Secure Firewall 1210/20 ASA Getting Started

Cisco Secure Firewall 1210CE
Updated NaN,

1 Before You Begin

Topics:

- Cable the firewall
- Power on the firewall
- Which application is installed: Firewall Threat Defense or ASA?
- Access the ASA CLI
- Obtain licenses

Check your software version, reimage if necessary, obtain your licenses, and make sure you can connect.

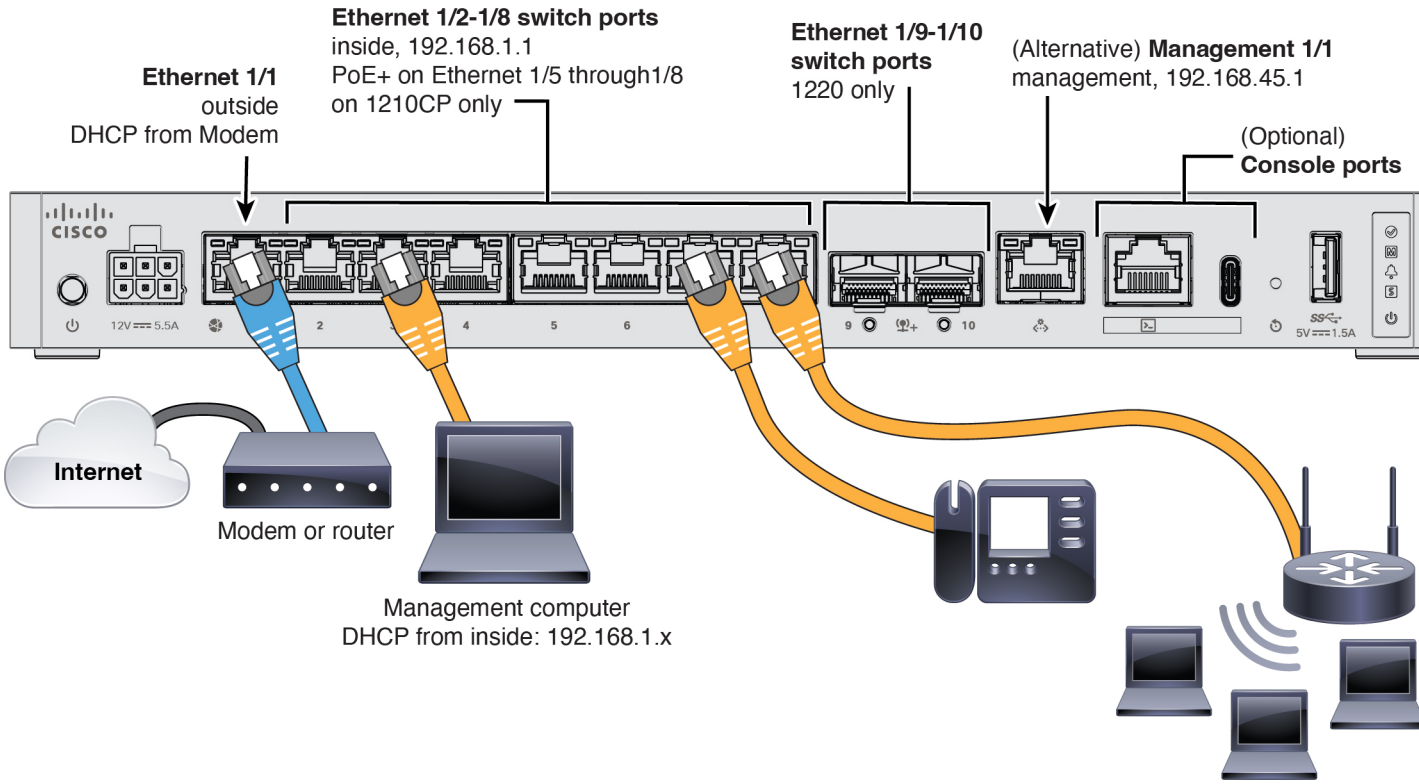
The Secure Firewall 1200 connects and protects the distributed enterprise. It extends Cisco's enterprise security policy and threat inspection to users and devices in branch offices and smaller sites. Powered by an efficient network processor, the Secure Firewall 1200 delivers high levels of security policy and threat defense without compromising user experience.

