Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide

First Published: 2014-01-01

Last Modified: 2024-07-09

Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide

This guide describes how to reimage between the Secure Firewall ASA and Secure Firewall Threat Defense (formerly Firepower Threat Defense), and also how to perform a reimage for the threat defense using a new image version; this method is distinct from an upgrade, and sets the threat defense to a factory default state. For ASA reimaging, see the ASA general operations configuration guide, where you can use multiple methods to reimage the ASA.

Supported Models

The following models support either ASA software or threat defense software. For ASA and threat defense version support, see the ASA compatibility guide or Cisco Secure Firewall Threat Defense Compatibility Guide.

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000
- ASA 5506-X, 5506W-X, and 5506H-X (Threat Defense 6.2.3 and earlier; ASA 9.16 and earlier)
- ASA 5508-X (threat defense 7.0 and earlier; ASA 9.16 and earlier)
- ASA 5512-X (threat defense 6.2.3 and earlier; ASA 9.12 and earlier)
- ASA 5515-X (threat defense 6.4 and earlier; ASA 9.12 and earlier)
- ASA 5516-X (threat defense 7.0 and earlier; ASA 9.16 and earlier)
- ASA 5525-X (threat defense 6.6 and earlier; ASA 9.14 and earlier)
- ASA 5545-X (threat defense 6.6 and earlier; ASA 9.14 and earlier)
- ASA 5555-X (threat defense 6.6 and earlier; ASA 9.14 and earlier)

Note The Firepower 4100 and 9300 also support either the ASA or threat defense, but they are installed as logical devices; see the FXOS configuration guides for more information.

Note For the threat defense on the ASA 5512-X through 5555-X, you must install a Cisco solid state drive (SSD). For more information, see the ASA 5500-X hardware guide. For the ASA, the SSD is also required to use the ASA FirePOWER module. (The SSD is standard on the ASA 5506-X, 5508-X, and 5516-X.)

Reimage the Firepower or Secure Firewall

The Firepower and Secure Firewall models support either threat defense or ASA software.

Download Software

Obtain the threat defense software or ASA software.

Note A Cisco.com login and Cisco service contract are required.

Table 1: Threat Defense Software

Threat Defense Model	Download Location	Packages
Firepower 1000	See: https://www.cisco.com/go/ftd-software	
	Threat Defense package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The package has a filename like cisco-ftd-fp1k.7.4.1-172**SPA**.
Firepower 2100	See: https://www.cisco.com/go/ftd-software	
	Threat Defense package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The package has a filename like cisco-ftd-fp2k.7.4.1-172**SPA**.

Threat Defense Model	Download Location	Packages
Secure Firewall 3100	See: https://www.cisco.com/go/ftd-software	
	Threat Defense package Choose your *model* > **Firepower Threat Defense Software** > *version*.	• 7.3 and later—The package has a filename like Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.**tar** • 7.2—The package has a filename like cisco-ftd-fp3k.7.2.6-127.**SPA**.
Secure Firewall 4200	See: https://www.cisco.com/go/ftd-software	
	Threat Defense package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The package has a filename like Cisco_Secure_FW_TD_4200-7.4.1-172.sh.REL.**tar**

Table 2: ASA Software

ASA Model	Download Location	Packages
Firepower 1000	See: https://www.cisco.com/go/asa-firepower-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-fp1k.9.20.2.2.**SPA**. This package includes ASA and ASDM.
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7202.**bin**.
Firepower 2100	See: https://www.cisco.com/go/asa-firepower-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-fp2k.9.20.2.2.**SPA**. This package includes ASA, ASDM, FXOS, and the Secure Firewall chassis manager (formerly Firepower Chassis Manager) .
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7202.**bin**.

ASA Model	Download Location	Packages
Secure Firewall 3100	See: https://cisco.com/go/asa-secure-firewall-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-fp3k.9.20.2.2.**SPA**. This package includes ASA and ASDM.
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7202.**bin**.
Secure Firewall 4200 series	See: https://cisco.com/go/asa-secure-firewall-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-fp4200.9.20.2.2.**SPA**. This package includes ASA and ASDM.
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7202.**bin**.

ASA→Threat Defense: Firepower or Secure Firewall

This task lets you reimage a Firepower or a Secure Firewall device from ASA to threat defense by booting the threat defense image from the ASA software.

Before you begin

- Make sure the image you want to upload is available on an FTP, HTTP(S), SCP, SMB, or TFTP server, or a USB drive formatted as EXT2/3/4 or VFAT/FAT32.

Note If your ASA does not have a strong encryption license (for example, you never registered it), then you can't use any secure protocols such as SCP or HTTPS.

- Make sure you can reach the server over an ASA interface. The default configuration includes:
  - Ethernet 1/2—192.168.1.1
  - Management 1/1—Firepower 1010: 192.168.45.1; Other models: DHCP and default route
  - Ethernet 1/1—DHCP and default route

You can also use the **configure factory-default** command to set a static IP address for Management 1/1 (Firepower 1010) or Ethernet 1/2 (other models). To configure a route, see the **route** command.

- (Firepower 2100) In 9.12 and earlier, only Platform mode is available. In 9.13 and later, Appliance mode is the default. If you upgrade a Platform mode device to 9.13 or later, then the ASA remains in Platform mode. Check the mode by using the **show fxos mode** command at the ASA CLI. Other models only support Appliance mode.

  If you have an ASA in Platform mode, you must use FXOS to reimage. See ASA→Threat Defense: Firepower 2100 Platform Mode, on page 8.

- (Secure Firewall 3100) To reimage from ASA to threat defense 7.3+ on the Secure Firewall 3100, you must first upgrade ASA to 9.19+ in order to update the ROMMON version to support the new image type introduced in 7.3. See the ASA upgrade guide.

Procedure

Step 1 Connect to the ASA CLI.

Step 2 Unregister the ASA from the Smart Software Licensing server, either from the ASA CLI/ASDM or from the Smart Software Licensing server.

license smart deregister

Example:

```
ciscoasa# license smart deregister
```

Step 3 Download the threat defense image to flash memory. This step shows an FTP copy.

copy ftp://[[*user@*]*server*[*/path*]*/ftd_image_name* **disk***n***:/**[*path/*]*ftd_image_name*

To use the USB drive, specify **disk1://**, except for the Firepower 2100, which uses **disk2://**.

Example:

Firepower 2100

```
ciscoasa# copy ftp://dwinchester@10.1.1.1/cisco-ftd-fp2k.7.4.1-172.SPA
disk0:/cisco-ftd-fp2k.7.4.1-172.SPA
```

Example:

Secure Firewall 3100

```
ciscoasa# copy ftp://dwinchester@10.1.1.1/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar
disk0:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar
```

Step 4 Boot the threat defense image (the one you just uploaded).

a) Access global configuration mode.

configure terminal

Example:

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

b) Show the current boot image configured, if present.

show running-config boot system

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the original ASA image from ROMMON, have a new device, or you removed the command manually.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.20.2.2.SPA
```

c) If you have a **boot system** command configured, remove it so that you can enter the new boot image.

no boot system disk*n***:/**[*path*/]*asa_image_name*

If you did not have a **boot system** command configured, skip this step.

Example:

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.20.2.2.SPA
```

d) Boot the threat defense image.

boot system disk*n***:/**[*path*/]*ftd_image_name*

You are prompted to reload.

