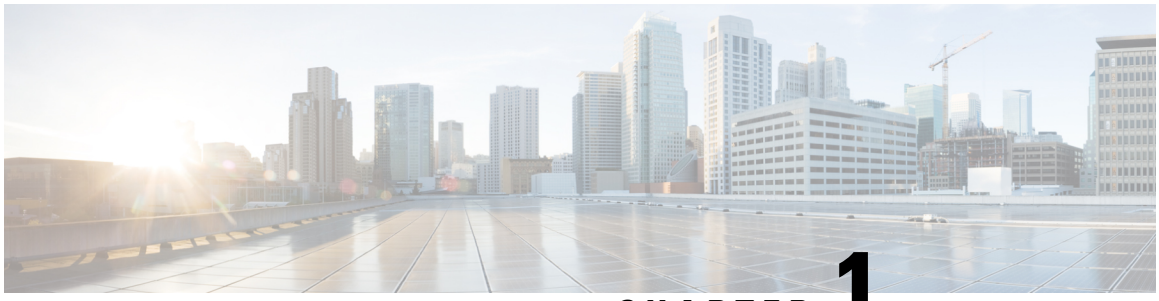
Secure Firewall 4200 ASA Getting Started

First Published: 2024-10-14

Last Modified: 2024-10-21

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



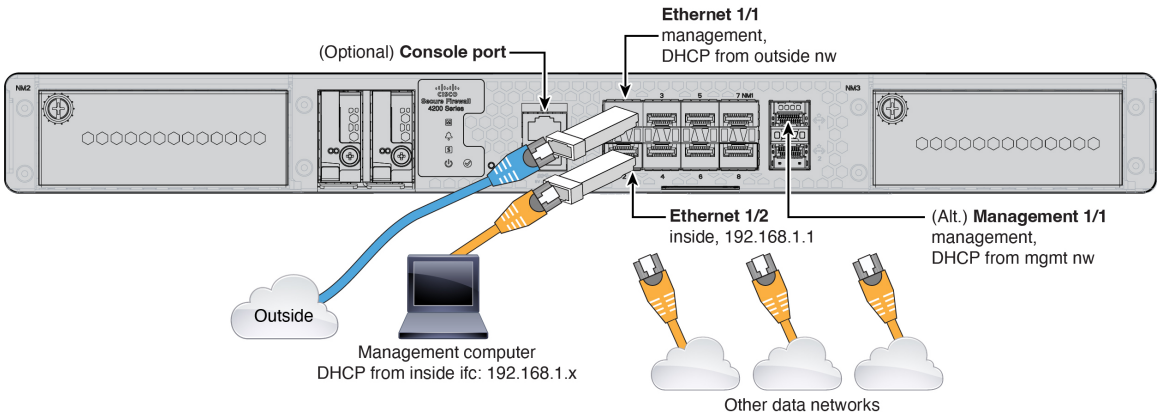
CHAPTER 1

Before You Begin

Configure an ASA using ASDM.

Cable the Firewall

- (Optional) Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.
- Install SFPs into the data interfaces and optional Management ports—The built-in ports are 1/10/25-Gb SFP28 ports that require SFP/SFP+/SFP28 modules.
- See the hardware installation guide for more information.



Power On the Firewall

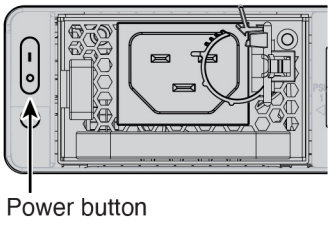
System power is controlled by a rocker power switch located on the rear of the firewall. The rocker power switch provides a soft notification that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Procedure

Step 1 Attach the power cord to the firewall, and connect it to an electrical outlet.

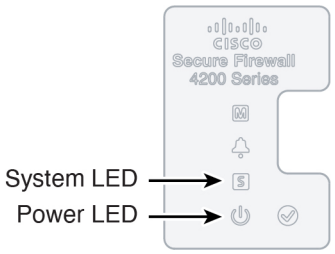
Step 2 Turn the power on using the rocker power switch located on the rear of the chassis, adjacent to the power cord.

