



ASA Deployment with ASDM

Is This Chapter for You?

To see all available operating systems and managers, see [Which Application and Manager is Right for You?](#). This chapter applies to ASA using ASDM.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See [Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#).

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the [Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense](#) for more information.

Privacy Collection Statement—The firewall 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 1](#)
- [End-to-End Tasks, on page 4](#)
- [Review the Network Deployment and Default Configuration, on page 6](#)
- [Cable the Device, on page 9](#)
- [Power On the Firewall, on page 10](#)
- [\(Optional\) Change the IP Address, on page 11](#)
- [Log Into ASDM, on page 12](#)
- [Configure Licensing, on page 13](#)
- [Configure the ASA, on page 18](#)
- [Access the ASA and FXOS CLI, on page 20](#)
- [What's Next?, on page 21](#)

About the ASA

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

Unsupported Features

General ASA Unsupported Features

The following ASA features are not supported on the Firepower 1010:

- Multiple context mode
- Active/Active failover
- Redundant interfaces
- Clustering
- ASA REST API
- ASA FirePOWER module
- Botnet Traffic Filter
- The following inspections:
 - SCTP inspection maps (SCTP stateful inspection using ACLs is supported)
 - Diameter
 - GTP/GPRS

VLAN Interface and Switch Port Unsupported Features

VLAN interfaces and switch ports do not support:

- Dynamic routing
- Multicast routing
- Policy based routing
- Equal-Cost Multi-Path routing (ECMP)
- Inline sets or Passive interfaces
- VXLAN
- EtherChannels
- Failover and state link
- Traffic zones
- Security group tagging (SGT)

Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Firepower 1010. However, you will need to modify your configuration. Also note some behavioral differences between the platforms.

1. To copy the configuration, enter the **more system:running-config** command on the ASA 5500-X.

2. Edit the configuration as necessary (see below).
3. Connect to the console port of the Firepower 1010, and enter global configuration mode:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Clear the current configuration using the **clear configure all** command.
5. Paste the modified configuration at the ASA CLI.

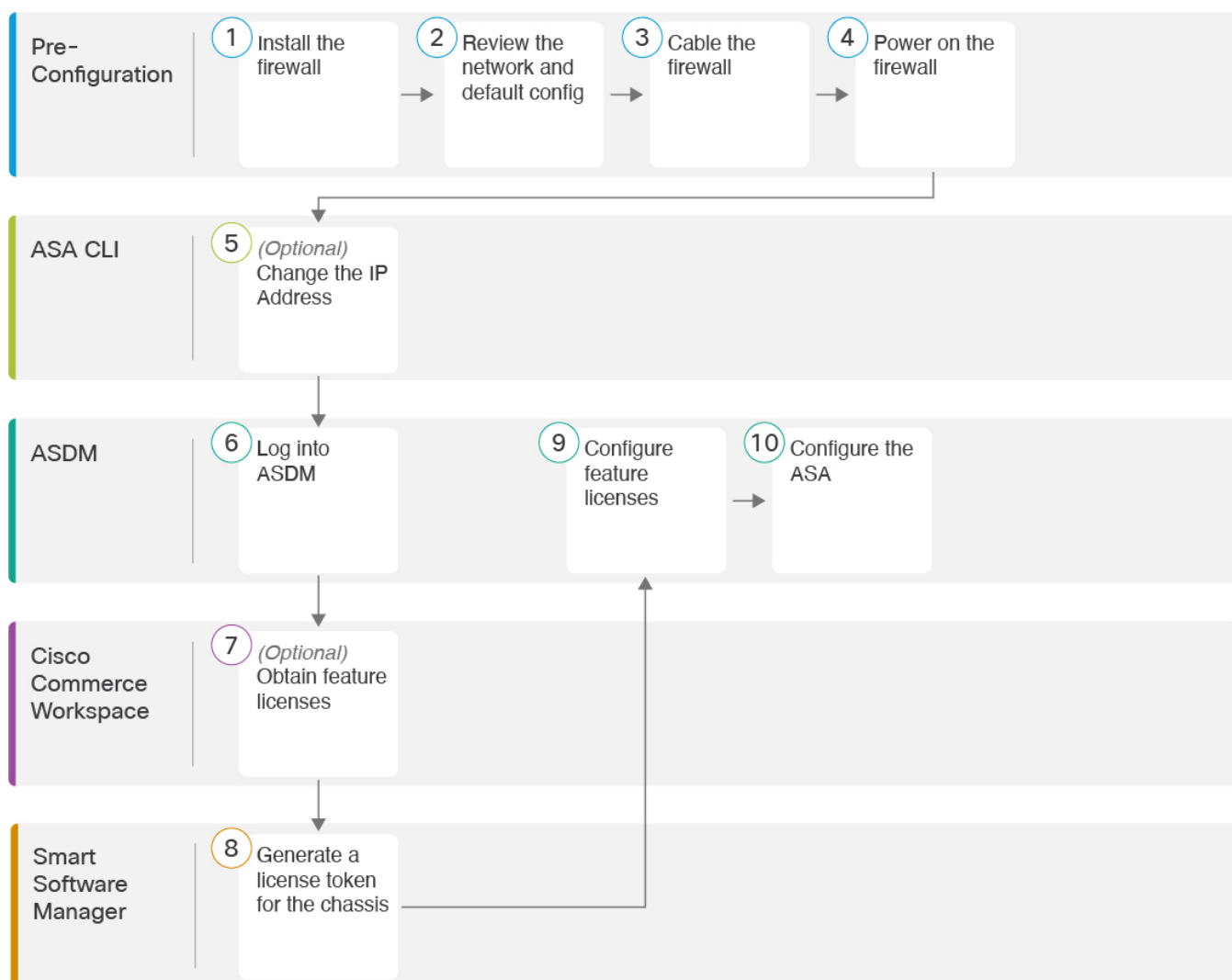
This guide assumes a factory default configuration, so if you paste in an existing configuration, some of the procedures in this guide will not apply to your ASA.