Configure an ASA using ASDM.

Cable the firewall

Learn how to cable the Secure Firewall 1210/20 so you can complete the initial hardware setup and prepare required ports for network connectivity before configuration.

- For the Secure Firewall 1220, install SFPs into Ethernet 1/9 and 1/10–They are 1/10-Gb SFP+ ports that require SFP/SFP+ modules.
- See the hardware installation guide for more information.



Power on the firewall

How to power on the Secure Firewall 1210/20 and confirm it started successfully by checking the front-panel LEDs for power and system status.

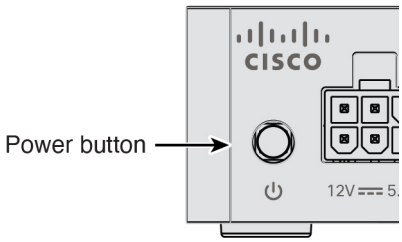
About this task

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

Procedure

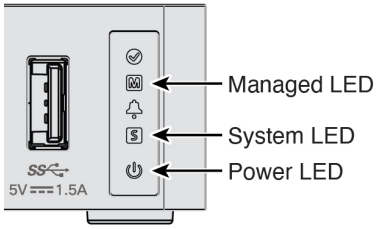
1. Attach the power cord to the firewall, and connect it to an electrical outlet.
2. Turn the power on using the power button located on the rear of the chassis, adjacent to the power cord.

Figure 1: Power button



3. Check the LEDs for the current status.

Figure 2: LEDs



- Power LED–Solid green means the firewall is powered on.
- System (S) LED–See the following behavior:

Table 1: System (S) LED Behavior

LED Behavior	Description	Time After Device Powered On (minutes:seconds)
Fast flashing green	Booting up	01:00
Fast flashing amber (error condition)	Failed to boot up	01:00
Solid green	Application loaded	15:00 - 30:00
Solid amber (error condition)	Application failed to load	15:00 - 30:00

Which application is installed: Firewall Threat Defense or ASA?

Learn how to determine whether your Secure Firewall 1210/20 is running Firewall Threat Defense or ASA by connecting to the console port and identifying the CLI prompt.

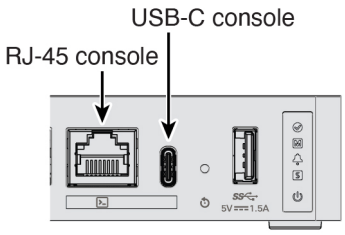
About this task

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

Procedure

1. Connect to the console port using either port type.

Figure 3: Console Port



2. See the CLI prompts to determine if your firewall is running Firewall Threat Defense or ASA.

   Firewall 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>
   ```

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

Access the ASA CLI

How to access the ASA CLI on the Secure Firewall 1210/20 for basic configuration and troubleshooting, including entering privileged EXEC mode and global configuration mode.

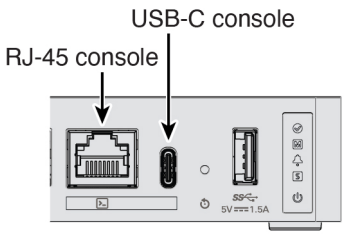
About this task

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

Procedure

1. Connect to the console port using either port type.

   Figure 4: Console Port



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

   ```
   ciscoasa>
   ```

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.

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

4. Access global configuration mode.

   configure terminal

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

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**.

```
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

Learn how to obtain Secure Firewall 1210/20 licenses in Cisco Smart Software Manager and Cisco Commerce Workspace, including identifying required license types and the license PIDs used to order additional entitlements.

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.