Figure 1: Power Button



Step 3 Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

Figure 2: System and Power LEDs



Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

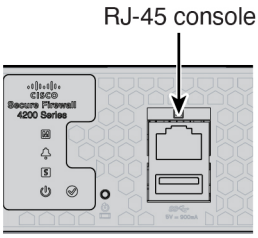
Which Application is Installed: Threat Defense or ASA?

Both applications, threat defense or ASA, are supported on the hardware. Connect to the console port and determine which application was installed at the factory.

Procedure

Step 1 Connect to the console port.

Figure 3: Console Port



Step 2 See the CLI prompts to determine if your firewall is running threat defense or ASA.

Threat Defense

You see the firepower login (FXOS) prompt. You can disconnect without logging in and setting a new password.

```
firepower login:
```

ASA

You see the ASA prompt.

```
ciscoasa>
```

Step 3 If you are running the wrong application, see Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

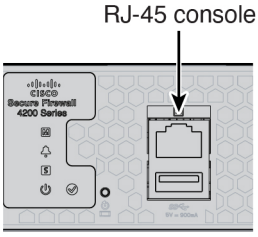
Access the ASA CLI

You might need to access the CLI for configuration or troubleshooting.

Procedure

Step 1 Connect to the console port.

Figure 4: Console Port



Step 2 You connect to the ASA CLI in user EXEC mode. This mode lets you use many **show** commands.

```
ciscoasa>
```

Step 3 Access privileged EXEC mode. This password-protected mode lets you perform many actions, including accessing configuration modes.