ASA 5500-X Configuration	Firepower 1010 Configuration
Ethernet 1/2 through 1/8 firewall interfaces	<p>Ethernet 1/2 through 1/8 switch ports</p> <p>These Ethernet ports are configured as switch ports by default. For each interface in your configuration, add the no switchport command to make them regular firewall interfaces. For example:</p> <pre>interface ethernet 1/2 no switchport ip address 10.8.7.2 255.255.255.0 nameif inside</pre>
PAK License	<p>Smart License</p> <p>PAK licensing is not applied when you copy and paste your configuration. There are no licenses installed by default. Smart Licensing requires that you connect to the Smart Licensing server to obtain your licenses. Smart Licensing also affects ASDM or SSH access (see below).</p>
Initial ASDM access	<p>Remove any VPN or other strong encryption feature configuration—even if you only configured weak encryption—if you cannot connect to ASDM or register with the Smart Licensing server.</p> <p>You can reenable these features after you obtain the Strong Encryption (3DES) license.</p> <p>The reason for this issue is that the ASA includes 3DES capability by default for management access only. If you enable a strong encryption feature, then ASDM and HTTPS traffic (like that to and from the Smart Licensing server) are blocked. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected.</p>

ASA 5500-X Configuration	Firepower 1010 Configuration
Interface IDs	Make sure you change the interface IDs to match the new hardware IDs. For example, the ASA 5525-X includes Management 0/0, and GigabitEthernet 0/0 through 0/5. The Firepower 1120 includes Management 1/1 and Ethernet 1/1 through 1/8.
boot system commands The ASA 5500-X allows up to four boot system commands to specify the booting image to use.	The Firepower 1010 only allows a single boot system command, so you should remove all but one command before you paste. You actually do not need to have <i>any</i> boot system commands present in your configuration, as it is not read at startup to determine the booting image. The last-loaded boot image will always run upon reload. The boot system command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA.

End-to-End Tasks

See the following tasks to deploy and configure the ASA.



1	Pre-Configuration	Install the firewall. See the hardware installation guide .
2	Pre-Configuration	Review the Network Deployment and Default Configuration , on page 6.
3	Pre-Configuration	Cable the Device , on page 9.
4	Pre-Configuration	Power On the Firewall
5	ASA CLI	(Optional) Change the IP Address , on page 11.
6	ASDM	Log Into ASDM , on page 12.

