cisco.



Firepower 1010 ASA Getting Started

First Published: 2024-10-16 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



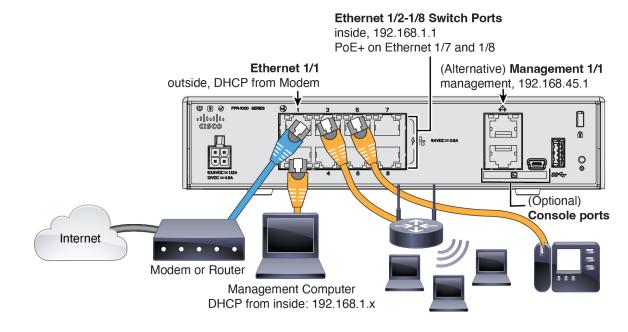
Before You Begin

Configure an ASA using ASDM.

- Cable the Firewall, on page 1
- Power On the Firewall, on page 1
- Which Application is Installed: Threat Defense or ASA?, on page 2
- Access the ASA CLI, on page 3
- Obtain Licenses, on page 4

Cable the Firewall

See the hardware installation guide for more information.



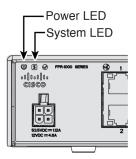
Power On the Firewall

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

Procedure

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

Step 2Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.Figure 1: System and Power LEDs



Step 3 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

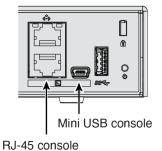
Which Application is Installed: Threat Defense or ASA?

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 using either port type.

Figure 2: 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.

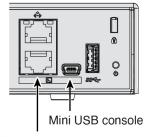
Access the ASA CLI

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

Procedure

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

Figure 3: Console Port



RJ-45 console

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 Plus—For Active/Standby failover
- Cisco Secure Client
- 1. If you need to add licenses yourself, go to Cisco Commerce Workspace and use the Search All field.

Figure 4: License Search

Envoices

Software Subsc...

Products & Ser...

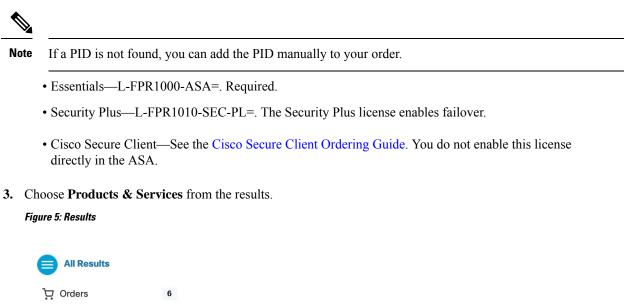
2

1

1

≡▼	Search All					Q
n	Catalog	Estimates	Deals & Quotes	Orders	Subscriptions & Services	Software

2. Search for the following license PIDs.





Configure a Basic Policy

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

- (Optional) Change the IP Address, on page 7
- Log Into ASDM, on page 8
- Configure Licensing, on page 9
- Configure the ASA with the Startup Wizard, on page 12

(Optional) Change the IP Address

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

- Ethernet 1/2 through Ethernet 1/8—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

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 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: no shutdown
Executing command: http server enable
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 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 1/1 interface IP address. 							
	Note	Be sure to specify ht	ttps://.					
	The Cisco ASDM web page appears. You may see browser security warnings because the ASA does not have a certificat installed; you can safely ignore these warnings and visit the web page.							
Step 2	Click Install ASD	OM Launcher.						
Step 3	Follow the onscre	en instructions to launch ASDM.						
	The Cisco ASDM	I-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 4.

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.

Cisco Software Central > Smart Software Licensing Smart Software Licensing



b) On the General tab, click New Token.

Product Instance Registration Tokens
The registration tokens below can be used to register new product instances t
New Token...
Token Expiration Date Uses

OWFINTZiYTgtY2Ew... 2024-May-18 17:41:53 (in 30 days) 0 of 10

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

Create Registration	Token			?	×		
This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.							
Virtual Account:							
Description:	Description						
* Expire After:	365	Days					
Max. Number of Uses:	Between 1 - 365, 30 d	days recommended	ximum uses is reached				
Allow export-controlled fur		s registered with this token 🕧					
			Create Token Ca	ncel			

• 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 6: View Token

Virtual Accou	nt				
Descriptions					
Description:					
Default Virtual A	ccount:	No			
he registration tok	ens below	can be used to register new prod	uct instance	s to this virtual	account.
New Token	ens below			s to this virtual	
New Token	ens below	can be used to register new prod Expiration Date	uct instance: Uses	s to this virtual	account.
			Uses		

- MjM3ZjihYTItZGQ4OS00Yjk2LT... 2017-Aug-16
- **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.

Press ctrl + c to copy selected text to clipboard.

c) (Optional) Check the **Enable Security Plus** check box.

The Security Plus tier enables failover.

- d) Click Apply.
- e) Click the Save icon in the toolbar.

Step 4 Click Register.