Example:

Secure Firewall 3100

```
ciscoasa(config)# boot system disk0:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar

fxos_set_boot_system_image(filename: Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar)
fxos_get_current_bundle_version(instance 41)
The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version:  2.14.1.131
   - The CSP (asa) version: 9.20.2.2
Preparing new image for install...
!!!!!!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Attention:
   If you proceed the system will be re-imaged and reboot automatically.
   All existing configuration will be lost and the default configuration applied.
Do you want to proceed? [confirm]
Finalizing image install process...

Installation succeeded.
```

Example:

Firepower 2100

```
ciscoasa(config)# boot system disk0:/cisco-ftd-fp2k.7.4.1-172.SPA

fxos_set_boot_system_image(filename: cisco-ftd-fp2k.7.4.1-172.SPA)
fxos_get_current_bundle_version(instance 41)
The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version:  2.14.1.131
   - The CSP (asa) version: 9.20.2.2
Preparing new image for install...
!!!!!!!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Attention:
   If you proceed the system will be re-imaged and reboot automatically.
   All existing configuration will be lost and the default configuration applied.
Do you want to proceed? [confirm]
Finalizing image install process...

Installation succeeded.
```

Step 5 Wait for the chassis to finish rebooting.

FXOS comes up first, but you still need to wait for the threat defense to come up.

After the application comes up and you connect to the application, you are prompted to accept the EULA and perform initial setup at the CLI. You can use either the Secure Firewall device manager (formerly Firepower Device Manager) or the Secure Firewall Management Center (formerly Firepower Management Center) to manage your device. See the Quick Start Guide for your model and your manager to continue setup: http://www.cisco.com/go/ftd-asa-quick

Example:

```
[...]
************ Attention *********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention *********
Executing S09database-init                                                [  OK  ]
Executing S11database-populate

Cisco FPR Series Security Appliance
firepower login: admin
Password:
Successful login attempts for user 'admin' : 1

Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
[...]

User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower>
firepower# connect ftd
You must accept the EULA to continue.
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
```

```
[...]
```

ASA→Threat Defense: Firepower 2100 Platform Mode

This task lets you reimage the Firepower 2100 in Platform mode to threat defense.

Note After performing this procedure, the FXOS admin password is reset to **Admin123**.

Before you begin

- You must use the FXOS CLI for this procedure.
- In 9.12 and earlier, only Platform mode is available. In 9.13 and later, Appliance mode is the default. If you upgrade a Platform mode device to 9.13 or later, then the ASA remains in Platform mode. Check the mode in 9.13 or later by using the **show fxos mode** command at the ASA CLI.

  If you have an ASA in Appliance mode, you cannot access these FXOS commands; reimaging to the threat defense takes place in the ASA OS. See ASA→Threat Defense: Firepower or Secure Firewall, on page 4.

Procedure

Step 1 Make sure the image you want to upload is available on an FTP, SCP, SFTP, or TFTP server connected to the FXOS Management 1/1 interface, or a USB drive formatted as EXT2/3/4 or VFAT/FAT32.

To verify or change the FXOS Management 1/1 IP address, see the Firepower 2100 getting started guide.

Step 2 Unregister the ASA from the Smart Software Licensing server, either from the ASA CLI/ASDM or from the Smart Software Licensing server.

Step 3 Connect to the FXOS CLI, either the console port (preferred) or using SSH to the Management 1/1 interface. If you connect at the console port, you access the FXOS CLI immediately. Enter the FXOS login credentials. The default username is **admin** and the default password is **Admin123**.

If you connect to the ASA management IP address using SSH, enter **connect fxos** to access FXOS. You can also SSH directly to the FXOS management IP address.

Step 4 Download the package to the chassis.

a) Enter firmware mode.

scope firmware

Example:

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

Example:

```
firepower-2110 /firmware # download image
scp://admin@10.88.29.181/cisco-ftd-fp2k.7.4.1-172.SPA
Password:
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Monitor the download process.

show download-task

Example:

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-ftd-fp2k.7.4.1-172.SPA
              Scp      10.122.84.45             0 admin           Downloading
firepower-2110 /firmware #
```

Step 5 When the new package finishes downloading (**Downloaded** state), boot the package.

a) View and copy the version number of the new package.

show package

Example:

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.20.2.2.SPA                9.20.2.2
cisco-ftd-fp2k.7.4.1-172.SPA               7.4.1-172
firepower-2110 /firmware #
```

b) Install the package.

Caution This step erases your configuration.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the image and reboots. This process can take approximately 5 minutes.

Note If you see the below error, you may have entered the package *name*, instead of the package *version*:

```
Invalid software pack
Please contact technical support for help
```

Example:

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.4.1-172

The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version: 2.14.1.131
   - The CSP (asa) version: 9.20.2.2
If you proceed with the upgrade 7.4.1-172, it will do the following:
   - upgrade to the new platform version 2.14.1.131
   - reimage the system from CSP asa version 9.20.2.2 to the CSP ftd version 7.4.1-172

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 7.4.1-172
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Step 6 Wait for the chassis to finish rebooting.

FXOS comes up first, but you still need to wait for the threat defense to come up.

After the application comes up and you connect to the application, you are prompted to accept the EULA and perform initial setup at the CLI. You can use either the device manager or the management center to manage your device. See the Quick Start Guide for your model and your manager to continue setup: http://www.cisco.com/go/ftd-asa-quick

Example:

```
[...]
************ Attention *********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention *********
Executing S09database-init                                          [  OK  ]
Executing S11database-populate
```

```
Cisco FPR Series Security Appliance
firepower login: admin
Password:
Successful login attempts for user 'admin' : 1

Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
[...]

User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower>
firepower# connect ftd
You must accept the EULA to continue.
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
[...]
```

Threat Defense→ASA: Firepower or Secure Firewall

This task lets you reimage the Firepower or the Secure Firewall device from threat defense to ASA. For the Firepower 2100 by default, the ASA is in Appliance mode. After you reimage, you can change it to Platform mode.

Note After performing this procedure, the FXOS admin password is reset to **Admin123**.

Procedure

Step 1 Make sure the image you want to upload is available on an FTP, HTTP(S), SCP, SFTP, or TFTP server connected to the Management 1/1 interface, or for the Secure Firewall 4200, Management 1/1 or 1/2, or a USB drive formatted as EXT2/3/4 or VFAT/FAT32.

For more information about the Management interface settings, see the threat defense **show network** and **configure network** commands in Cisco Secure Firewall Threat Defense Command Reference.

Step 2 Unlicense the threat defense.

- If you are managing the threat defense from the management center, delete the device from the management center.
- If you are managing the threat defense using the device manager, be sure to unregister the device from the Smart Software Licensing server, either from the device manager or from the Smart Software Licensing server.

Step 3 Connect to the FXOS CLI, either the console port (preferred) or using SSH to the Management interface. If you connect at the console port, you access the FXOS CLI immediately. Enter the FXOS login credentials. The default username is **admin** and the default password is **Admin123**.

If you connect to the threat defense management IP address using SSH, enter **connect fxos** to access FXOS.

Step 4 Download the package to the chassis.

a) Enter firmware mode.

scope firmware

Example:

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **http:**//*username@server*/[*path*/]*image_name*
- **https:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

Example:

```
firepower-2110 /firmware # download image
scp://admin@10.88.29.181/cisco-asa-fp2k.9.20.2.2.SPA
Password:
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Monitor the download process.

show download-task

Example:

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.20.2.2.SPA
              Scp      10.122.84.45             0 admin           Downloading
firepower-2110 /firmware #
```

Step 5 When the new package finishes downloading (**Downloaded** state), boot the package.

a) View and copy the version number of the new package.

show package

Example:

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.20.2.2.SPA                9.20.2.2
cisco-ftd-fp2k.7.4.1-172.SPA               7.4.1-172
firepower-2110 /firmware #
```

b) Install the package.

Caution This step erases your configuration.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the image and reboots.This process, including reloading, can take approximately 30 minutes.

Note If you see the below error, you may have entered the package *name*, instead of the package *version*:

```
Invalid software pack
Please contact technical support for help
```

Example:

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.20.2.2

The system is currently installed with security software package 7.4.1-172, which has:
   - The platform version: 2.14.1.131
   - The CSP (ftd) version: 7.4.1-172
If you proceed with the upgrade 9.20.2.2, it will do the following:
   - upgrade to the new platform version 2.14.1.131
   - reimage the system from CSP ftd version 7.4.1-172 to the CSP asa version 9.20.2.2

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 9.20.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Step 6 Wait for the chassis to finish rebooting.