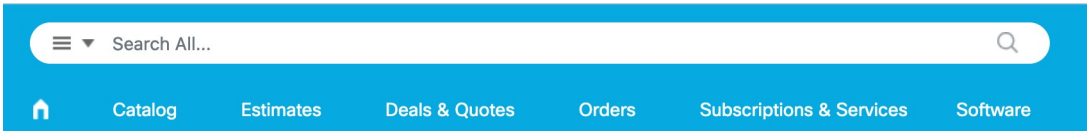
The ASA has the following licenses:

- Essentials—Required
-
- Security Contexts

- Cisco Secure Client

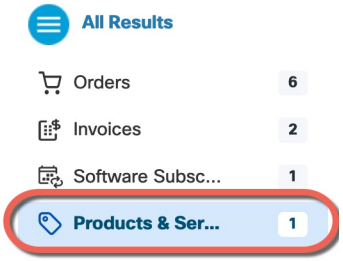
1. If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

   Figure 5: License Search



2. Search for the license PIDs. Check with your ordering guide for the PIDs you want.
3. Choose **Products & Services** from the results.

   Figure 6: Results



2 Configure a Basic Policy

Topics:

- (Optional) Change the IP address
- Log Into ASDM
- Configure licensing
- Configure the ASA with the Startup Wizard

Configure a basic security policy to get your Secure Firewall 1210/20 up and running.

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

(Optional) Change the IP address

How to change the Secure Firewall 1210/20 management IP address when you cannot use the default ASDM addresses, so you can reach ASDM from your network.

About this task

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

- Ethernet 1/2 and higher—192.168.1.1
- Management 1/1—192.168.45.1

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

Procedure

1. Connect to the console port and access global configuration mode. See Access the ASA CLI on page 6.
2. Restore the default configuration with your chosen IP address.

   configure factory-default [*ip_address* [*mask*]]

```
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)#
```

3. Save the default configuration to flash memory.

   write memory

Log Into ASDM

How to log into ASDM on the Secure Firewall 1210/20 using the default HTTPS URL so you can manage and configure ASA through the ASDM interface.

About this task

Launch ASDM so you can configure the ASA.

Procedure

1. Enter one of the following URLs in your browser.
   - **https://192.168.1.1**–Inside interface IP address.You can connect to the inside address on any inside switch port (Ethernet1/2 and higher).
   - **https://192.168.45.1**–Management 1/1 interface IP address.

   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.
2. Click **Install ASDM Launcher**.
3. Follow the onscreen instructions to launch ASDM.

   The **Cisco ASDM-IDM Launcher** appears.
4. Leave the username and password fields empty, and click **OK**.

   The main ASDM window appears.

Configure licensing

Learn how to configure Smart Licensing in ASDM for Secure Firewall 1210/20 by enabling Essentials entitlements and registering the device with a Cisco Smart Software Manager token.

Before you begin

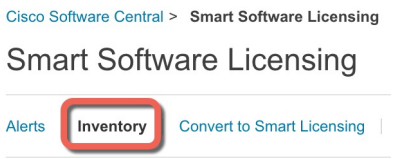
Obtain licenses for your firewall according to Obtain licenses on page 7.

About this task

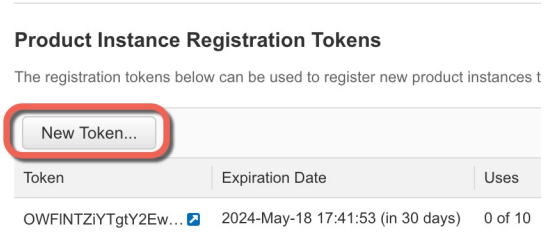
Register the firewall with the Smart Software Manager.

