling a Remote Management Deployment



The management center and your management computer reside at a remote headquarters, and can reach the threat defense over the internet.

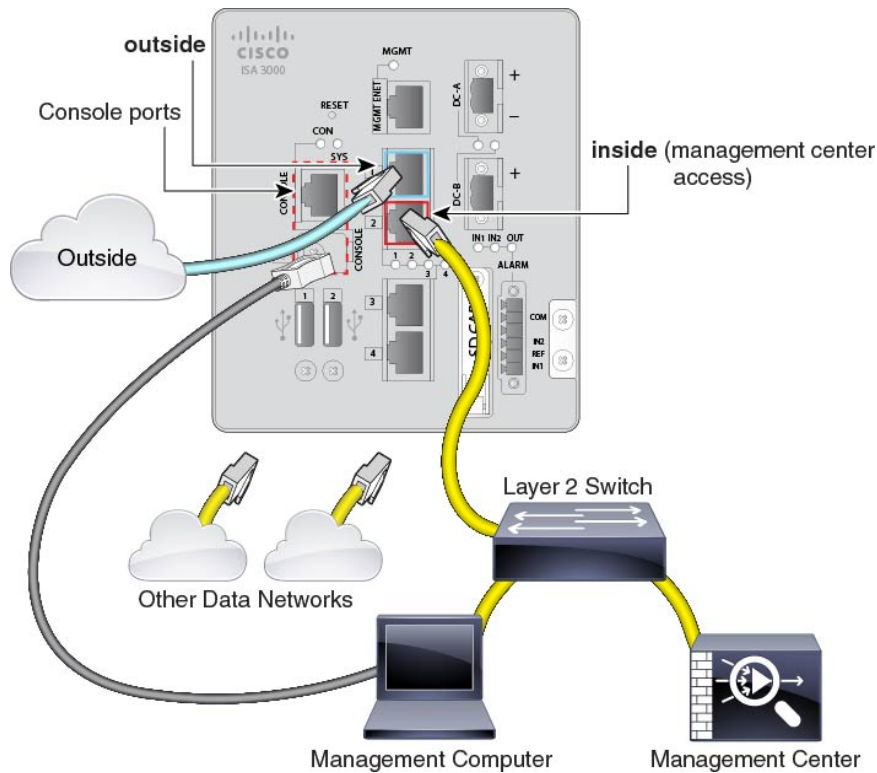
- a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

You can perform initial CLI setup at headquarters, and then send the threat defense to the remote branch office. At the branch office, the console connection is not required for everyday use; it may be required for troubleshooting purposes.

- b) Cable your inside network (for example, GigabitEthernet 1/2).
- c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

Step 3 (6.7 and later) Cable for an inside management deployment:

Figure 18: Cabling an Inside Management Deployment

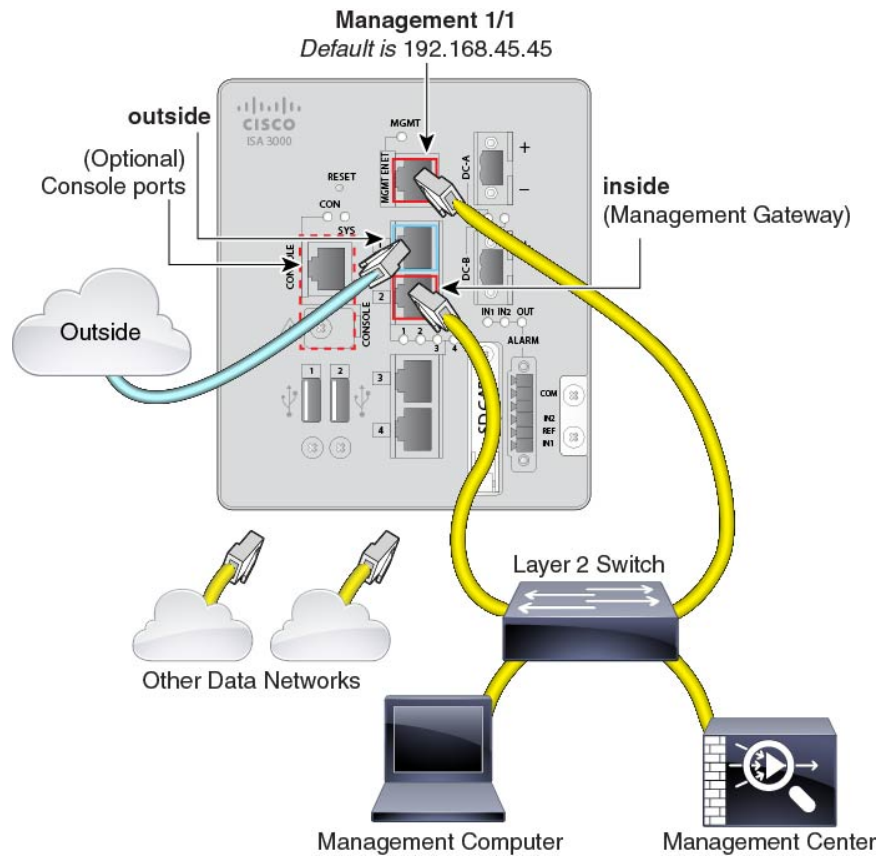


The management center and your management computer reside on the inside network with your other inside end points.