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#
```

Step 4 Access global configuration mode.

configure terminal

Example:

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

Step 5 Access the FXOS CLI. Use this CLI for troubleshooting at the hardware level.

connect fxos [**admin**]

- **admin**—Provides admin-level access. Without this option, you have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Example:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Obtain Licenses

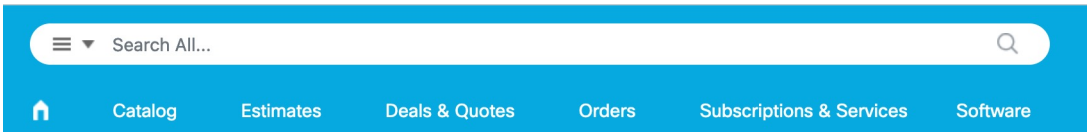
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.

The ASA has the following licenses:

- Essentials—Required
- Security Contexts
- Carrier—Diameter, GTP/GPRS, M3UA, SCTP
- Cisco Secure Client

1. If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

Figure 5: License Search



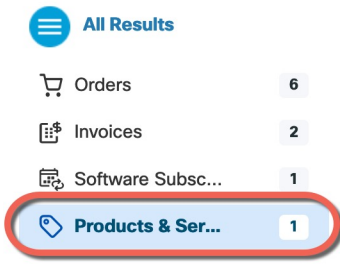
2. Search for the following license PIDs.

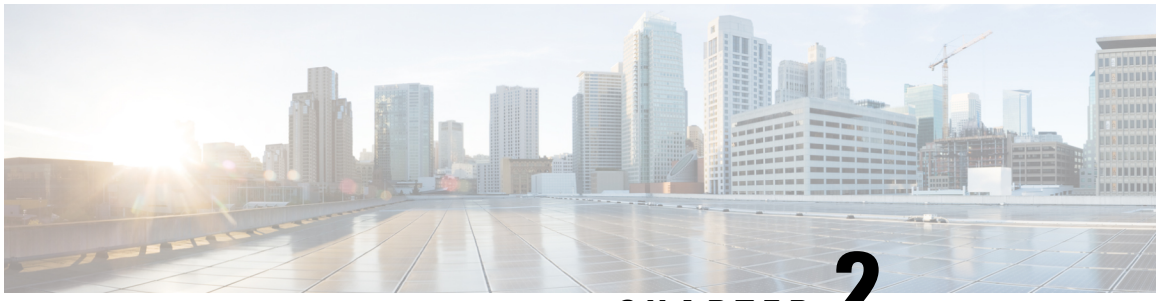
Note If a PID is not found, you can add the PID manually to your order.

- Essentials—*Included automatically*.
- 5 context—L-FPR4200-ASASC-5=. Context licenses are additive; buy multiple licenses.
- 10 context—L-FPR4200-ASASC-10=. Context licenses are additive; buy multiple licenses.
- Carrier (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide. You do not enable this license directly in the ASA.