ASA 9.13 and later (defaults to Appliance mode)

The ASA starts up, and you access user EXEC mode at the CLI.

Example:

```
 [...]
Attaching to ASA CLI ...
Type help or '?' for a list of available commands.
ciscoasa>
```

ASA 9.12 and earlier (defaults to Platform mode)

FXOS comes up first, but you still need to wait for the ASA to come up.

After the application comes up and you connect to the application, you access user EXEC mode at the CLI.

Example:

```
 [...]
Cisco FPR Series Security Appliance
firepower-2110 login: admin
Password:

Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2024, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2110# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

Threat Defense→Threat Defense: Firepower or Secure Firewall

For the Secure Firewall 3100 only, the reimage method depends on your current version.

Threat Defense→Threat Defense: Firepower or Secure Firewall (Except 3100)

These models offer multiple levels of reimaging, from erasing the configuration only, to replacing the image, to restoring the device to a factory default condition.

Procedure

Step 1 For reimaging procedures, see the troubleshooting guide.

Step 2 If you want to load a new version, use the "Reimage the System with a New Software Version" procedure.

Use the other reimaging methods for troubleshooting purposes, such as an inability to boot up or resetting the password.

Threat Defense→Threat Defense: Secure Firewall 3100

The Secure Firewall 3100 offers multiple levels of reimaging, from erasing the configuration only, to replacing the image, to restoring the device to a factory default condition. See the following options for reimaging depending on your starting and ending version.

Procedure

Step 1 **Reimage to 7.2, or 7.3+ to 7.3+:** For reimaging procedures, see the troubleshooting guide.

If you want to load a new version, use the "Reimage the System with a New Software Version" procedure.

Use the other reimaging methods for troubleshooting purposes, such as an inability to boot up or resetting the password.

Step 2 **Reimage from 7.1/7.2 to 7.3+:** If you want to reimage from 7.1/7.2 to 7.3+, you must first reimage to ASA 9.19+, then reimage to 7.3+.

7.3+ uses a new type of image file. Before you can use this image file, you need to update ROMMON, which is why you need to reimage to ASA 9.19+ (which is supported with the old ROMMON, but which also upgrades to the new ROMMON) before you can reimage to 7.3+. There is no separate ROMMON updater.

Note If you want to *upgrade* from 7.1/7.2 to 7.3+, then you can upgrade as usual. The ROMMON will be updated as part of the upgrade process.

a) Reimage from threat defense to ASA 9.19+. See Threat Defense→ASA: Firepower or Secure Firewall, on page 11.

b) Reimage from ASA to threat defense 7.3+. See ASA→Threat Defense: Firepower or Secure Firewall, on page 4.

ASA→ASA: Firepower and Secure Firewall

Reimaging an ASA may be required to troubleshoot bootup issues and perform password recovery. For normal upgrading, you do not need to perform a reimage.

Procedure

Step 1 For reimaging procedures, see the troubleshooting guide.

Step 2 To load a new software image, see the ASA Upgrade Guide instead of reimaging.

Reimage the ASA 5500-X or ISA 3000

Many models in the ASA 5500-X or ISA 3000 series support either threat defense or ASA software.

Console Port Access Required

To perform the reimage, you must connect your computer to the console port.

For the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X, you might need to use a third party serial-to-USB cable to make the connection. Other models include a Mini USB Type B console port, so you can use any mini USB cable. For Windows, you may need to install a USB-serial driver from software.cisco.com. See the hardware guide for more information about console port options and driver requirements: http://www.cisco.com/go/asa5500x-install

Use a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Download Software

Obtain the threat defense software, or ASA, ASDM, and ASA FirePOWER module software. The procedures in this document require you to put software on a TFTP server for the initial download. Other images can be downloaded from other server types, such as HTTP or FTP. For the exact software package and server type, see the procedures.

Note A Cisco.com login and Cisco service contract are required.

Attention The threat defense boot image and system package are version-specific and model-specific. Verify that you have the correct boot image and system package for your platform. A mismatch between the boot image and system package can cause boot failure. A mismatch would be using an older boot image with a newer system package.

Table 3: Threat Defense Software

Threat Defense Model	Download Location	Packages
ASA 5506-X, ASA 5508-X, and ASA 5516-X	See: http://www.cisco.com/go/asa-firepower-sw.	**Note** You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.
	Boot image Choose your *model* > **Firepower Threat Defense Software** > *version*.	The boot image has a filename like ftd-boot-9.6.2.0**.lfbff**.
	System software install package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The system software install package has a filename like ftd-6.1.0-330**.pkg**.
ASA 5512-X through ASA 5555-X	See: http://www.cisco.com/go/asa-firepower-sw.	**Note** You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.
	Boot image Choose your *model* > **Firepower Threat Defense Software** > *version*.	The boot image has a filename like ftd-boot-9.6.2.0**.cdisk**.
	System software install package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The system software install package has a filename like ftd-6.1.0-330**.pkg**.
ISA 3000	See: http://www.cisco.com/go/isa3000-software	**Note** You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.
	Boot image Choose your *model* > **Firepower Threat Defense Software** > *version*.	The boot image has a filename like ftd-boot-9.9.2.0**.lfbff**.
	System software install package Choose your *model* > **Firepower Threat Defense Software** > *version*.	The system software install package has a filename like ftd-6.2.3-330**.pkg**.

Table 4: ASA Software

ASA Model	Download Location	Packages
ASA 5506-X, ASA 5508-X, and ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**lfbff-k8.SPA**.
	ASDM Software Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide
	ROMMON Software Choose your *model* > **ASA Rommon Software** > *version*.	The ROMMON software file has a filename like asa5500-firmware-1108**.SPA**.
ASA 5512-X through ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**smp-k8.bin**.
	ASDM Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide
	ASA Device Package for Cisco Application Policy Infrastructure Controller (APIC) Choose your *model* > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > *version*.	For APIC 1.2(7) and later, choose either the Policy Orchestration with Fabric Insertion, or the Fabric Insertion-only package. The device package software file has a filename like asa-device-pkg-1.2.7.10**.zip**. To install the ASA device package, see the "Importing a Device Package" chapter of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

ASA Model	Download Location	Packages
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**lfbff-k8.SPA**.
	ASDM Software Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.

Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X, ISA 3000)

Follow these steps to upgrade the ROMMON image for the ASA 5506-X series, ASA 5508-X, ASA 5516-X, and ISA 3000. For the ASA models, the ROMMON version on your system must be 1.1.8 or greater. We recommend that you upgrade to the latest version.

You can only upgrade to a new version; you cannot downgrade.

Caution The ASA 5506-X, 5508-X, and 5516-X ROMMON upgrade for 1.1.15 and the ISA 3000 ROMMON upgrade for 1.0.5 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

Before you begin

Obtain the new ROMMON image from Cisco.com, and put it on a server to copy to the ASA. The ASA supports FTP, TFTP, SCP, HTTP(S), and SMB servers. Download the image from:

- ASA 5506-X, 5508-X, 5516-X: https://software.cisco.com/download/home/286283326/type
- ISA 3000: https://software.cisco.com/download/home/286288493/type

Procedure

Step 1 For threat defense software, enter the Diagnostic CLI, and then enter enable mode.

system support diagnostic-cli

enable

Press enter without entering a password when prompted for a password.

Example:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa> enable
Password:
ciscoasa#
```

Step 2 Copy the ROMMON image to the ASA flash memory. This procedure shows an FTP copy; enter **copy ?** for the syntax for other server types.

copy ftp://[*username***:***password***@**]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

For threat defense software, make sure you have a data interface configured; the diagnostic CLI does not have access to the dedicated Management interface. Also due to CSCvn57678, the **copy** command may not work in the regular threat defense CLI for your threat defense version, so you cannot access the dedicated Management interface with that method.