Procedure

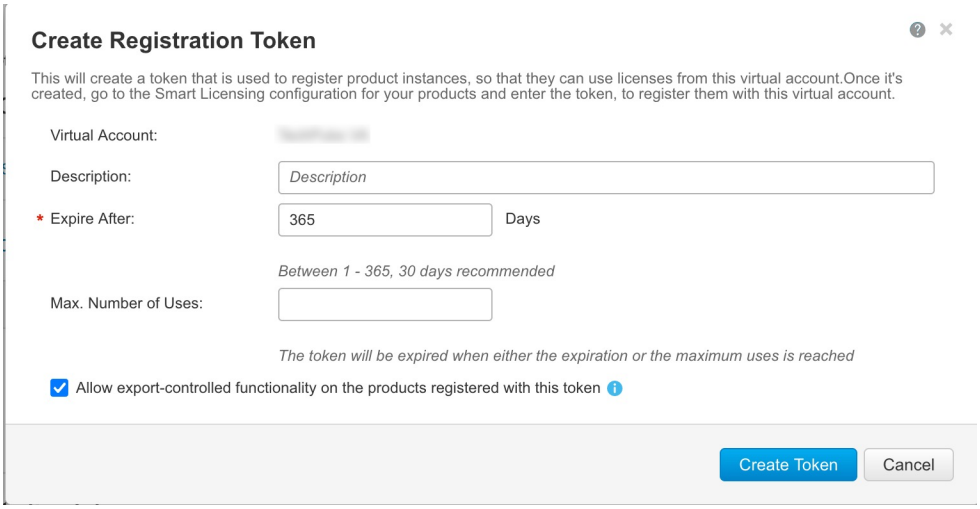
1. In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.
   a) Click **Inventory**.



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

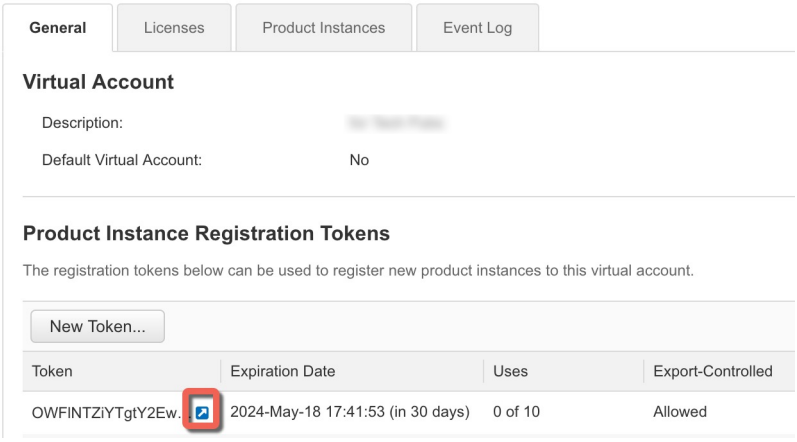
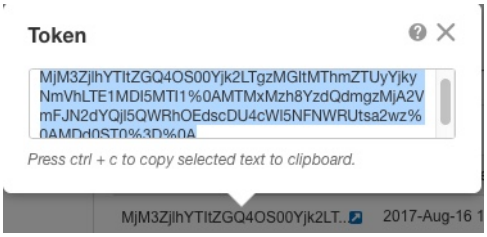