3. Choose **Products & Services** from the results.

Figure 6: Results





CHAPTER 2

Configure a Basic Policy

Configure licensing and add onto your default configuration using ASDM wizards.

(Optional) Change the IP Address

By default, you can launch ASDM from the following interfaces:

- Ethernet 1/2—192.168.1.1
- Management 1/1—IP address from DHCP

If you cannot use the default IP address, you can set the IP address of the Ethernet 1/2 interface at the ASA CLI.

Procedure

Step 1 Connect to the console port and access global configuration mode. See Access the ASA CLI, on page 3.

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 ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Step 3 Save the default configuration to flash memory.

write memory

Log Into ASDM

Launch ASDM so you can configure the ASA.

Procedure

Step 1 Enter one of the following URLs in your browser.

- **https://192.168.1.1**—Inside (Ethernet 1/2) interface IP address.
- **https://***management_ip*—Management 1/1 interface IP address assigned from DHCP.

Note Be sure to specify **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 **Install ASDM Launcher**.

Step 3 Follow the onscreen instructions to launch ASDM.

The **Cisco ASDM-IDM Launcher** appears.

Step 4 Leave the username and password fields empty, and click **OK**.

The main ASDM window appears.

Configure Licensing

Register the firewall with the Smart Software Manager.

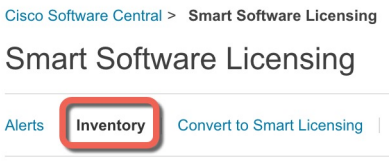
Before you begin

Obtain licenses for your firewall according to Obtain Licenses, on page 5.

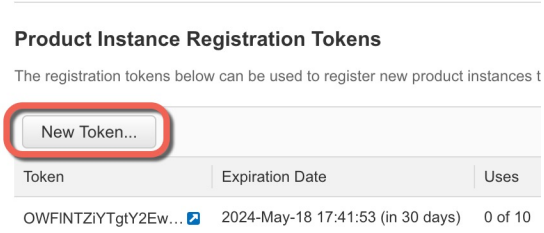
Procedure

Step 1 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

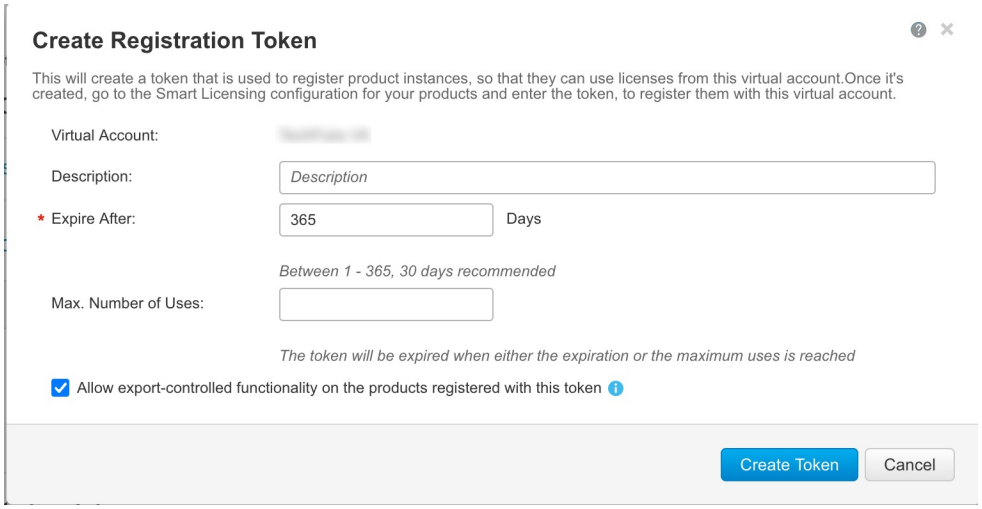
a) Click **Inventory**.



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



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



- **Description**

- **Expire After**—Cisco recommends 30 days.
- **Max. Number of Uses**
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

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 ASA.

Figure 7: View Token

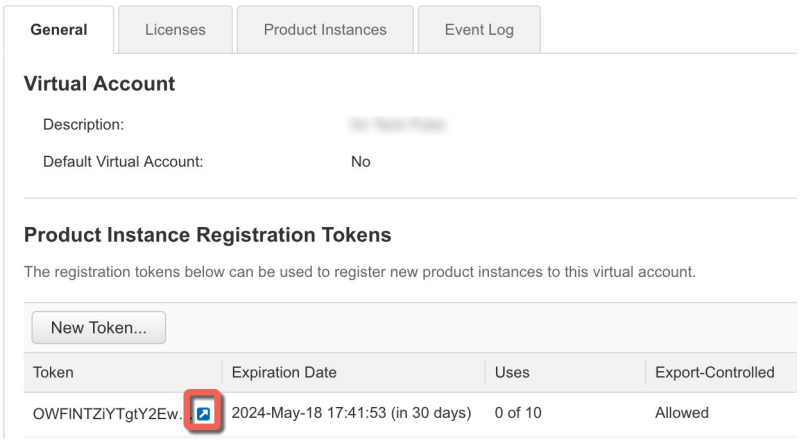
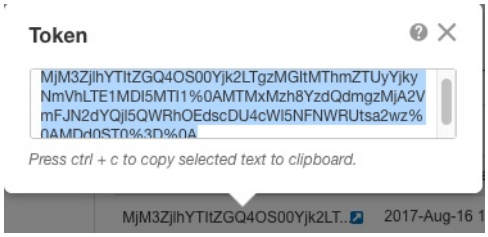


Figure 8: Copy Token



Step 2 In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 3 Set the licensing entitlements.

a) Check **Enable Smart license configuration**.

b) From the **Feature Tier** drop-down list, choose **Essentials**.

Only the Essentials tier is available.

c) (Optional) For the **Context** license, enter the number of contexts.

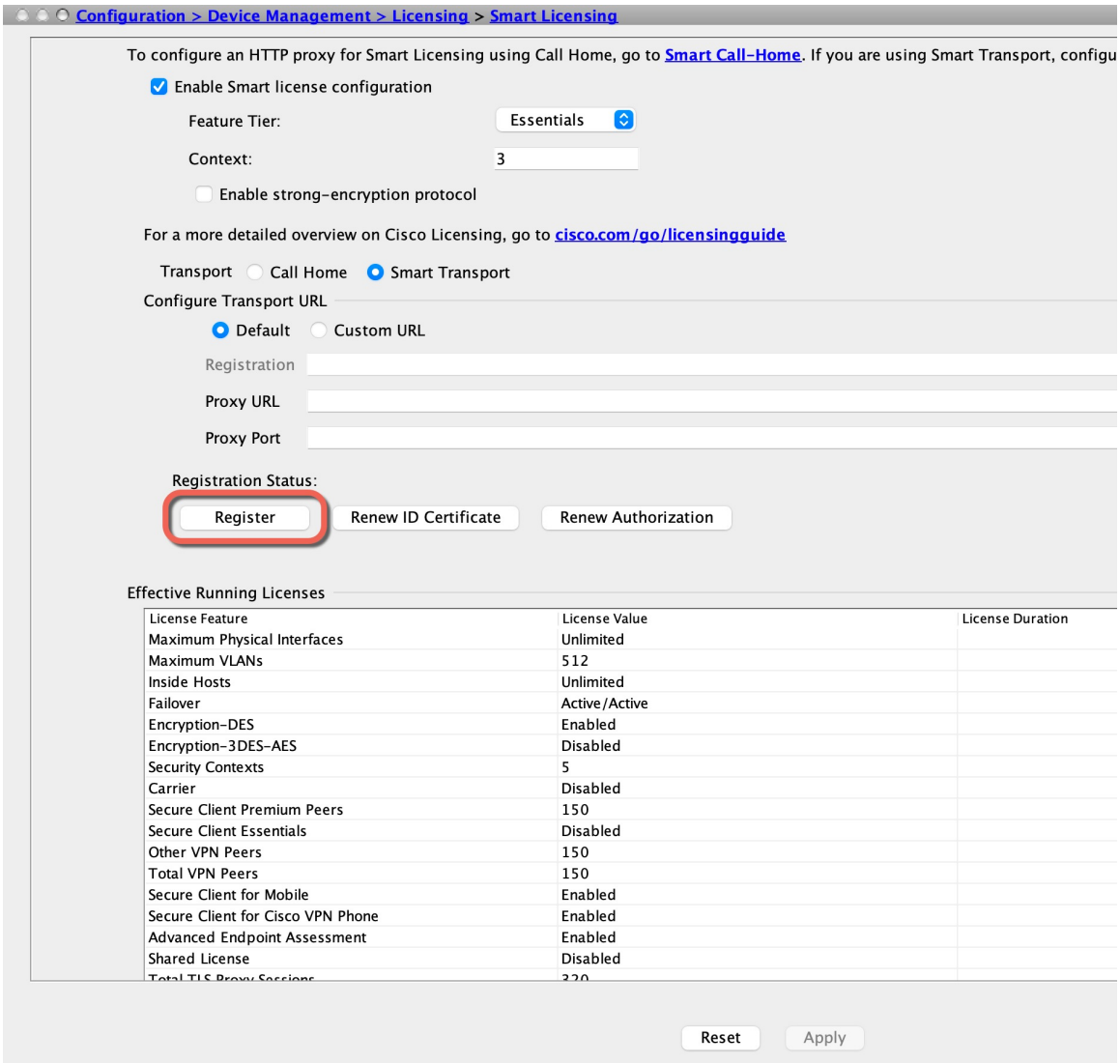
You can use 2 contexts without a license. The maximum number of contexts depends on your model:

- Secure Firewall 4200—100 contexts