Step 3 To see your current version, enter the **show module** command and look at the Fw Version in the output for Mod 1 in the MAC Address Range table:

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Step 4 Upgrade the ROMMON image:

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

Example:

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
```

```
Proceed with reload? [confirm]
```

Step 5 Confirm to reload the ASA when you are prompted.

The ASA upgrades the ROMMON image, and then reloads the operating system.

ASA→Threat Defense: ASA 5500-X or ISA 3000

To reimage the ASA to threat defense software, you must access the ROMMON prompt. In ROMMON, you must use TFTP on the Management interface to download the threat defense boot image; only TFTP is supported. The boot image can then download the threat defense system software install package using HTTP or FTP. The TFTP download can take a long time; ensure that you have a stable connection between the ASA and the TFTP server to avoid packet loss.

Before you begin

To ease the process of reimaging back to an ASA, do the following:

1. Perform a complete system backup using the **backup** command.

   See the configuration guide for more information, and other backup techniques.
2. Copy and save the current activation key(s) so you can reinstall your licenses using the **show activation-key** command.
3. For the ISA 3000, disable hardware bypass when using the management center; this feature is only available using the device manager in version 6.3 and later.

Procedure

Step 1 Download the threat defense boot image (see Download Software, on page 16) to a TFTP server accessible by the ASA on the Management interface.

For the ASA 5506-X, 5508-X, 5516-X, ISA 3000: You must use the Management 1/1 port to download the image. For the other models, you can use any interface.

Step 2 Download the threat defense system software install package (see Download Software, on page 16) to an HTTP or FTP server accessible by the ASA on the Management interface.

Step 3 From the console port, reload the ASA:

reload

Example:

```
ciscoasa# reload
```

Step 4 Press **Esc** during the bootup when prompted to reach the ROMMON prompt.

Pay close attention to the monitor.

Example:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Press **Esc** at this point.

If you see the following message, then you waited too long, and must reload the ASA again after it finishes booting:

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Step 5 Set the network settings, and load the boot image using the following ROMMON commands:

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

The threat defense boot image downloads and boots up to the boot CLI.

See the following information:

- **interface**—(ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X only) Specifies the interface ID. Other models always use the Management 1/1 interface.
- **set**—Shows the network settings. You can also use the **ping** command to verify connectivity to the server.
- **sync**—Saves the network settings.
- **tftpdnld**—Loads the boot image..

Example:

Example for the ASA 5555-X:

```
rommon 0 > interface gigabitethernet0/0
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.86.118.21
```

```
rommon 4 > gateway 10.86.118.1
rommon 5 > file ftd-boot-latest.cdisk
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 7 > sync

Updating NVRAM Parameters...

rommon 8 > tftpdnld
```

Example for the ASA 5506-X:

```
rommon 0 > address 10.86.118.4
rommon 1 > netmask 255.255.255.0
rommon 2 > server 10.86.118.21
rommon 3 > gateway 10.86.118.21
rommon 4 > file ftd-boot-latest.lfbff
rommon 5 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=ftd-boot-latest.lfbff
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 6 > sync

Updating NVRAM Parameters...

rommon 7 > tftpdnld
```

Ping to troubleshoot connectivity to the server:

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Step 6 Enter **setup**, and configure network settings for the Management interface to establish temporary connectivity to the HTTP or FTP server so that you can download and install the system software package.

Note If you have a DHCP server, the threat defense automatically sets the network configuration. See the following sample startup messages when using DHCP:

```
Configuring network interface using DHCP
Bringing up network interface.
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.123.123.123
Using IPv6 address: fe80::2a0:c9ff:fe00:0
Using DNS server: 64.102.6.247
Using DNS server: 173.36.131.10
Using default gateway: 10.123.123.1
```

Example:

```
                  Cisco FTD Boot 6.3.0
               Type ? for list of commands
firepower-boot>
firepower-boot>setup


 Welcome to Cisco FTD Setup
 [hit Ctrl-C to abort]
 Default values are inside []

Enter a hostname [firepower]: example.cisco.com
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]:
n
Enter an IPv4 address: 10.123.123.123
Enter the netmask: 255.255.255.0
Enter the gateway: 10.123.123.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: n
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address [64.102.6.247]: 10.123.123.2
Do you want to configure Secondary DNS Server? (y/n) [y]: n
Any previously configured secondary DNS servers will be removed.
Do you want to configure Local Domain Name? (y/n) [n]: n
Do you want to configure Search domains? (y/n) [y]: n
Any previously configured search domains will be removed.
Do you want to enable the NTP service? [N]: n
Please review the final configuration:
Hostname: example.cisco.com
Management Interface Configuration

IPv4 Configuration: static
 IP Address: 10.123.123.123
 Netmask: 255.255.255.0
 Gateway: 10.123.123.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
 DNS Server:
 10.123.123.2

NTP configuration: Disabled

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
```

```
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]: y
Configuration saved successfully!
Applying...
Restarting network services...
Done.
Press ENTER to continue...
firepower-boot>
```

Step 7 Download the threat defense system software install package. This step shows an HTTP installation.

system install [**noconfirm**] *url*

Include the **noconfirm** option if you do not want to respond to confirmation messages.

Example:

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

You are prompted to erase the internal flash drive. Enter **y**.

```
######################## WARNING ############################
# The content of disk0: will be erased during installation! #
#############################################################

Do you want to continue? [y/N] y
```

The installation process erases the flash drive and downloads the system image. You are prompted to continue with the installation. Enter **y**.

```
Erasing disk0 ...
Verifying
Downloading
Extracting
Package Detail
 Description: Cisco ASA-NGFW 6.3.0 System Install
 Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
```

When the installation finishes, press **Enter** to reboot the device.

```
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

The reboot takes upwards of 30 minutes, and could take much longer. Upon reboot, you will be in the threat defense CLI.

Step 8 To troubleshoot network connectivity, see the following examples.

Example:

View the network interface configuration:

```
firepower-boot>show interface
eth0 Link encap:Ethernet HWaddr 00:a0:c9:00:00:00
 inet addr:10.123.123.123 Bcast:10.123.123.255 Mask:255.255.255.0
 inet6 addr: fe80::2a0:c9ff:fe00:0/64 Scope:Link
 inet6 addr: 2001:420:270d:1310:2a0:c9ff:fe00:0/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:522369 errors:0 dropped:0 overruns:0 frame:0
 TX packets:2473 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:42120849 (40.1 MiB) TX bytes:170295 (166.3 KiB)
...
```

Ping a server:

```
firepower-boot>ping www.example.com
PING www.example.com (10.125.29.106) 56(84) bytes of data.
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=1 ttl=42 time=28.8 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=2 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=3 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=4 ttl=42 time=29.0 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 28.159/28.549/29.022/0.437 ms

firepower-boot>
```

Traceroute to test network connectivity:

```
firepower-boot>traceroute -n 10.100.100.1
traceroute to 10.100.100.1 (10.100.100.1), 30 hops max, 60 byte packets
 1 10.123.123.1 0.937 ms 1.078 ms 1.154 ms^C
firepower-boot>
```

Step 9 To troubleshoot installation failures, see the following examples.

Example:

"Timed out" error

At the downloading stage, if the file server is not reachable, it will fail due to a time out.

```
   ...
Erasing disk0 ...
Verifying

timed out
Upgrade aborted
firepower-boot>
```

In this case, make sure the file server is reachable from the ASA. You can verify by pinging the file server.

"Package not found" error

If the file server is reachable, but the file path or name is wrong, the installation fails with a "Package not found" error:

```
  ...
Erasing disk0 ...
Verifying

Package not found. Please correct the URL, which should include the full path including
package name.
Upgrade aborted.
firepower-boot>
```

In this case, make sure the threat defense package file path and name is correct.