7	Cisco Commerce Workspace	Configure Licensing, on page 13 : Obtain feature licenses.
8	Smart Software Manager	Configure Licensing, on page 13 : Generate a license token for the chassis.
9	ASDM	Configure Licensing, on page 13 : Configure feature licenses.
10	ASDM	Configure the ASA, on page 18 .

Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the ASA using the default configuration.

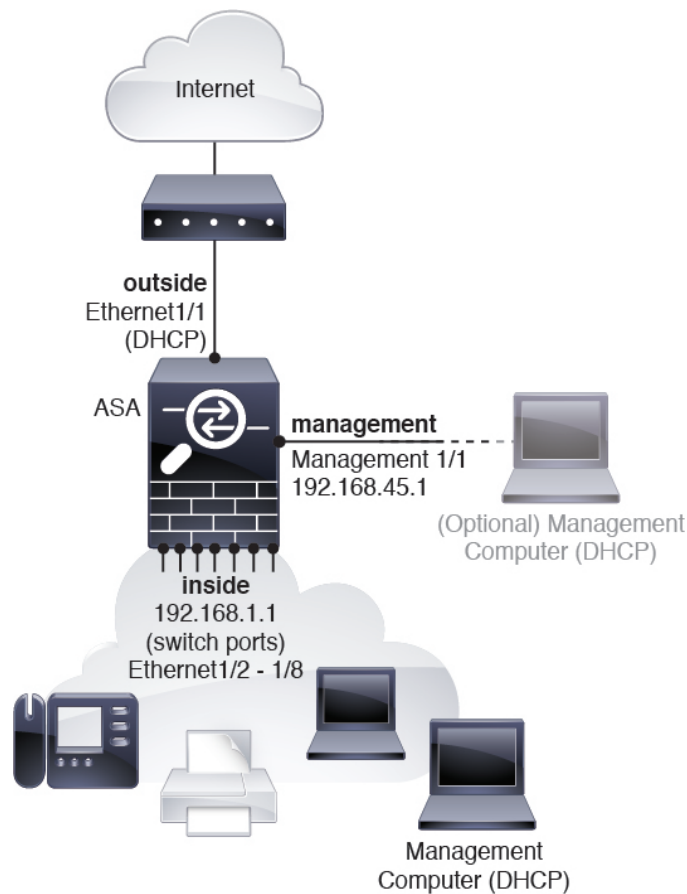
If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of the ASDM Startup Wizard.



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 11](#).

If you need to change the inside IP address, you can do so using the ASDM Startup Wizard. For example, you may need to change the inside IP address in the following circumstances:

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



Firepower 1010 Default Configuration

The default factory configuration for the Firepower 1010 configures the following:

- **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
- **inside→outside** traffic flow—Ethernet 1/1 (outside), VLAN1 (inside)
- **management**—Management 1/1 (management), IP address 192.168.45.1
- **outside IP address** from DHCP, inside IP address—192.168.1.1
- **DHCP server** on inside interface, management interface
- **Default route** from outside DHCP
- **ASDM access**—Management and inside hosts allowed. Management hosts are limited to the 192.168.45.0/24 network, and inside hosts are limited to the 192.168.1.0/24 network.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **DNS servers**—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```

interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
management-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface

```

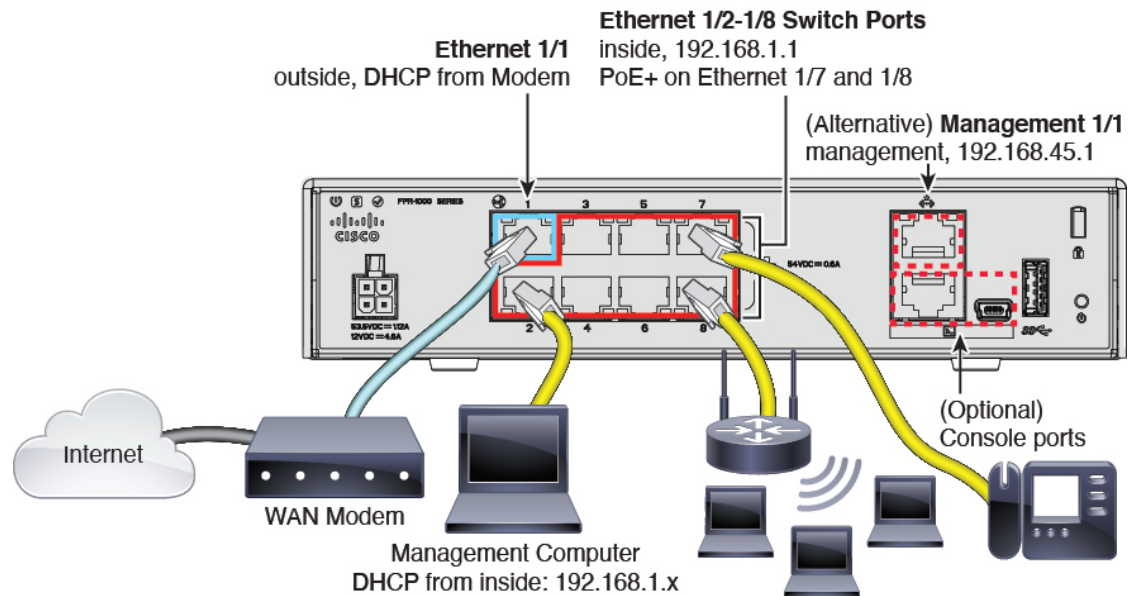