Figure 8: Copy Token



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

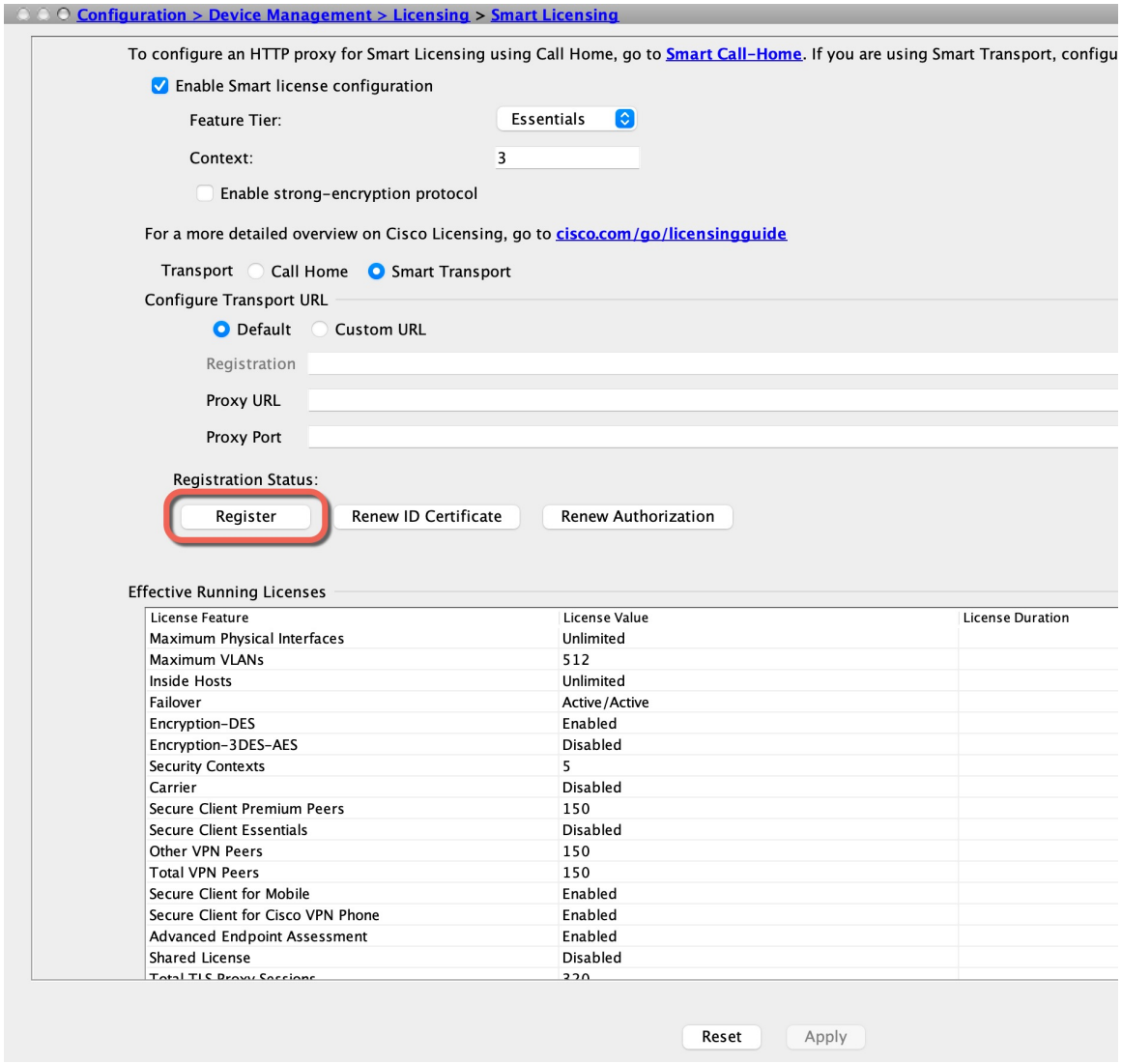
   c) Optional: For the **Context** license, enter the number of contexts.

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

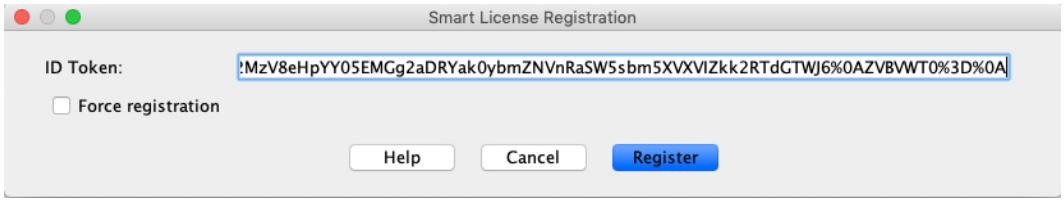
      - Secure Firewall 1210—5 contexts
      - Secure Firewall 1220—10 contexts

      For example, to use the maximum of 10 contexts on the Firepower 1220, enter 8 for the number of contexts; this value is added to the default of 2.

   d) Click **Apply**.
   e) Click the **Save** icon in the toolbar.
4. Click **Register**.

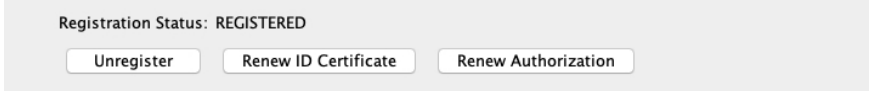


5. Enter the registration token from the Cisco Smart Software Manager in the **ID Token** field.



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.



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

How to use the ASDM Startup Wizard to set up a basic Secure Firewall 1210/20 configuration, including initial interface addressing, routing, and DHCP settings for inside-to-outside connectivity.