Installation failed with unknown error

When the installation occurs after the system software has been downloaded, the cause is generally displayed as "Installation failed with unknown error". When this error happens, you can troubleshoot the failure by viewing the installation log:

```
firepower-boot>support view logs

===View Logs===

============================
Directory: /var/log
----------sub-dirs----------
cisco
sa
-----------files------------
2015-09-24 19:56:33.150011 | 102668 | install.log
2015-09-24 19:46:28.400002 | 292292 | lastlog
2015-09-24 19:45:15.510001 | 250 | ntp.log
2015-09-24 19:46:28.400002 | 5760 | wtmp

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> install.log
Thu Sep 24 19:53:44 UTC 2015: Begin installation ...
Found hard drive(s): /dev/sda
Erasing files from flash ...
...
```

You can also view the upgrade.log, pyos.log, and commandd.log under /var/log/cisco with the same command for boot CLI related issues.

Step 10 You can use either the device manager or the management center to manage your device. See the Quick Start Guide for your model and your manager to continue setup: http://www.cisco.com/go/ftd-asa-quick

Threat Defense→ASA: ASA 5500-X or ISA 3000

To reimage the threat defense to ASA software, you must access the ROMMON prompt. In ROMMON, you must erase the disks, and then use TFTP on the Management interface to download the ASA image; only TFTP is supported. After you reload the ASA, you can configure basic settings and then load the FirePOWER module software.

Before you begin

- Ensure that you have a stable connection between the ASA and the TFTP server to avoid packet loss.

Procedure

Step 1 If you are managing the threat defense from the management center, delete the device from the management center.

Step 2 If you are managing the threat defense using the device manager, be sure to unregister the device from the Smart Software Licensing server, either from the device manager or from the Smart Software Licensing server.

Step 3 Download the ASA image (see Download Software, on page 16) to a TFTP server accessible by the threat defense on the Management interface.

For the ASA 5506-X, 5508-X, 5516-X, ISA 3000: You must use the Management 1/1 port to download the image. For the other models, you can use any interface.

Step 4 At the console port, reboot the threat defense device.

reboot

Enter **yes** to reboot.

Example:

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': yes
```

Step 5 Press **Esc** during the bootup when prompted to reach the ROMMON prompt.

Pay close attention to the monitor.

Example:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Press **Esc** at this point.

If you see the following message, then you waited too long, and must reboot the threat defense again after it finishes booting:

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Step 6 Erase all disk(s) on the threat defense. The internal flash is called disk0. If you have an external USB drive, it is disk1.

Example:

```
Example:
rommon #0> erase disk0:

About to erase the selected device, this will erase
all files including configuration, and images.
Continue with erase? y/n [n]: y

Erasing Disk0:
.......................
[...]
```

This step erases the threat defense files so that the ASA does not try to load an incorrect configuration file, which causes numerous errors.

Step 7 Set the network settings, and load the ASA image using the following ROMMON commands.

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

The ASA image downloads and boots up to the CLI.

See the following information:

- **interface**—(ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X only) Specifies the interface ID. Other models always use the Management 1/1 interface.
- **set**—Shows the network settings. You can also use the **ping** command to verify connectivity to the server.
- **sync**—Saves the network settings.
- **tftpdnld**—Loads the boot image..

Example:

Example for the ASA 5555-X:

```
rommon 2 > interface gigabitethernet0/0
rommon 3 > address 10.86.118.4
rommon 4 > netmask 255.255.255.0
rommon 5 > server 10.86.118.21
rommon 6 > gateway 10.86.118.1
rommon 7 > file asalatest-smp-k8.bin
```

```
rommon 8 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asalatest-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 9 > sync

Updating NVRAM Parameters...

rommon 10 > tftpdnld
```

Example for the ASA 5506-X:

```
rommon 2 > address 10.86.118.4
rommon 3 > netmask 255.255.255.0
rommon 4 > server 10.86.118.21
rommon 5 > gateway 10.86.118.21
rommon 6 > file asalatest-lfbff-k8.SPA
rommon 7 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=asalatest-lfbff-k8.SPA
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 8 > sync

Updating NVRAM Parameters...

rommon 9 > tftpdnld
```

Example:

Ping to troubleshoot connectivity to the server:

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Step 8 Configure network settings and prepare the disks.

When the ASA first boots up, it does not have any configuration on it. you can either follow the interactive prompts to configure the Management interface for ASDM access, or you can paste a saved configuration or, if you do not have a saved configuration, the recommended configuration (below).

If you do not have a saved configuration, we suggest pasting the recommended configuration if you are planning to use the ASA FirePOWER module. The ASA FirePOWER module is managed on the Management interface and needs to reach the internet for updates. The simple, recommended network deployment includes an inside switch that lets you connect Management (for FirePOWER management only), an inside interface (for ASA management and inside traffic), and your management PC to the same inside network. See the quick start guide for more information about the network deployment:

- http://www.cisco.com/go/asa5506x-quick
- http://www.cisco.com/go/asa5508x-quick
- http://www.cisco.com/go/asa5500x-quick

a) At the ASA console prompt, you are prompted to provide some configuration for the Management interface.

```
Pre-configure Firewall now through interactive prompts [yes]?
```

If you want to paste a configuration or create the recommended configuration for a simple network deployment, then enter **no** and continue with the procedure.

If you want to configure the Management interface so you can connect to ASDM, enter **yes**, and follow the prompts.

b) At the console prompt, access privileged EXEC mode.

enable

The following prompt appears:

```
Password:
```

c) Press **Enter**. By default, the password is blank.

d) Access global configuration mode.

configure terminal

e) If you did not use the interactive prompts, copy and paste your configuration at the prompt.

If you do not have a saved configuration, and you want to use the simple configuration described in the quick start guide, copy the following configuration at the prompt, changing the IP addresses and interface IDs as appropriate. If you did use the prompts, but want to use this configuration instead, clear the configuration first with the **clear configure all** command.

```
interface gigabitethernetn/n
   nameif outside
   ip address dhcp setroute
   no shutdown
interface gigabitethernetn/n
   nameif inside
   ip address ip_address netmask
   security-level 100
   no shutdown
interface managementn/n
   no shutdown
object network obj_any
   subnet 0 0
   nat (any,outside) dynamic interface
```

```
http server enable
http inside_network netmask inside
dhcpd address inside_ip_address_start-inside_ip_address_end inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

For the ASA 5506W-X, add the following for the wifi interface:

```
same-security-traffic permit inter-interface
interface GigabitEthernet 1/9
security-level 100
nameif wifi
ip address ip_address netmask
no shutdown
http wifi_network netmask wifi
dhcpd address wifi_ip_address_start-wifi_ip_address_end wifi
dhcpd enable wifi
```

f) Reformat the disks:

format disk0:

format disk1:

The internal flash is called disk0. If you have an external USB drive, it is disk1. If you do not reformat the disks, then when you try to copy the ASA image, you see the following error:

```
%Error copying ftp://10.86.89.125/asa971-smp-k8.bin (Not enough space on device)
```

g) Save the new configuration:

write memory

Step 9 Install the ASA and ASDM images.

Booting the ASA from ROMMON mode does not preserve the system image across reloads; you must still download the image to flash memory. You also need to download ASDM to flash memory.

a) Download the ASA and ASDM images (see Download Software, on page 16) to a server accessible by the ASA. The ASA supports many server types. See the **copy** command for more information: http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368.

b) Copy the ASA image to the ASA flash memory. This step shows an FTP copy.

copy ftp://*user***:***password***@***server_ip***/***asa_file* **disk0:***asa_file*

Example:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asa961-smp-k8.bin disk0:asa961-smp-k8.bin
```

c) Copy the ASDM image to the ASA flash memory. This step shows an FTP copy.

copy ftp://*user***:***password***@***server_ip***/***asdm_file* **disk0:***asdm_file*

Example:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asdm-761.bin disk0:asdm-761.bin
```

d) Reload the ASA:

reload

The ASA reloads using the image in disk0.

Step 10 (Optional) Install the ASA FirePOWER module software.