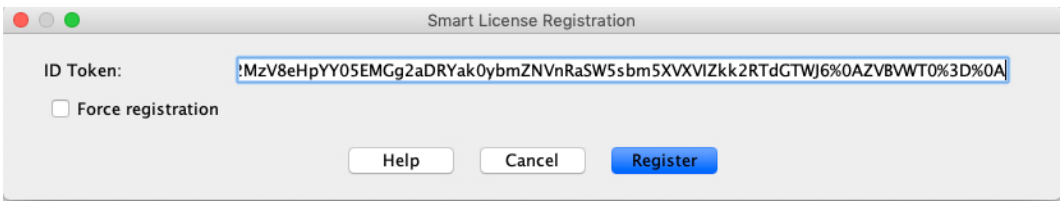
For example, to use the maximum of 100 contexts on the Secure Firewall 4215, enter 98 for the number of contexts; this value is added to the default of 2.

d) (Optional) Check **Enable Carrier** for Diameter, GTP/GPRS, SCTP inspection.
e) Click **Apply**.
f) Click the **Save** icon in the toolbar.

Step 4 Click **Register**.

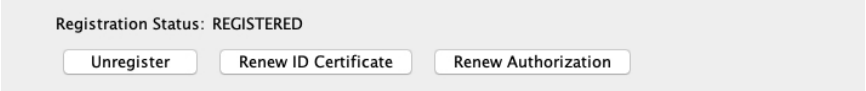


Step 5 Enter the registration token from the Cisco Smart Software Manager in the **ID Token** field.



Step 6 Click **Register**.

ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 7 Quit ASDM and relaunch it.

When you change licenses, you need to relaunch ASDM to show updated screens.

Configure the ASA with the Startup Wizard

Using ASDM, you can use wizards to configure basic and advanced features. The Startup Wizard builds on the default configuration:

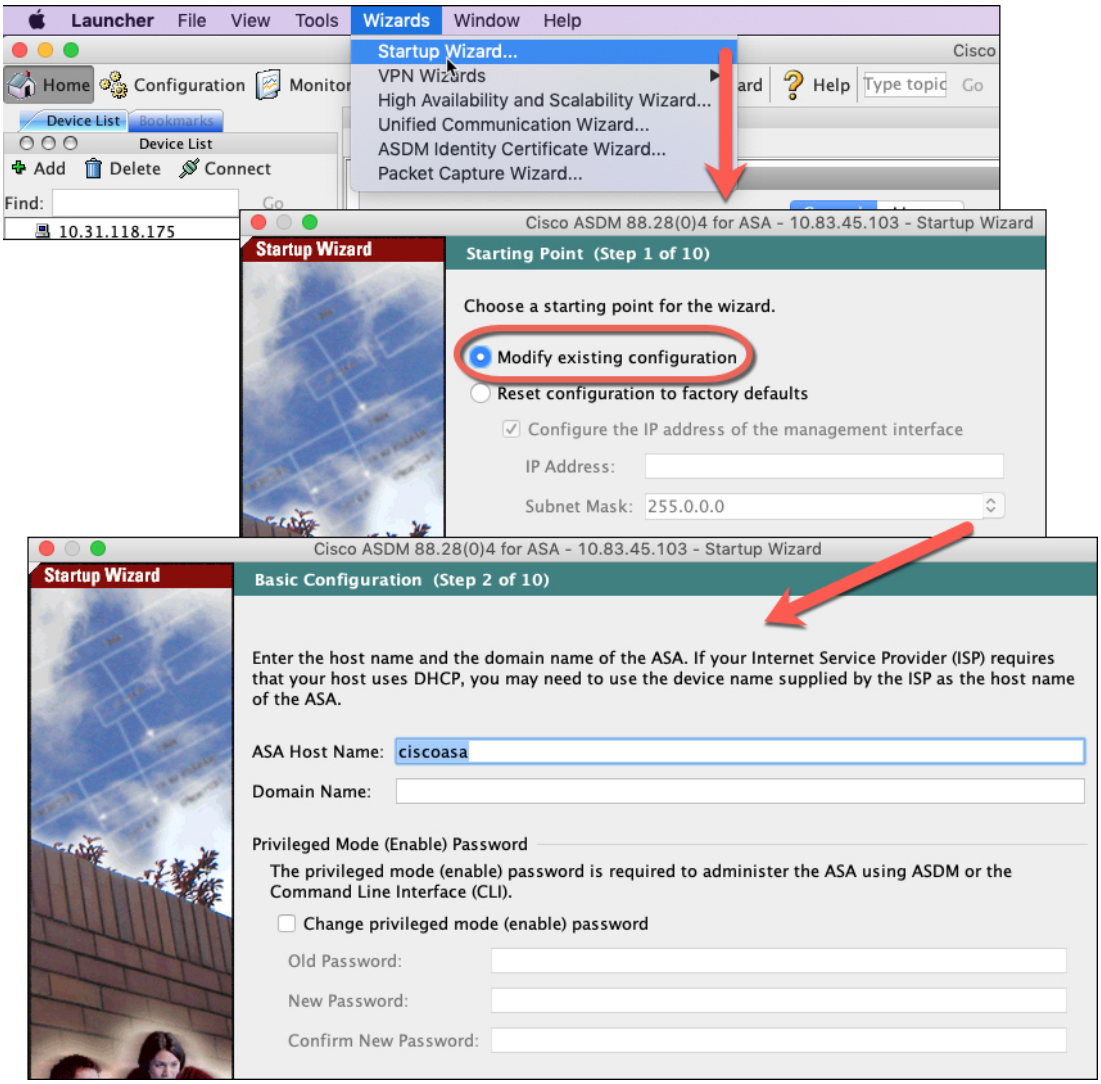
- inside→outside traffic flow
- Interface PAT for all traffic from inside to outside.

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...

Procedure

Step 1 Choose **Wizards > Startup Wizard**, and click the **Modify existing configuration** radio button.



Step 2 Click **Next** on each page to conifgure the features you want.

Step 3 For other wizards, see the ASDM general operations configuration guide.