- a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.
- b) Cable the following to the inside network (for example, GigabitEthernet 1/2):
 - Management Center
 - Management computer
- c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

Step 4 (6.6 and earlier) Cable for an edge deployment.

Figure 19: Cabling an Edge Deployment



- Cable the following to a Layer 2 Ethernet switch:
 - Inside interface (for example, GigabitEthernet 1/2)
 - Management 1/1 interface
 - Management Center
 - Management computer
- 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.
- Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- 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 uninterruptible 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 Threat Defense Initial Configuration Using the CLI

Connect to the threat defense 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. In 6.7 and later: If you do not want to use the Management interface for the management center access, you can use the CLI to configure a data interface instead. You will also configure management center communication settings.

Procedure

- Step 1** Connect to the threat defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. 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**.
- Note** If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the [reimage guide](#) for instructions.
- Step 3** The first time you log in to the threat defense, 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**.

Note In 6.7 and later: The Management interface settings are used even when you enable the management center access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—In 6.7 and later: If you want to use a data interface for the management center access instead of the management interface, choose **manual**. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface**—In 6.7 and later: If you want to use a data interface for the management center access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the management center access data interface. If you want to use the Management interface for the management center access, you should set a gateway IP address on the Management 1/1 network.
- **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.
- **Manage the device locally?**—Enter **no** to use management center. A **yes** answer means you will use the device manager instead.
- **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. Note that data interface management center access is only supported in routed firewall mode.

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]: no
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 management center that will manage this threat defense.

```
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 management center. If the management center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the management center or the threat defense, 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 threat defense 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 management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumeric 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 management center when you register the threat defense when one side does not specify a reachable IP address or hostname. It is required if you set the management center to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Note If you use a data interface for management, then you must specify the NAT ID on both the threat defense and the management center for registration.

Example:

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

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

Example:

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

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

Example:

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

Step 5 (Optional) (6.7 and Later) Configure a data interface for the management center access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command:

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network {ipv4 | ipv6} manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- Management Center access from a data interface has the following limitations:
 - You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
 - This interface cannot be management-only.
 - Routed firewall mode only, using a routed interface.
 - PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
 - The interface must be in the global VRF only.
 - You cannot use separate management and event-only interfaces.
 - SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.
- When you add the threat defense to the management center, the management center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In management center, you can later make changes to the management center access interface configuration, but make sure you don't make changes that can prevent the threat defense

or management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.

- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (<https://help.dyn.com/remote-access-api/>).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in the management center, including the DNS servers, to match the threat defense configuration.

- You can change the management interface after you register the threat defense to the management center, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data management, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichon:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

Example:

```

> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

```

Step 6 (Optional) (6.7 and Later) Limit data interface access to an management center on a specific network.

