Reimage the Cisco ASA or Firepower Threat Defense Device

First Published: May 10, 2016
Last Updated: December 13, 2016

Supported Models

The following models support either ASA software or Firepower Threat Defense Software:

- ASA 5506-X
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

Download Software

Obtain Firepower 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.

ASA 5506-X, ASA 5508-X, and ASA 5516-X

Firepower Threat Defense Software

See: http://www.cisco.com/go/asa-firepower-sw.

- 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**.

Note: You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.

ASA Software

See: 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**.
- ASA FirePOWER module software—Choose your *model* > **FirePOWER Services Software for ASA** > *version*.
  - Boot image—The boot image has a filename like asasfr-5500x-boot-6.1.0-330**.img**.
  - System software install package—The system software install package has a filename like asasfr-sys-6.1.0-330**.pkg**.

  Note: You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.

ASA 5512-X through ASA 5555-X

Firepower Threat Defense software

See: http://www.cisco.com/go/asa-firepower-sw.

- 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**.

Note: You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.

ASA Software

- ASA software—See: http://www.cisco.com/go/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—See: http://www.cisco.com/go/asa-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**.
- ASA FirePOWER module software—See: http://www.cisco.com/go/asa-firepower-sw. Choose your *model* > **FirePOWER Services Software for ASA** > *version*.
  - Boot image—The boot image has a filename like asasfr-5500x-boot-6.1.0-330**.img**.
  - System software install package—The system software install package has a filename like asasfr-sys-6.1.0-330**.pkg**.

Note: You will also see patch files ending in **.sh**; the patch upgrade process is not covered in this document.

Console Port Access Required

To perform the reimage, you must connect your PC 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.

Verify and Upgrade the ROMMON Image

For the ASA 5506-X series, ASA 5508-X, and ASA 5516-X models only, the ROMMON version on your system should be 1.1.8 or greater to reimage to the Firepower Threat Defense software. Follow these steps to verify the ROMMON version and, if necessary, upgrade the ROMMON image. You can only upgrade to a new version; you cannot downgrade.

Before You Begin

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          1.1.2        9.6(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Procedure

1. Obtain the new ROMMON image from Cisco.com, and put it on a server to copy to 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.

   Download the image from:

   https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

2. Copy the ROMMON image to the ASA flash memory. This step shows an FTP copy.

   copy ftp://*user*:*password*@*server_ip*/**asa5500-firmware**-*xxxx*.**SPA disk0:asa5500-firmware**-*xxxx*.**SPA**

   Example:

   ```
   ciscoasa# copy ftp://admin:test@10.86.118.21/asa5500-firmware-1108.SPA
   disk0:asa5500-firmware-1108.SPA
   ```

3. 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]
```

4. Confirm to reload the ASA when you are prompted.

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

Reimage from ASA to Firepower Threat Defense

To reimage the ASA to Firepower Threat Defense software, you must access the ROMMON prompt. In ROMMON, you must use TFTP on the Management interface to download the Firepower Threat Defense boot image; only TFTP is supported. The boot image can then download the Firepower 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:

   http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/admin-swconfig.html#ID-2152-000009af

2. Copy and save the current activation key(s) so you can reinstall your licenses using the **show activation-key** command.

Procedure

1. Download the Firepower Threat Defense boot image (see Download Software, page 1) to a TFTP server accessible by the ASA on the Management interface.

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

2. Download the Firepower Threat Defense system software install package (see Download Software, page 1) to an HTTP or FTP server accessible by the ASA on the Management interface.
3. From the console port, reload the ASA:

   ```
   ciscoasa# reload
   ```

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.
   [...]
   ```

5. Set the following network settings:
   - (ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X only) Management interface ID. Other models always use the Management 1/1 interface.
   - Management interface IP address
   - TFTP server IP address
   - Gateway IP address. Set this address to be the same as the server IP address if they're on the same network.
   - TFTP file path and name.

   Then load the boot image.

   Example:

   ```
   rommon #0> interface gigabitethernet0/0
   rommon #1> address 10.86.118.4
   rommon #2> server 10.86.118.21
   rommon #3> gateway 10.86.118.21
   rommon #4> file ftd-boot-latest.cdisk
   rommon #5> 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=ftd-boot-latest.cdisk
     CONFIG=
     LINKTIMEOUT=20
     PKTTIMEOUT=4
     RETRY=20
   ```

```
rommon #5> sync

Updating NVRAM Parameters...

rommon #6: tftpdnld
```

The Firepower Threat Defense boot image downloads and boots up to the boot CLI. The **set** command views the settings. The **sync** command saves the configuration for future use. You can also use the **ping** command to verify connectivity to the server.