You need to install the ASA FirePOWER boot image, partition the SSD, and install the system software according to this procedure.

a) Copy the boot image to the ASA. Do not transfer the system software; it is downloaded later to the SSD. This step shows an FTP copy.

copy ftp://*user***:***password***@***server_ip***/***firepower_boot_file* **disk0:***firepower_boot_file*

Example:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asasfr-5500x-boot-6.0.1.img
disk0:/asasfr-5500x-boot-6.0.1.img
```

b) Download the ASA FirePOWER services system software install package from Cisco.com to an HTTP, HTTPS, or FTP server accessible from the Management interface. Do not download it to disk0 on the ASA.

c) Set the ASA FirePOWER module boot image location in ASA disk0:

sw-module module sfr recover configure image disk0:*file_path*

Example:

```
ciscoasa# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-6.0.1.img
```

d) Load the ASA FirePOWER boot image:

sw-module module sfr recover boot

Example:

```
ciscoasa# sw-module module sfr recover boot

Module sfr will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.

Recover module sfr? [confirm] y
Recover issued for module sfr.
```

e) Wait a few minutes for the ASA FirePOWER module to boot up, and then open a console session to the now-running ASA FirePOWER boot image. You might need to press **Enter** after opening the session to get to the login prompt. The default username is **admin** and the default password is **Admin123**.

Example:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

asasfr login: admin
Password: Admin123
```

If the module boot has not completed, the session command will fail with a message about not being able to connect over ttyS1. Wait and try again.

a) Configure the system so that you can install the system software install package.

setup

You are prompted for the following. Note that the management address and gateway, and DNS information, are the key settings to configure.

- Host name—Up to 65 alphanumeric characters, no spaces. Hyphens are allowed.
- Network address—You can set static IPv4 or IPv6 addresses, or use DHCP (for IPv4) or IPv6 stateless autoconfiguration.
- DNS information—You must identify at least one DNS server, and you can also set the domain name and search domain.
- NTP information—You can enable NTP and configure the NTP servers, for setting system time.

Example:

```
asasfr-boot> setup

                Welcome to Cisco FirePOWER Services Setup
                          [hit Ctrl-C to abort]
                      Default values are inside []
```

a) Install the system software install package:

system install [**noconfirm**] *url*

Include the **noconfirm** option if you do not want to respond to confirmation messages. Use an HTTP, HTTPS, or FTP URL; if a username and password are required, you will be prompted to supply them. This file is large and can take a long time to download, depending on your network.

When installation is complete, the system reboots. The time required for application component installation and for the ASA FirePOWER services to start differs substantially: high-end platforms can take 10 or more minutes, but low-end platforms can take 60-80 minutes or longer. (The **show module sfr** output should show all processes as Up.)

Example:

```
asasfr-boot> system install
http://admin:pa$$wd@upgrades.example.com/packages/asasfr-sys-6.0.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 6.0.1-58 System Install
        Requires reboot:                Yes
```

```
Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system. [type
Enter]
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2016):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

a) If you need to install a patch release, you can do so later from your manager: ASDM or the management center.

Step 11 Obtain a Strong Encryption license and other licenses for an existing ASA for which you did not save the activation key: see http://www.cisco.com/go/license. In the **Manage** > **Licenses** section you can re-download your licenses.

To use ASDM (and many other features), you need to install the Strong Encryption (3DES/AES) license. If you saved your license activation key from this ASA before you previously reimaged to the threat defense device, you can re-install the activation key. If you did not save the activation key but own licenses for this ASA, you can re-download the license. For a new ASA, you will need to request new ASA licenses.

Step 12 Obtain licenses for a new ASA.

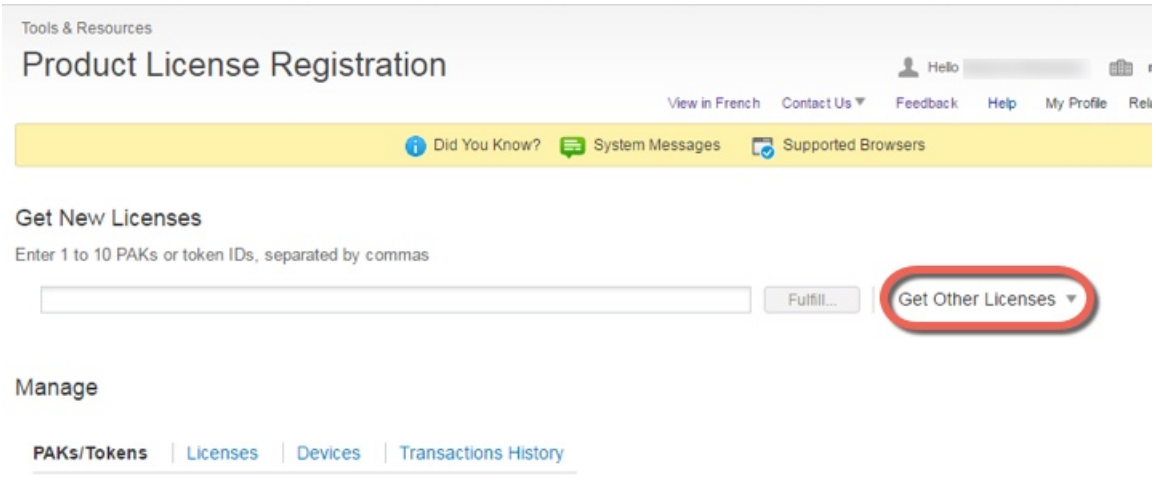
a) Obtain the serial number for your ASA by entering the following command:

show version | grep Serial

This serial number 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.

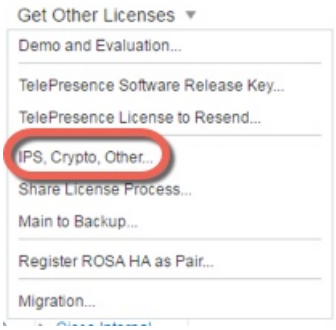
b) See http://www.cisco.com/go/license, and click **Get Other Licenses**.

Figure 1: Get Other Licenses



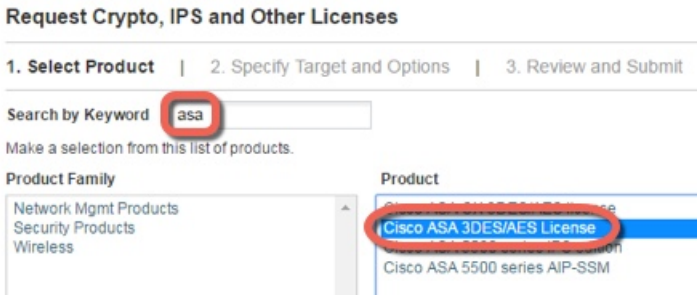
c) Choose **IPS, Crypto, Other**.

Figure 2: IPS, Crypto, Other



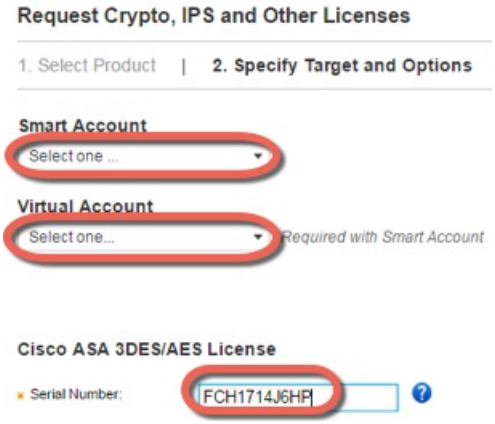
d) In the **Search by Keyword** field, enter **asa**, and select **Cisco ASA 3DES/AES License**.

Figure 3: Cisco ASA 3DES/AES License



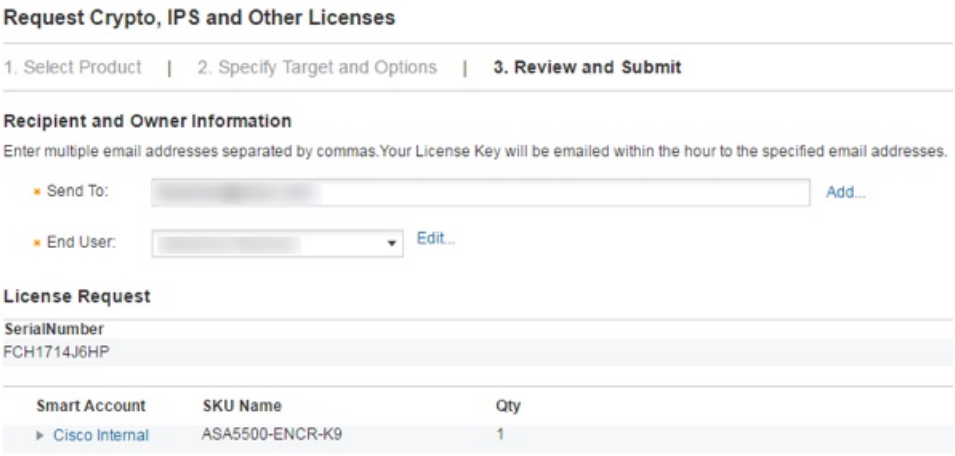
e) Select your **Smart Account**, **Virtual Account**, enter the ASA **Serial Number**, and click **Next**.

Figure 4: Smart Account, Virtual Account, and Serial Number



f) Your Send To email address and End User name are auto-filled; enter additional email addresses if needed. Check the **I Agree** check box, and click **Submit**.

Figure 5: Submit



g) You will then receive an email with the activation key, but you can also download the key right away from the **Manage** > **Licenses** area.

h) If you want to upgrade from the Base license to the Security Plus license, or purchase an AnyConnect license, see http://www.cisco.com/go/ccw. After you purchase a license, you will receive an email with a Product Authorization Key (PAK) that you can enter on http://www.cisco.com/go/license. 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 resulting activation key includes all features you have registered so far for permanent licenses, including the 3DES/AES license. For time-based licenses, each license has a separate activation key.

Step 13 Apply the activation key.

activation-key *key*

Example:

```
ciscoasa(config)# activation-key 7c1aff4f e4d7db95 d5e191a4 d5b43c08 0d29c996
Validating activation key. This may take a few minutes...
Failed to retrieve permanent activation key.
Both Running and Flash permanent activation key was updated with the requested key.
```

Because this ASA did not yet have an activation key installed, you see the "Failed to retrieve permanent activation key." message. You can ignore this message.

You can only install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one. If you ordered additional licenses after you installed the 3DES/AES license, the combined activation key includes all licenses plus the 3DES/AES license, so you can overwrite the 3DES/AES-only key.

Step 14 The ASA FirePOWER module uses a separate licensing mechanism from the ASA. No licenses are pre-installed, but depending on your order, the box might include a PAK on a printout that lets you obtain a license activation key for the following licenses:

- **Control and Protection**. Control is also known as "Application Visibility and Control (AVC)" or "Apps". Protection is also known as "IPS". In addition to the activation key for these licenses, you also need "right-to-use" subscriptions for automated updates for these features.

The **Control** (AVC) updates are included with a Cisco support contract.

The **Protection** (IPS) updates require you to purchase the IPS subscription from http://www.cisco.com/go/ccw. This subscription includes entitlement to Rule, Engine, Vulnerability, and Geolocation updates. **Note**: This right-to-use subscription does not generate or require a PAK/license activation key for the ASA FirePOWER module; it just provides the right to use the updates.

If you did not buy an ASA 5500-X that included the ASA FirePOWER services, then you can purchase an upgrade bundle to obtain the necessary licenses. See the Cisco ASA with FirePOWER Services Ordering Guide for more information.

Other licenses that you can purchase include the following:

- **Secure Firewall Threat Defense Malware Defense license**
- **Secure Firewall Threat Defense URL Filtering license**

These licenses do generate a PAK/license activation key for the ASA FirePOWER module. See the Cisco ASA with FirePOWER Services Ordering Guide for ordering information. See also the Cisco Secure Firewall Management Center Feature Licenses.

To install the Control and Protection licenses and other optional licenses, see the ASA quick start guide for your model.

Threat Defense→Threat Defense: ASA 5500-X or ISA 3000

This procedure describes how to use ROMMON to reimage an existing threat defense to a new version of threat defense software. This procedure restores the device to a factory default condition. If you want to perform a regular upgrade, see the upgrade guide instead.

In ROMMON, you must use TFTP on the management interface to download the new threat defense boot image; only TFTP is supported. The boot image can then download the threat defense system software install package using HTTP or FTP. The TFTP download can take a long time; ensure that you have a stable connection between the threat defense and the TFTP server to avoid packet loss.

Procedure

Step 1 If you are managing the threat defense using the management center, delete the device from the management center.

Step 2 If you are managing the threat defense using device manager, be sure to unregister the device in the Smart Software Licensing server, either from the device manager or from the Smart Software Licensing server.

Step 3 Download the threat defense boot image (see Download Software, on page 16) to a TFTP server accessible by the threat defense on the Management interface.

For the ASA 5506-X, 5508-X, 5516-X, ISA 3000: You must use the Management 1/1 port to download the image. For the other models, you can use any interface.

Step 4 Download the threat defense system software install package (see Download Software, on page 16) to an HTTP or FTP server accessible by the threat defense on the management interface.

Step 5 At the console port, reboot the threat defense device.

reboot

Example:

Enter **yes** to reboot.

Example:

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': yes
```

Step 6 Press **Esc** during the bootup when prompted to reach the ROMMON prompt.

Pay close attention to the monitor.

Example:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Press **Esc** at this point.

If you see the following message, then you waited too long, and must reload the threat defense again after it finishes booting:

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Step 7 Erase all disk(s) on the threat defense. The internal flash is called disk0. If you have an external USB drive, it is disk1.

Example:

```
Example:
rommon 1 > erase disk0:
erase: Erasing 7583 MBytes ......................................

rommon 2 >
```

This step erases the old threat defense boot and system images. If you do not erase the system image, you must remember to escape out of the boot process after you load the boot image in the next step; if you miss the escape window, the threat defense will continue to load the old threat defense system image, which can take a long time, and you will have to start the procedure over again.

Step 8 Set the network settings, and load the new boot image using the following ROMMON commands:

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file *path/filename*

set

sync

tftpdnld

The threat defense boot image downloads and boots up to the boot CLI.

Note If you did not erase the disk in the previous step, then you need to press **Esc** to enter the boot CLI:

```
==============================================
Use ESC to interrupt boot and launch boot CLI.
Use SPACE to launch Cisco FTD immediately.
Cisco FTD launch in 24 seconds ...
Launching boot CLI ...
...
```

See the following information:

- **interface**—(ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X only) Specifies the interface ID. Other models always use the Management 1/1 interface.
- **set**—Shows the network settings. You can also use the **ping** command to verify connectivity to the server.
- **sync**—Saves the network settings.
- **tftpdnld**—Loads the boot image..