```
configure network management-data-interface client ip_address netmask
```

By default, all networks are allowed.

What to do next

Register your device to a management center.

Log Into the Management Center

Use the management center to configure and monitor the threat defense.

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 Management Center

All licenses are supplied to the threat defense by the management center. You can purchase the following licenses:

- **Threat**—Security Intelligence and Next-Generation IPS
- **Malware**—Malware defense
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Before you begin

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

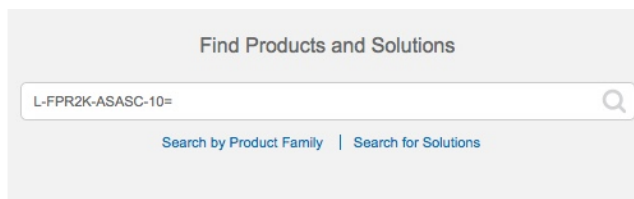
Procedure

Step 1

Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the [Cisco Commerce Workspace](#). Search for the following license PIDs:

Figure 20: License Search



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 Secure Client Ordering Guide](#).

Step 2 If you have not already done so, register the management center with the Smart Licensing server. Registering requires you to generate a registration token in the Smart Software Manager. See the [Cisco Secure Firewall Management Center Administration Guide](#) for detailed instructions.

Register the Threat Defense with the Management Center

Register the threat defense to the management center manually using the device IP address or hostname.

Before you begin

- Gather the following information that you set in the threat defense initial configuration:
 - The threat defense management IP address or hostname, and NAT ID
 - The management center registration key

Procedure

Step 1 In the management center, choose **Devices > Device Management**.

Step 2 From the **Add** drop-down list, choose **Add Device**.

The screenshot shows the 'Add Device' configuration window. It contains the following fields and options:

- Host:** A text input field containing 'ftd-1.cisco.com'.
- Display Name:** A text input field containing 'ftd-1.cisco.com'.
- Registration Key:*** A text input field containing '....'.
- Group:** A dropdown menu with 'None' selected.
- Access Control Policy:*** A dropdown menu with 'inside-outside' selected.
- Smart Licensing:** Three checked checkboxes: Malware, Threat, and URL Filtering.
- Advanced:**
 - Unique NAT ID:†** A text input field containing 'natid56'.
 - Transfer Packets:** A checked checkbox.

At the bottom right, there are two buttons: 'Cancel' and 'Register'.

Set the following parameters:

- **Host**—Enter the IP address or hostname of the threat defense you want to add. You can leave this field blank if you specified both the management center IP address and a NAT ID in the threat defense initial configuration.
 - Note** In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.
- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.
- **Registration Key**—Enter the same registration key that you specified in the threat defense 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 64](#).

Figure 21: New Policy

New Policy ?

Name:
ftd-ac-policy

Description:

Select Base Policy:
None

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

Cancel Save

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use 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 Client remote access VPN license after you add the device, from the **System > Licenses > Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial configuration.
- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, but packet data is not sent.

Step 3 Click **Register**, or if you want to add another device, click **Register and Add Another** 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 threat defense fails to register, check the following items:

- **Ping**—Access the threat defense CLI, and ping the management center 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 threat defense Management IP address, use the **configure network {ipv4 | ipv6} manual** command. If you configured a data interface for the management center access, use the **configure network management-data-interface** command.