6. Type **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. For example:
   - Hostname: **ftd1**
   - IPv4 address: **10.86.118.4**
   - Netmask: **255.255.252.0**
   - Gateway: **10.86.116.1**
   - DNS servers: **10.86.116.5**
   - Ntp server: **ntp.example.com**
7. Download the Firepower Threat Defense system software install package. This step shows an HTTP installation.

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

   Example:

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

   Include the **noconfirm** option if you do not want to respond to confirmation messages.
8. When installation is complete, choose **Yes** when the device reboot option is displayed.

   Reboot takes upwards of 30 minutes, and could take much longer. Upon reboot, you will be in the Firepower Threat Defense CLI.
9. Log in using the default username: **admin**, and password: **Admin123**.
10. Accept the EULA, change the password, and re-enter the network settings for Management.
11. See the quick start guide to complete your configuration, including identifying the Firepower Management Center, adding the device to the Management Center, and applying licenses: http://www.cisco.com/go/ftd-asa-quick

Reimage from Firepower Threat Defense to ASA

To reimage the Firepower 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.

1. Boot the ASA Image over TFTP, page 7
2. Configure Network Settings, page 8
3. Install the ASA and ASDM Images, page 10
4. Install the ASA FirePOWER Module Software, page 10
5. Install a Strong Encryption License, Other Licenses, page 12
6. What's Next?, page 15

Boot the ASA Image over TFTP

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

Procedure

1. Delete the Firepower Threat Defense device from the Firepower Management Center.
2. Download the ASA image (see Download Software, page 1) to a TFTP server accessible by the Firepower Threat Defense device on the Management interface.

   For the ASA 5506-X, 5508-X, and 5516-X, you must use the Management 1/1 port to download the image. For the other models, you can use any interface.
3. At the console port, reboot the Firepower Threat Defense device:

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

   Enter **yes** to reboot.
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 reboot the Firepower Threat Defense device again after it finishes booting:

   ```
   Launching BootLoader...
   Boot configuration file contains 2 entries.
   [...]
   ```
5. Erase all disk(s) on the Firepower Threat Defense device. The internal flash is called disk0. If you have an external USB drive, it is disk1.

   ```
   rommon #0> erase disk0:
   rommon #1> erase disk1:
   ```

   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 Firepower Threat Defense files so that the ASA does not try to load an incorrect configuration file, which causes numerous errors.

6. Set the following network settings:
   - (ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X only) Management interface ID. Other models always use the Management 1/1 interface.
   - Management interface IP address
   - TFTP server IP address
   - Gateway IP address. Set this address to be the same as the server IP address if they're on the same network.
   - TFTP file path and name.

   Then load the boot image.

   Example:

```
rommon #2> interface gigabitethernet0/0
rommon #3> address 10.86.118.4
rommon #4> server 10.86.118.21
rommon #5> gateway 10.86.118.21
rommon #6> file asa961-smp-k8.bin
rommon #7> 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

rommon #8> sync

Updating NVRAM Parameters...

rommon #9: tftpdnld
```

   The ASA image downloads and boots up to the CLI. The **set** command views the settings. The **sync** command saves the configuration for future use. You can also use the **ping** command to verify connectivity to the server.

Configure Network Settings

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

Procedure

1. 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.

2. At the console prompt, access privileged EXEC mode:

   enable

   The following prompt appears:

   ```
   Password:
   ```

3. Press **Enter**. By default, the password is blank.

4. Access global configuration mode:

   configure terminal

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

   If you do not have a saved configuration, 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
   ```

6. Save the new configuration:

   write memory

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.

Procedure

1. Download the ASA and ASDM images (see Download Software, page 1) 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.
2. 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
   ```

3. 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
   ```

4. Reload the ASA:

   reload

   The ASA reloads using the image in disk0.

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.

Procedure

1. 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
   ```

2. 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.
3. 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
   ```

4. 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]
   Recover issued for module sfr.
   ```

5. 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**.

   ```
   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.

6. Configure the system so that you can install the system software install package:

   ```
   asasfr-boot> setup
   ```

   Example:

   ```
   asasfr-boot> setup

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

   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.

7. Install the system software install package:

   ```
   asasfr-boot> 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.)

For 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.
(press 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.
```

8. If you need to install a patch release, you can do so later from your manager: ASDM or the Firepower Management Center.

Install a Strong Encryption License, Other 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 Firepower 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.