	Fo configure an HTTP proxy for Smart Licensing	using Call Home, go to Smart Call-Home. If yo	ou are using Smart Transport, config
	✓ Enable Smart license configuration		
	Feature Tier:	Essentials 📀	
	Context:	3	
	Enable strong-encryption protocol		
	For a more detailed overview on Cisco Licensi	ng, go to <u>cisco.com/go/licensingguide</u>	
	Transport Call Home O Smart Trans	port	
	O Default O Custom URL		
	Registration		
	Proxy URL		
	Proxy Port		
	Register Renew ID Certifica	te Renew Authorization	
- F	ffective Running Licenses		
E	Effective Running Licenses	License Value	License Duration
E	License Feature	License Value Unlimited	License Duration
E		License Value Unlimited 512	License Duration
E	License Feature Maximum Physical Interfaces	Unlimited	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs	Unlimited 512	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts	Unlimited 512 Unlimited	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES	Unlimited 512 Unlimited Active /Active Enabled Disabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-JDES-AES Security Contexts	Unlimited 512 Unlimited Active/Active Enabled Disabled 5	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier	Unlimited 512 Unlimited Active/Active Enabled Disabled 5 Disabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-JDES-AES Security Contexts Carrier Secure Client Premium Peers	Unlimited 512 Unlimited Active/Active Enabled Disabled 5 Disabled 150	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials	Unlimited 512 Unlimited Active / Active Enabled Disabled 5 Disabled 150 Disabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-JDES Encryption-JDES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials Other VPN Peers	Unlimited 512 Unlimited Active /Active Enabled Disabled 5 Disabled 150 Disabled 150	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials	Unlimited 512 Unlimited Active / Active Enabled Disabled 5 Disabled 150 Disabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers	Unlimited512UnlimitedActive /ActiveEnabledDisabledSDisabled150150150	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers Secure Client for Mobile	Unlimited\$12UnlimitedActive/ActiveEnabledDisabled5Disabled150150150Enabled150Enabled150Enabled150Enabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers Secure Client for Mobile Secure Client for Cisco VPN Phone	Unlimited\$12UnlimitedActive/ActiveEnabledDisabled5Disabled150Disabled150Enabled150EnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-3DES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers Secure Client for Mobile Secure Client for Cisco VPN Phone	Unlimited\$12UnlimitedActive/ActiveEnabledDisabled5Disabled150Disabled150Enabled150EnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabledEnabled	License Duration
E	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-JES Encryption-JES Encryption-JDES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers Total VPN Peers Secure Client for Mobile Secure Client for Cisco VPN Phone Advanced Endpoint Assessment Shared License	Unlimited 512 Unlimited Active / Active Enabled Disabled 5 Disabled 150 Disabled 150 Enabled 150 Enabled Enabled Enabled Disabled Disabled	
	License Feature Maximum Physical Interfaces Maximum VLANs Inside Hosts Failover Encryption-DES Encryption-JDES-AES Security Contexts Carrier Secure Client Premium Peers Secure Client Premium Peers Secure Client Essentials Other VPN Peers Total VPN Peers Secure Client for Mobile Secure Client for Cisco VPN Phone Advanced Endpoint Assessment Shared License Total TLS Prove Sections	Unlimited 512 Unlimited Active/Active Enabled Disabled 5 Disabled 150 Disabled 150 Enabled Enabled Enabled Disabled 220	у

ID Token:	!MzV8eHpYY05EMGg2aDRYak0ybmZNVnRaSW5sbm5XVXVIZkk2RTdGTWJ6%0AZVBVWT0%3D%0A
Force registration	
	Help Cancel Register

Step 6 Click Register.

.

Step 5

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.

Unregister Renew ID Certificate Renew Authorization

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.

Ś	Launcher	File	View	Tools	Wizards	Window I	Help			
	evice List Bo	okmarks vice List		Monitor	VPN Wi High Av Unified ASDM I	ailability and Communicat	Scalability Wiza ion Wizard ïicate Wizard ard	rd	? Help Type	Cisco e topic Go
	10.31.118.1	75		0		Cis	sco ASDM 88.28(0)4 for ASA	- 10.83.45.103	3 - Startup Wizard
					ASDM 88.	Choose a s Modify Reset Co IP / Sul 28(0)4 for AS	Noint (Step 1 of starting point for y existing config configuration to onfigure the IP ad Address: bnet Mask: 255. SA - 10.83.45.103	r the wizard. uration factory defa ldress of the	ults • management i	nterface
S	tartup Wizard		Bas	ic Config	uration ((tep 2 of 10				
		C	that of the ASA	: your hos he ASA.	ne: cisco	CP, you may i				ovider (ISP) requires e ISP as the host name
(W.F										
	come .	s and all				Password -				
					ged mode Line Interf		word is required	to administe	er the ASA usin	g ASDM or the
1	44	Щ	0	Old Pass		l mode (enab	le) password			
1	T	IT	T	New Pass	sword:					
	-	3	T		New Passv	ord:				

- **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.

I

 $^{\odot}$ 2024 Cisco Systems, Inc. All rights reserved.