- **Registration key, NAT ID, and the management center 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 management center using the **configure manager add** command.

For more troubleshooting information, see <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.

1	Configure Interfaces, on page 56.
2	Configure the DHCP Server, on page 59.
3	Add the Default Route, on page 60.
4	Configure NAT, on page 62.
5	Allow Traffic from Inside to Outside, on page 64.
6	Deploy the Configuration, on page 65.

Configure Interfaces

Enable the threat defense 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** (✎) for the firewall.
- Step 2** Click **Interfaces**.

The screenshot shows the Cisco Management Center interface for a Cisco Firepower 9000 Series SM-24 Threat Defense device. The 'Devices' tab is active, and the 'Interfaces' sub-tab is selected. A table lists the interfaces:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		SubInterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

- Step 3** Click **Edit** (✎) for the interface that you want to use for *inside*.
The **General** tab appears.

The 'Edit Physical Interface' dialog box is shown with the 'General' tab selected. The configuration is as follows:

- Name:** inside
- Enabled:** Enabled
- Management Only:** Management Only
- Description:** (empty text box)
- Mode:** None
- Security Zone:** inside_zone
- Interface ID:** GigabitEthernet0/0
- MTU:** 1500 (range: 64 - 9000)

- Enter a **Name** up to 48 characters in length.
For example, name the interface **inside**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- 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**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

Step 4 Click the **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

Note If you pre-configured this interface for manager access, then the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You can still configure the Security Zone on this screen for through traffic policies.

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.

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1', with a range of '(1 - 255)' shown to the right.

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

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

Procedure

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

Step 2 Choose **DHCP > DHCP Server**.

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.

Step 4 Click **OK**.

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:

The screenshot shows the 'Add Static Route Configuration' dialog box with the following settings:

- Type: IPv4 IPv6
- Interface*: outside
- Available Network: any-ipv4 (selected)
- Selected Network: any-ipv4
- Gateway*: default-gateway
- Metric: 1 (range 1 - 254)
- Tunneled: (Used only for default Route)
- Route Tracking: (empty)

- **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.

The screenshot shows the Cisco Management Center interface with the following details:

- Navigation: Overview, Analysis, Policies, **Devices**, Objects, AMP, Intelligence
- Sub-navigation: Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, Certificates
- Version: 10.89.5.20
- Device: Cisco Firepower 9000 Series SM-24 Threat Defense
- Routing Configuration:

Network	Interface	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes						
any-ipv4	outside	10.99.10.1	false	1		
▼ IPv6 Routes						

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

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

Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

The screenshot shows the 'New Policy' dialog box. The 'Name' field is set to 'interface_PAT'. The 'Description' field is empty. Under 'Targeted Devices', there are two lists: 'Available Devices' and 'Selected Devices'. The 'Available Devices' list contains one item: '192.168.0.16'. The 'Selected Devices' list also contains one item: '192.168.0.16', which is highlighted with a red circle. An 'Add to Policy' button is located between the two lists. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

The policy is added to the management center. 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:

The screenshot shows the 'Add NAT Rule' dialog box. The 'NAT Rule' dropdown is set to 'Auto NAT Rule'. The 'Type' dropdown is set to 'Dynamic'. The 'Enable' checkbox is checked. Below are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'.

- **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.

The screenshot shows the 'Add NAT Rule' dialog box with the 'Interface Objects' tab selected. The 'NAT Rule' is set to 'Auto NAT Rule' and the 'Type' is 'Dynamic'. The 'Enable' checkbox is checked. In the 'Available Interface Objects' section, 'outside_zone' is selected and marked with a red '1'. The 'Add to Destination' button is marked with a red '2'. The 'Destination Interface Objects (1)' section contains 'outside_zone' and is marked with a red '3'. The 'Source Interface Objects (0)' section is empty.

Step 6 On the **Translation** page, configure the following options:

The screenshot shows the 'Add NAT Rule' dialog box with the 'Translation' tab selected. The 'NAT Rule' is 'Auto NAT Rule' and the 'Type' is 'Dynamic'. The 'Enable' checkbox is checked. In the 'Original Packet' section, 'Original Source:*' is set to 'all-ipv4' (circled in red) and 'Original Port' is set to 'TCP'. In the 'Translated Packet' section, 'Translated Source' is set to 'Destination Interface IP' (circled in red). The 'Translated Port' field is empty.

- **Original Source**—Click **Add (+)** to add a network object for all IPv4 traffic (0.0.0.0/0).

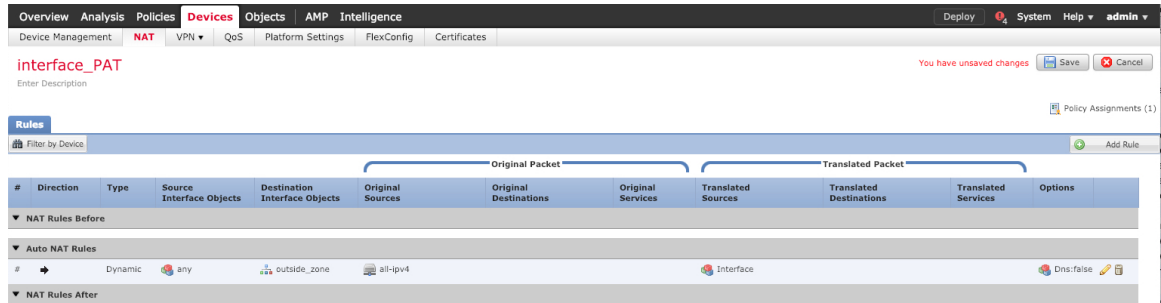
The screenshot shows the 'New Network Object' dialog box. The 'Name' field contains 'all-ipv4'. The 'Description' field is empty. The 'Network' radio button is selected and circled in red. The 'Network' field contains '0.0.0.0/0' and is circled in red. The 'Allow Overrides' checkbox is unchecked. The 'Save' and 'Cancel' buttons are at the bottom.

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.

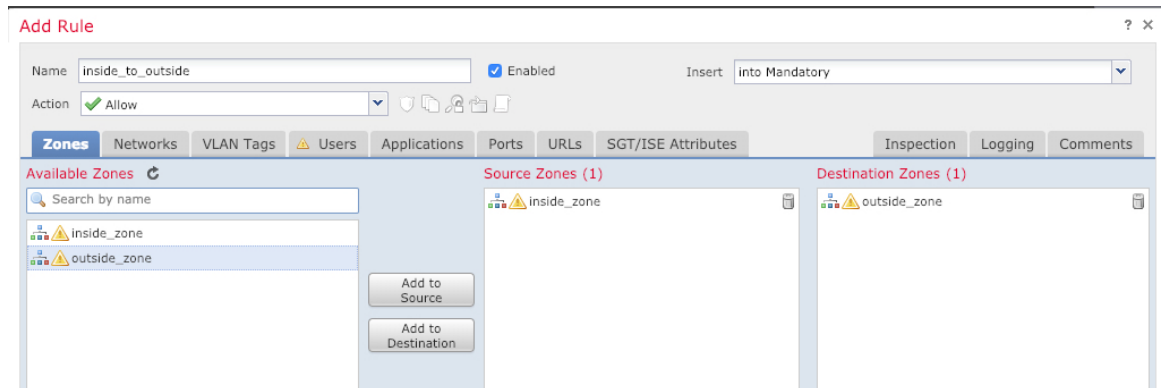
Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the threat defense, 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.

Procedure

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

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



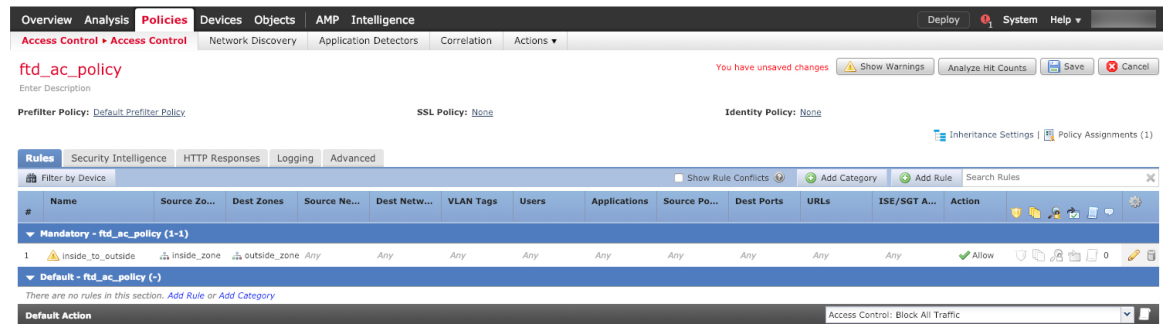
- **Name**—Name this rule, for example, **inside_to_outside**.

- **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 threat defense; none of your changes are active on the device until you deploy them.

Procedure

Step 1 Click **Deploy** in the upper right.

Figure 22: Deploy



Step 2 Either click **Deploy All** to deploy to all devices or click **Advanced Deploy** to deploy to selected devices.

Figure 23: Deploy All

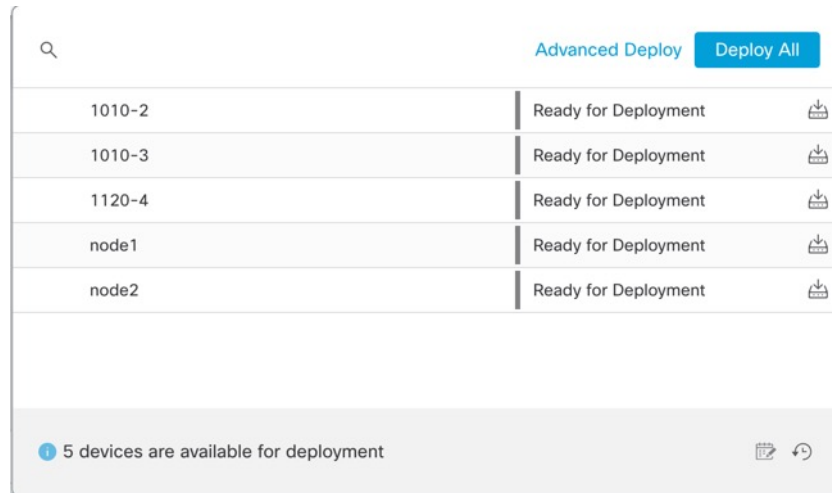
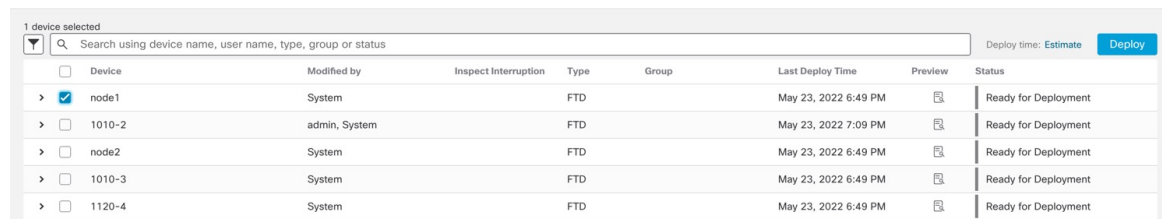
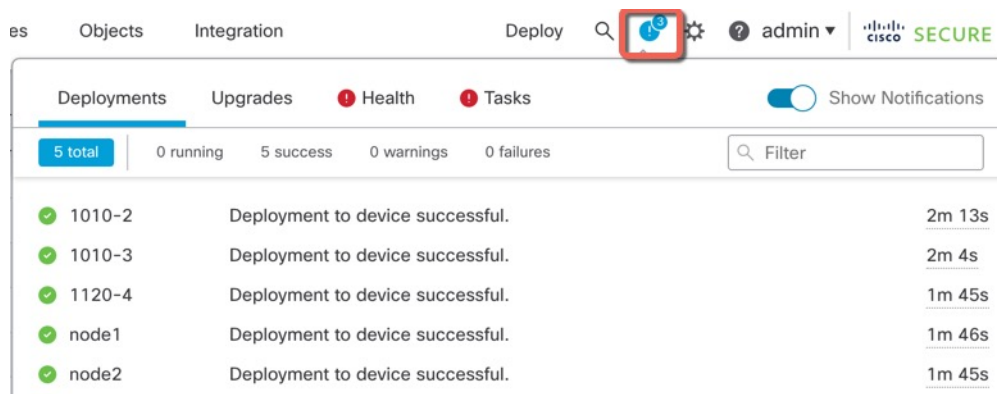


Figure 24: Advanced Deploy

**Step 3**

Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 25: Deployment Status



Access the 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 threat defense 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., 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

Step 2 Log in to the threat defense 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 Firewall

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

The ISA 3000 chassis does not have an external power switch. You can power off the device using the management center device management page, or you can use the CLI.

Power Off the Firewall Using the Management Center

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch 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 firewall.



Note Shutting down is supported in 7.0.2+/7.2+.

You can shut down your system properly using the management center.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device that you want to restart, click the edit icon (✎).
- Step 3** Click the **Device** tab.
- Step 4** Click the shut down device icon (🔴) in the **System** section.
- Step 5** When prompted, confirm that you want to shut down the device.
- Step 6** Monitor the shutdown process. If you cannot monitor the device, wait approximately 3 minutes to ensure the system has shut down.

- **Console**—If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

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