About this task

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

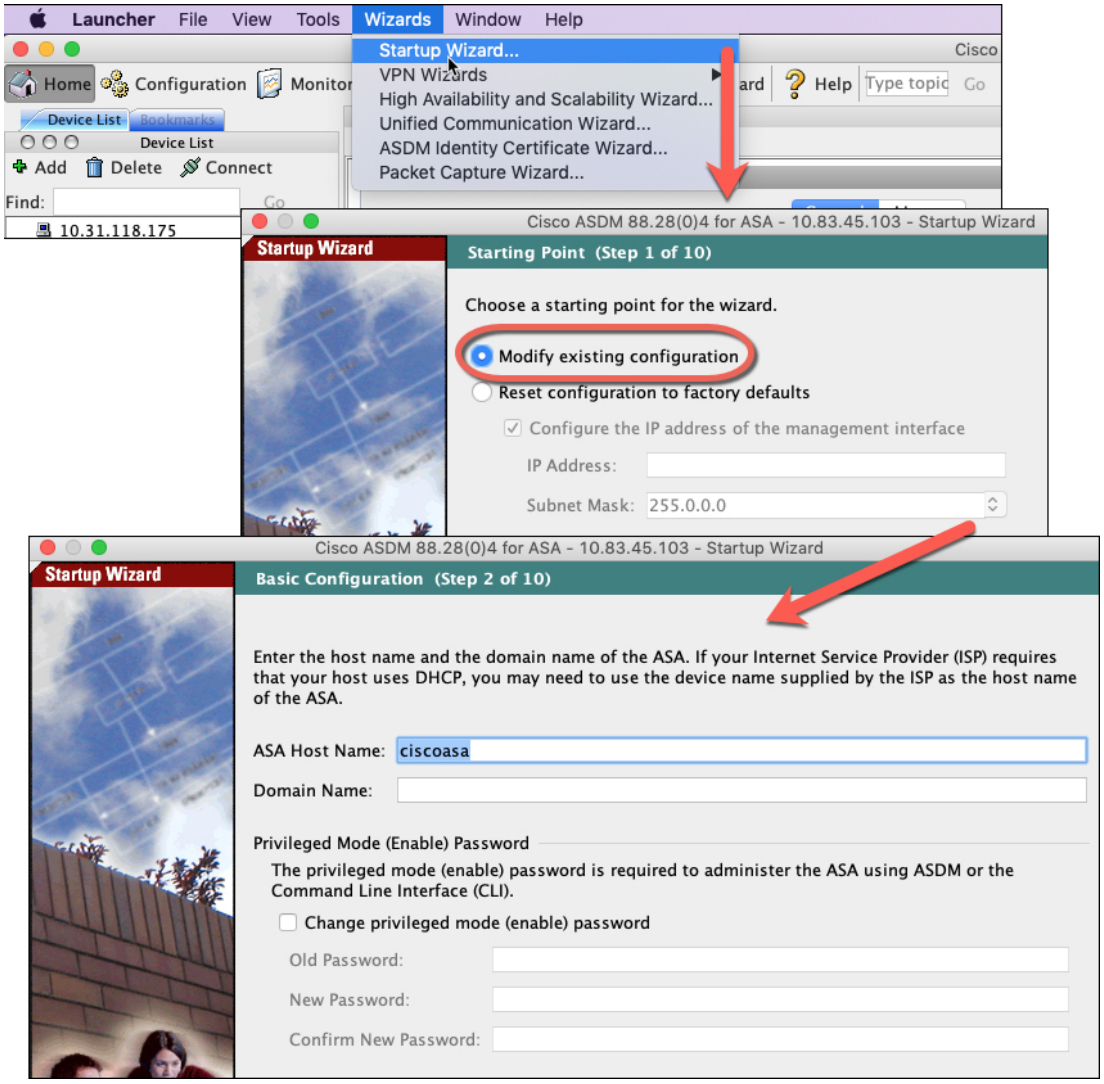
- inside→outside traffic flow
- Interface PAT for all traffic from inside to outside.

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

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



2. Click **Next** on each page to conifgure the features you want.
3. For other wizards, see the ASDM general operations configuration guide.