```

!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!

```

Cable the Device



Manage the Firepower 1010 on either Management 1/1, or on Ethernet 1/2 through 1/8 (inside switch ports). The default configuration also configures Ethernet 1/1 as outside.

Procedure

- Step 1** Install the chassis. See the [hardware installation guide](#).
- Step 2** Connect your management computer to one of the following interfaces:
 - **Ethernet 1/2 through 1/8**—The inside interface 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 [Firepower 1010 Default Configuration, on page 7](#)).

- **Management 1/1**—Management 1/1 has a default IP address (192.168.45.1) 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 management network settings (see [Firepower 1010 Default Configuration, on page 7](#)). Only clients on 192.168.45.0/24 can access the ASA.

If you need to change the Management 1/1 IP address from the default, you must also cable your management computer to the console port. See [\(Optional\) Change the IP Address, on page 11](#).

Step 3 Connect the outside network to the Ethernet 1/1 interface.
For Smart Software Licensing, the ASA needs internet access.

Step 4 Connect inside devices to the remaining inside switch ports, Ethernet 1/2 through 1/8.
Ethernet 1/7 and 1/8 are PoE+ ports.

Note PoE is not supported on the Firepower 1010E.

Power On the Firewall

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



Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

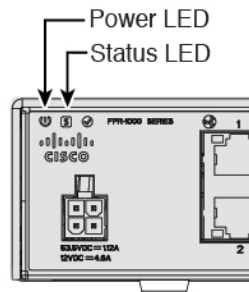
Before you begin

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

Procedure

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

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



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

(Optional) Change 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 and FXOS CLI, on page 20](#) 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 ASDM

Launch ASDM so you can configure the ASA.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.



Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

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**—Inside interface IP address. You can connect to the inside address on any inside switch port (Ethernet1/2 through 1/8).
- **https://192.168.45.1**—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 **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

The ASA uses Smart Licensing. You can use regular Smart Licensing, which requires internet access; or for offline management, you can configure Permanent License Reservation or a Smart Software Manager On-Prem (formerly known as a Satellite server). For more information about these offline licensing methods, see [Cisco ASA Series Feature Licenses](#); this guide applies to regular Smart Licensing.

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

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the firewall and the Smart Software Manager. It also assigns the firewall to the appropriate virtual account. Until you register with the Smart Software Manager, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. Licensed features include:

- Essentials
- Security Plus—For Active/Standby failover
- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.
- Cisco Secure Client—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.



Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

When you request the registration token for the ASA from the Smart Software Manager, check the **Allow export-controlled functionality on the products registered with this token** check box so that the full Strong Encryption license is applied (your account must be qualified for its use). The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the chassis, so no additional action is required. If your Smart Account is not authorized for strong encryption, but Cisco has

determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

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

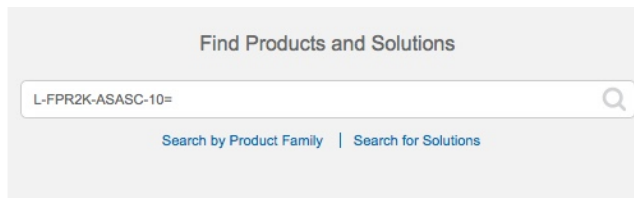
Procedure

Step 1

Make sure your Smart Licensing account contains the available licenses you need, including at a minimum the Essentials license.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software Manager 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 1: License Search



- Essentials license—L-FPR1000-ASA=. The Essentials license is free, but you still need to add it to your Smart Software Licensing account.
- Security Plus license—L-FPR1010-SEC-PL=. The Security Plus license enables failover.
- Strong Encryption (3DES/AES) license—L-FPR1K-ENC-K9=. Only required if your account is not authorized for strong encryption.
- Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#). You do not enable this license directly in the ASA.

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.

- Click **Inventory**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts **Inventory** License Conversion Reports Email Notification Satellites Activity

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

The screenshot shows the 'Product Instance Registration Tokens' section in the ASA configuration interface. The 'New Token...' button is highlighted with a red circle. Below the button is a table with the following data:

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 'Create Registration Token' dialog box is shown. The 'Description' field is highlighted with a blue border. The 'Expire After' field is set to 30 days. 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.

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 2: View Token

General | Licenses | Product Instances | Event Log

Virtual Account

Description: Product Instance

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
MjM3ZjYhYTItZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed		Actions

Figure 3: Copy Token

Token

MjM3ZjYhYTItZGQ4OS00Yjk2LTg2MGlhMTMhZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEpscDU4cWI5NFNWRUtsa2wz%0AMDMhST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjYhYTItZGQ4OS00Yjk2LT... 2017-Aug-16 1

Step 3 In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 4 Click **Register**.

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

☐ Enable Smart license configuration

Feature Tier:

Throughput Level:

Privacy ☐ Host Name ☐ Version

Transport ☒ Call Home ☐ Smart Transport

Configure Transport URL

☒ Default ☐ URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

☐ Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

License Feature	License Value
Maximum VLANs	200
Inside Hosts	Unlimited
Failover	Active/Active
Encryption-DES	Enabled
Encryption-3DES-AES	Enabled
Security Contexts	2
Carrier	Disabled

Step 5 Enter the registration token in the **ID Token** field.

Smart License Registration

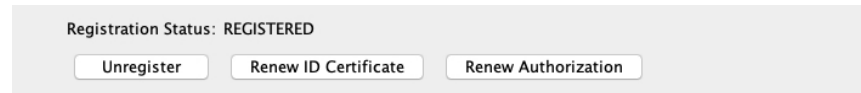
ID Token:

☐ Force registration

You can optionally check the **Force registration** check box to register the ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6 Click **Register**.

The ASA registers with the Smart Software Manager using the pre-configured outside interface, and requests authorization for the configured license entitlements. The Smart Software Manager also applies the Strong Encryption (3DES/AES) license if your account allows. 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**

Set the following parameters:

- a) Check **Enable Smart license configuration**.
- b) From the **Feature Tier** drop-down list, choose **Essentials**.
Only the Essentials tier is available.
- c) (Optional) Check **Enable Security Plus**.

The Security Plus tier enables Active/Standby failover.

Step 8

Click **Apply**.

Step 9

Click the **Save** icon in the toolbar.

Step 10

Quit ASDM and relaunch it.

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

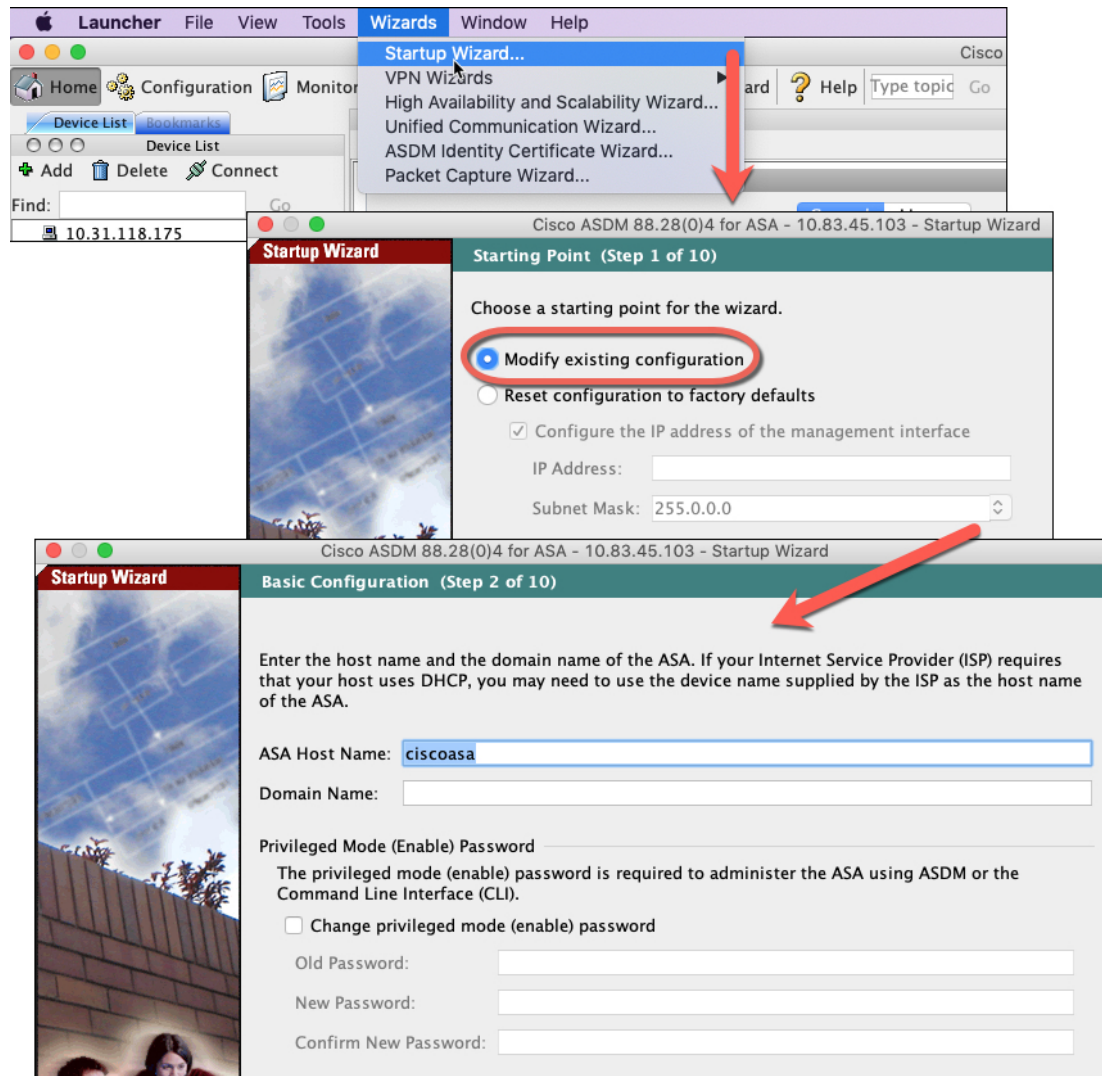
Configure the ASA

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards.

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 and FXOS CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting to the console port. You can later configure SSH access to the ASA on any interface; SSH access is disabled by default. See the [ASA general operations configuration guide](#) for more information.

You can also access the FXOS CLI from the ASA CLI for troubleshooting purposes.

Procedure

Step 1 Connect your management computer to the console port. Be sure to install any necessary 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#
```

The enable password that you set on the ASA is also the FXOS **admin** user password if the ASA fails to boot up, and you enter FXOS failsafe mode.

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

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

Step 3 Access global configuration mode.

configure terminal

Example:

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

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

Step 4 (Optional) Connect to the FXOS CLI.

connect fxos [admin]

- **admin**—Provides admin-level access. Without this option, users 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**.

Within FXOS, you can view user activity using the **scope security/show audit-logs** command.

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#
```

What's Next?

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