```
To restart the device, you must Power cycle to the device.
```

- Step 7** You can now unplug the power to physically remove power from the chassis if necessary.
-

Power Off the Firewall at the CLI

It's important that you shut down your system properly. Simply unplugging the power can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your system. The ISA 3000 chassis does not have an external power switch.



Note Shutting down is supported in 7.0.2+/7.2+.

Procedure

- Step 1** Connect to the console port to access the threat defense CLI, and then shut down the threat defense.

shutdown

Example:

```
> shutdown
```

```

This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfidf... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on brl [ 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.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface brl 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.

To restart the device, you must Power cycle to the device.

```

- Step 2** After the threat defense 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.

What's Next?

To continue configuring your threat defense, see the documents available for your software version at [Navigating the Cisco Firepower Documentation](#).

For information related to using the management center, see the [Firepower Management Center Configuration Guide](#).



CHAPTER 4

ASA 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 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
- (9.16 and earlier) FirePOWER Module

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

The ISA 3000 hardware can run either ASA software or threat defense software. Switching between ASA and threat defense requires you to reimage the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

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 72](#)
- [End-to-End Procedure, on page 72](#)
- [Review the Network Deployment and Default Configuration, on page 74](#)
- [Cable the Firewall, on page 76](#)
- [Power on the Device, on page 77](#)
- [\(Optional\) Change the IP Address, on page 77](#)
- [Log Into the ASDM, on page 78](#)
- [\(Optional\) Configure ASA Licensing, on page 79](#)
- [Configure the ASA, on page 80](#)
- [Access the ASA CLI, on page 82](#)
- [What's Next?, on page 83](#)

About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device.

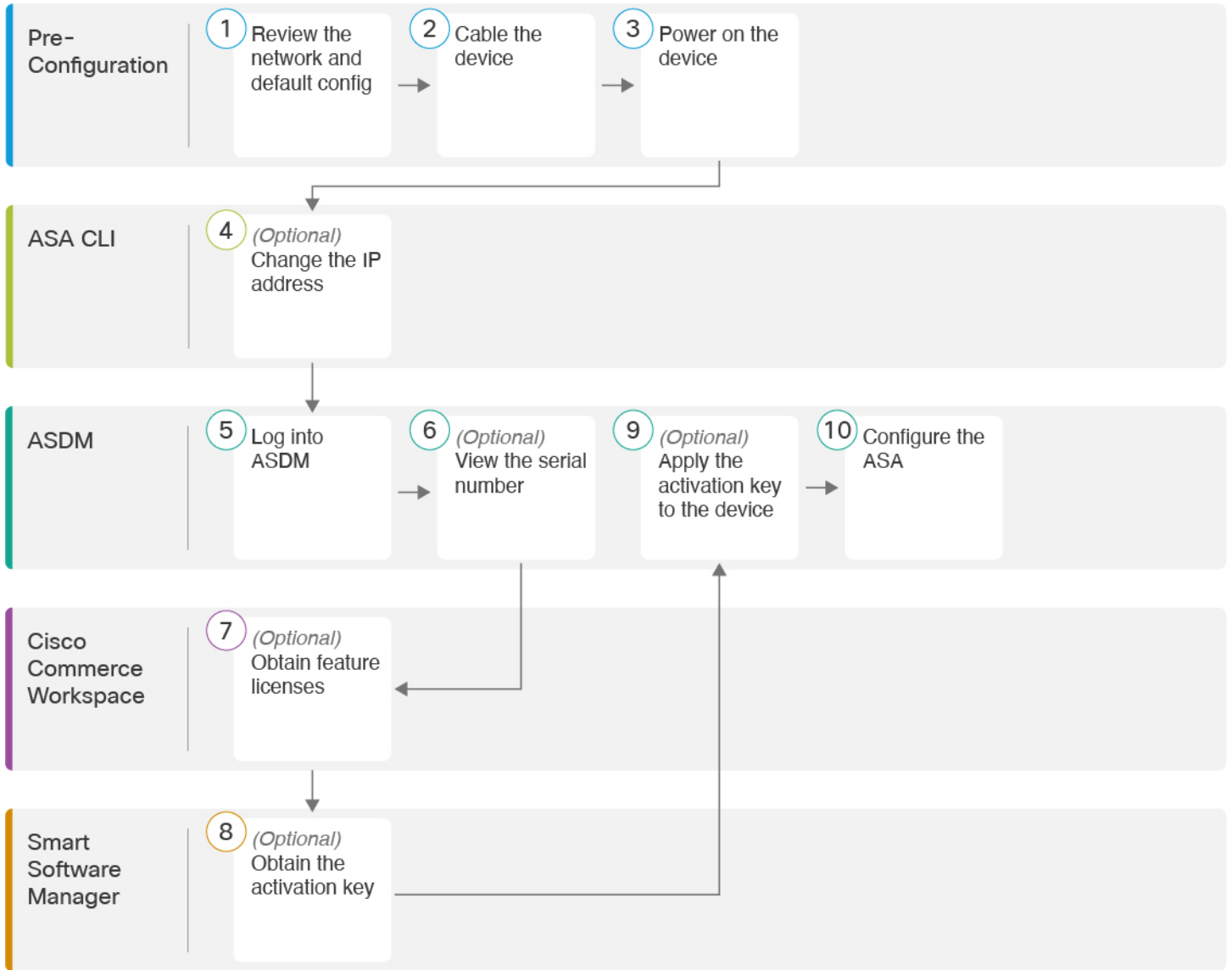
You can manage the ASA using one of the following managers:

- ASDM (covered in this guide)—A single device manager included on the device.
- CLI
- CDOF—A simplified, cloud-based multi-device manager
- Cisco Security Manager—A multi-device manager on a separate server.

End-to-End Procedure

See the following tasks to deploy and configure the ASA on your chassis.

Figure 26: End-to-End Procedure



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 74.
2	Pre-Configuration	Cable the Firewall, on page 76.
3	Pre-Configuration	Power on the Device, on page 77.
4	ASA CLI	(Optional) Change the IP Address, on page 77.
5	ASDM	Log Into the ASDM, on page 78.

6	ASDM	(Optional) Configure ASA Licensing, on page 79 : View the serial number.
7	Cisco Commerce Workspace	(Optional) Configure ASA Licensing, on page 79 : Obtain feature licenses.
8	Smart Software Manager	(Optional) Configure ASA Licensing, on page 79 : Obtain the activation key.
9	ASDM	(Optional) Configure ASA Licensing, on page 79 : Apply the activation key to the device.
10	ASDM	Configure the ASA, on page 80 .

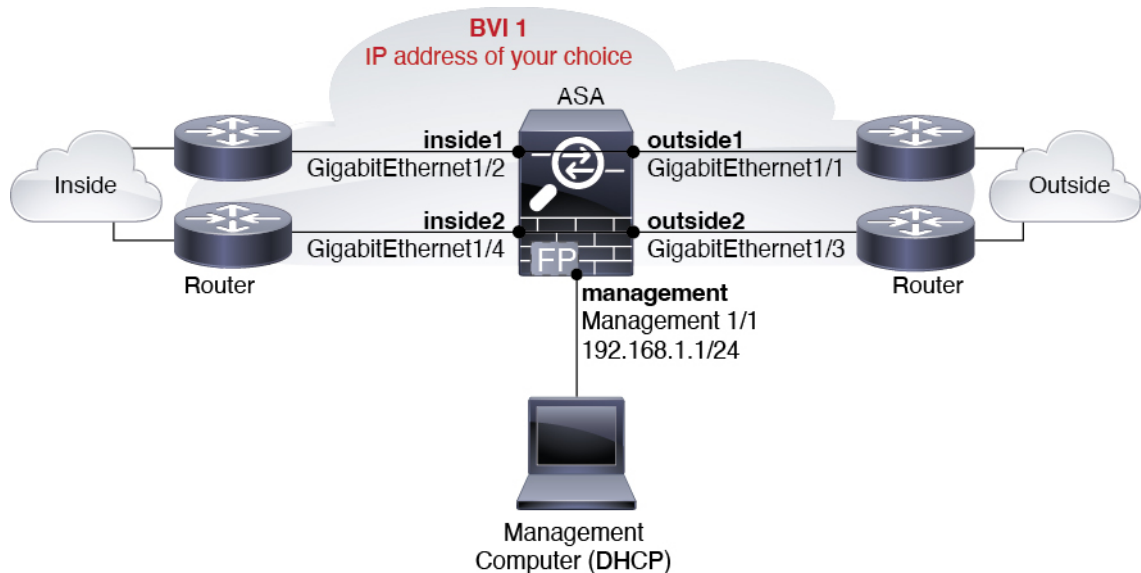
Review the Network Deployment and Default Configuration

The following figure shows the recommended network deployment for the ISA 3000.



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 77](#).

Figure 27: ISA 3000 Network



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.

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
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

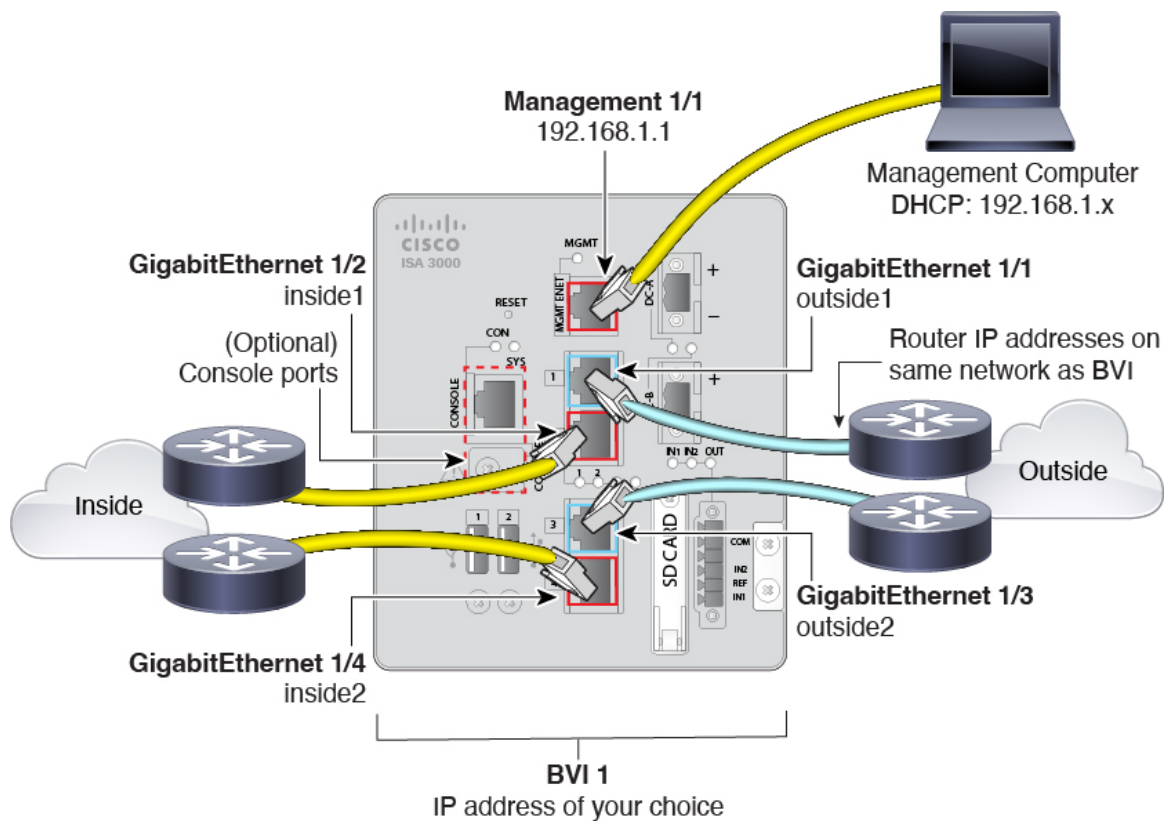
http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