Example:

Example for the ASA 5508-X:

```
rommon 0 > address 10.86.118.4
rommon 1 > netmask 255.255.255.0
rommon 2 > server 10.86.118.1
rommon 3 > gateway 10.86.118.21
rommon 4 > file ftd-boot-latest.lfbff
rommon 5 > set
    ADDRESS=10.86.118.4
    NETMASK=255.255.255.0
    GATEWAY=10.86.118.1
    SERVER=10.86.118.21
    IMAGE=ftd-boot-latest.lfbff
    CONFIG=
    PS1="rommon ! > "


rommon 6 > sync
rommon 7 > tftpdnld
             ADDRESS: 10.86.118.4
             NETMASK: 255.255.255.0
             GATEWAY: 10.86.118.1
              SERVER: 10.86.118.21
               IMAGE: ftd-boot-latest.lfbff
```

```
              MACADDR: 84:b2:61:b1:92:e6
            VERBOSITY: Progress
                RETRY: 40
           PKTTIMEOUT: 7200
              BLKSIZE: 1460
             CHECKSUM: Yes
                 PORT: GbE/1
              PHYMODE: Auto Detect

IP: Detected unsupported IP packet fragmentation.  Try reducing TFTP_BLKSIZE.
IP: Retrying with a TFTP block size of 512..
Receiving ftd-boot-99.15.1.178.lfbff from 10.19.41.228!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Example for the ASA 5555-X:

```
rommon 0 > interface gigabitethernet0/0
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.86.118.21
rommon 4 > gateway 10.86.118.1
rommon 5 > file ftd-boot-latest.cdisk
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 7 > sync

Updating NVRAM Parameters...

rommon 8 > tftpdnld
```

Ping to troubleshoot connectivity to the server:

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Step 9 Enter **setup**, and configure network settings for the Management interface to establish temporary connectivity to the HTTP or FTP server so that you can download and install the system software package.

Note If you have a DHCP server, the threat defense automatically sets the network configuration. See the following sample startup messages when using DHCP:

```
Configuring network interface using DHCP
Bringing up network interface.
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.123.123.123
Using IPv6 address: fe80::2a0:c9ff:fe00:0
Using DNS server: 64.102.6.247
Using DNS server: 173.36.131.10
Using default gateway: 10.123.123.1
```

Example:

```
                  Cisco FTD Boot 6.3.0
               Type ? for list of commands
firepower-boot>
firepower-boot>setup


 Welcome to Cisco FTD Setup
 [hit Ctrl-C to abort]
 Default values are inside []

Enter a hostname [firepower]: example.cisco.com
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]:
n
Enter an IPv4 address: 10.123.123.123
Enter the netmask: 255.255.255.0
Enter the gateway: 10.123.123.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: n
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address [64.102.6.247]: 10.123.123.2
Do you want to configure Secondary DNS Server? (y/n) [y]: n
Any previously configured secondary DNS servers will be removed.
Do you want to configure Local Domain Name? (y/n) [n]: n
Do you want to configure Search domains? (y/n) [y]: n
Any previously configured search domains will be removed.
Do you want to enable the NTP service? [N]: n
Please review the final configuration:
Hostname: example.cisco.com
Management Interface Configuration

IPv4 Configuration: static
 IP Address: 10.123.123.123
 Netmask: 255.255.255.0
 Gateway: 10.123.123.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
 DNS Server:
 10.123.123.2

NTP configuration: Disabled

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
```

```
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]: y
Configuration saved successfully!
Applying...
Restarting network services...
Done.
Press ENTER to continue...
firepower-boot>
```

Step 10 Download the threat defense system software install package. This step shows an HTTP installation.

system install [**noconfirm**] *url*

Include the **noconfirm** option if you do not want to respond to confirmation messages.

Example:

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

You are prompted to erase the internal flash drive. Enter **y**.

```
######################## WARNING ############################
# The content of disk0: will be erased during installation! #
#############################################################

Do you want to continue? [y/N] y
```

The installation process erases the flash drive and downloads the system image. You are prompted to continue with the installation. Enter **y**.

```
Erasing disk0 ...
Verifying
Downloading
Extracting
Package Detail
 Description: Cisco ASA-NGFW 6.3.0 System Install
 Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
```

When the installation finishes, press **Enter** to reboot the device.

```
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

The reboot takes upwards of 30 minutes, and could take much longer. Upon reboot, you will be in the threat defense CLI.

Step 11 To troubleshoot network connectivity, see the following examples.

Example:

View the network interface configuration:

```
firepower-boot>show interface
eth0 Link encap:Ethernet HWaddr 00:a0:c9:00:00:00
 inet addr:10.123.123.123 Bcast:10.123.123.255 Mask:255.255.255.0
 inet6 addr: fe80::2a0:c9ff:fe00:0/64 Scope:Link
 inet6 addr: 2001:420:270d:1310:2a0:c9ff:fe00:0/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:522369 errors:0 dropped:0 overruns:0 frame:0
 TX packets:2473 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:42120849 (40.1 MiB) TX bytes:170295 (166.3 KiB)
...
```

Ping a server:

```
firepower-boot>ping www.example.com
PING www.example.com (10.125.29.106) 56(84) bytes of data.
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=1 ttl=42 time=28.8 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=2 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=3 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=4 ttl=42 time=29.0 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 28.159/28.549/29.022/0.437 ms

firepower-boot>
```

Traceroute to test network connectivity:

```
firepower-boot>traceroute -n 10.100.100.1
traceroute to 10.100.100.1 (10.100.100.1), 30 hops max, 60 byte packets
 1 10.123.123.1 0.937 ms 1.078 ms 1.154 ms^C
firepower-boot>
```

Step 12 To troubleshoot installation failures, see the following examples.

Example:

"Timed out" error

At the downloading stage, if the file server is not reachable, it will fail due to a time out.

```
   ...
Erasing disk0 ...
Verifying

timed out
Upgrade aborted
firepower-boot>
```

In this case, make sure the file server is reachable from the ASA. You can verify by pinging the file server.

"Package not found" error

If the file server is reachable, but the file path or name is wrong, the installation fails with a "Package not found" error:

```
  ...
Erasing disk0 ...
Verifying

Package not found. Please correct the URL, which should include the full path including
package name.
Upgrade aborted.
firepower-boot>
```

In this case, make sure the threat defense package file path and name is correct.

Installation failed with unknown error

When the installation occurs after the system software has been downloaded, the cause is generally displayed as "Installation failed with unknown error". When this error happens, you can troubleshoot the failure by viewing the installation log:

```
firepower-boot>support view logs

===View Logs===

============================
Directory: /var/log
----------sub-dirs----------
cisco
sa
-----------files------------
2015-09-24 19:56:33.150011 | 102668 | install.log
2015-09-24 19:46:28.400002 | 292292 | lastlog
2015-09-24 19:45:15.510001 | 250 | ntp.log
2015-09-24 19:46:28.400002 | 5760 | wtmp

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> install.log
Thu Sep 24 19:53:44 UTC 2015: Begin installation ...
Found hard drive(s): /dev/sda
Erasing files from flash ...
...
```

You can also view the upgrade.log, pyos.log, and commandd.log under /var/log/cisco with the same command for boot CLI related issues.

Step 13 You can use either the device manager or the management center to manage your device. See the Quick Start Guide for your model and your manager to continue setup: http://www.cisco.com/go/ftd-asa-quick

ASA→ASA: ASA 5500-X or ISA 3000

If you cannot boot up, you can boot an image using ROMMON. You can then download a new image file to flash memory from the ASA OS.

Procedure

Step 1 Power off the ASA, then power it on.

Step 2 During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

Step 3 In ROMMOM mode, define the interface settings to the ASA, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

Note Be sure that the connection to the network already exists.

The **interface** command is ignored on the ASA 5506-X, ASA 5508-X, and ASA 5516-X, and ISA 3000 platforms, and you must perform TFTP recovery on these platforms from the Management 1/1 interface.

Step 4 Validate your settings:

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

Step 5 Ping the TFTP server:

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Step 6 Save the network settings for future use:

```
rommon #8> sync
Updating NVRAM Parameters...
```

Step 7 Load the software image:

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
```

```
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

After the software image is successfully loaded, the ASA automatically exits ROMMON mode.

Step 8 Booting the ASA from ROMMON mode does not preserve the system image across reloads; you must still download the image to flash memory. See the Cisco ASA Upgrade Guide for full upgrade procedures.

What's Next?

See the quick start guide for your model and management application:

- ASA 5506-X
  - ASA 5506-X for Firepower Device Manager
  - ASA 5506-X for Firepower Management Center
  - ASA 5506-X for ASA
- ASA 5508-X/5516-X
- ASA 5512-X through ASA 5555-X
  - ASA 5512-X through ASA 5555-X for Firepower Device Manager
  - ASA 5512-X through ASA 5555-X for Firepower Management Center
  - ASA 5512-X through ASA 5555-X for ASA
- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000