```

Cable the Firewall

Figure 28: Cable the Firewall



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 computer (or network).
- Step 4** (Optional) Connect the management computer to the console port. If you need to change the management IP address from the default, you must also cable your management computer to the console port. See [\(Optional\) Change the IP Address, on page 77](#).
-

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 of the management interface 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 82](#) 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 management1/1
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 the ASDM

Launch the 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
```

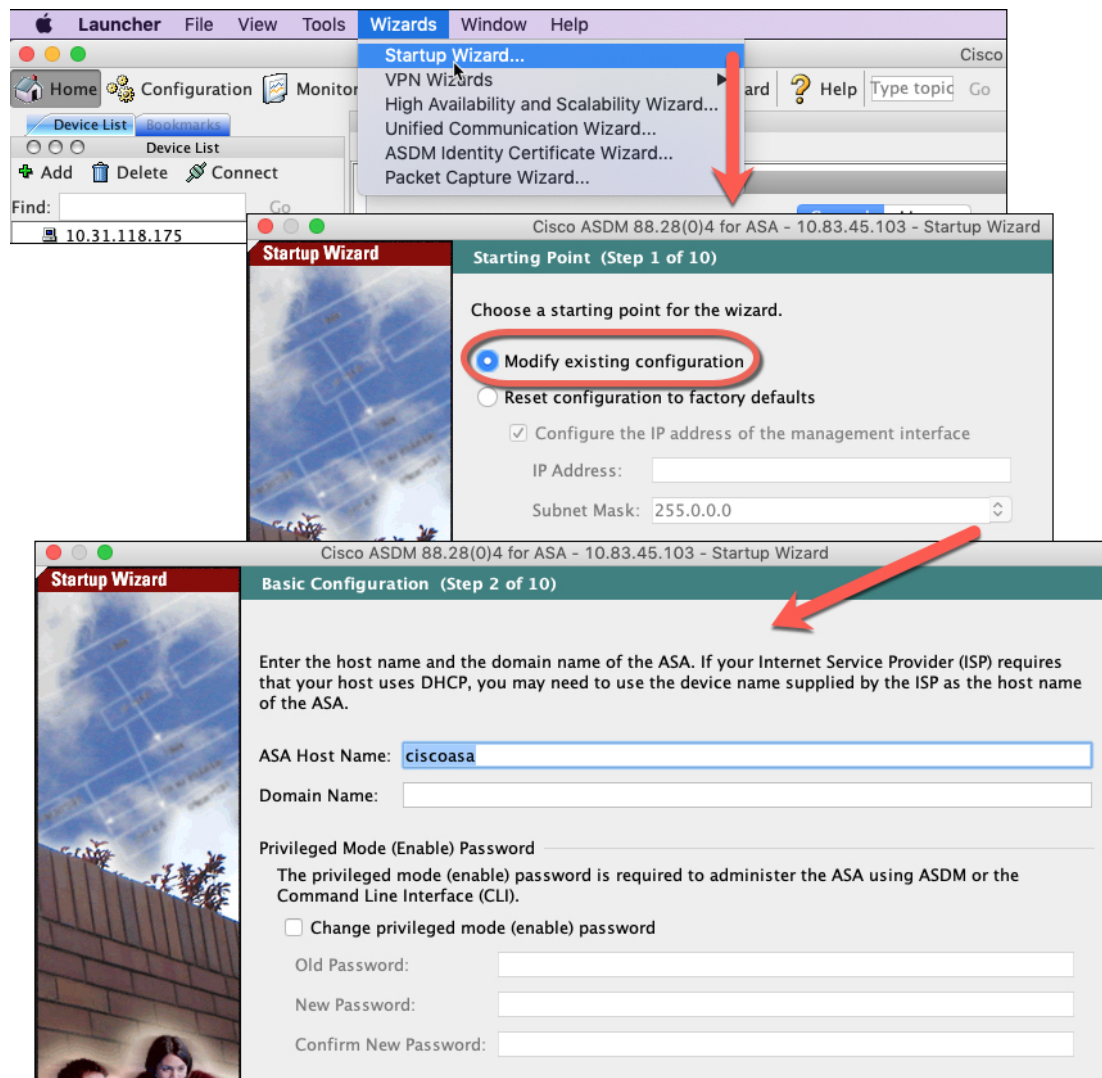
Step 5 Click **Update Activation Key**.

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

Step 4 To continue configuring your ASA, see the documents available for your software version at [Navigating the Cisco ASA Series Documentation](#).

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.

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.

What's Next?

- To continue configuring your ASA, see the documents available for your software version at [Navigating the Cisco ASA Series Documentation](#).