Before You Begin

When you purchase 1 or more licenses for the device, you manage them in the Cisco Smart Software Manager:

https://software.cisco.com/#module/SmartLicensing

If you do not yet have an account, set up a new account. The Smart Software Manager lets you create a master account for your organization.

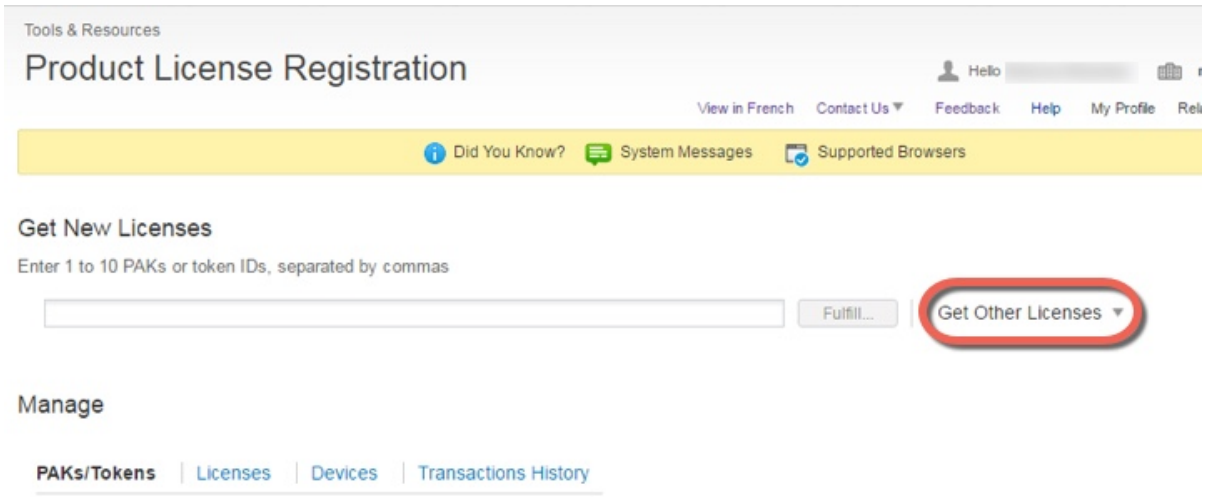
Procedure

1. 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 redownload your licenses.
2. For a new ASA:
   a. Obtain the serial number for your ASA by entering the following command.

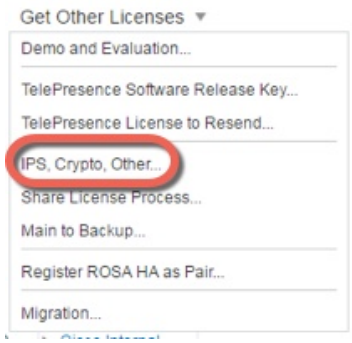
      ```
      show version | grep Serial
      ```

      Note: 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.

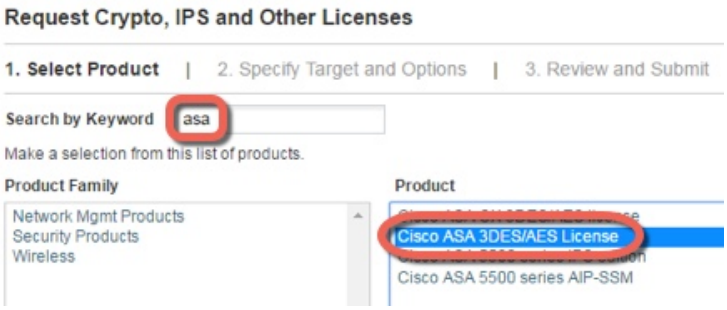
   b. For the Strong Encryption license (which is free), see http://www.cisco.com/go/license, and click **Get Other Licenses**.



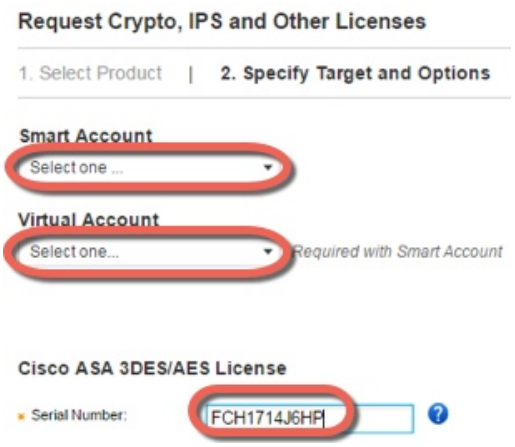
c. Choose **IPS, Crypto, Other**.



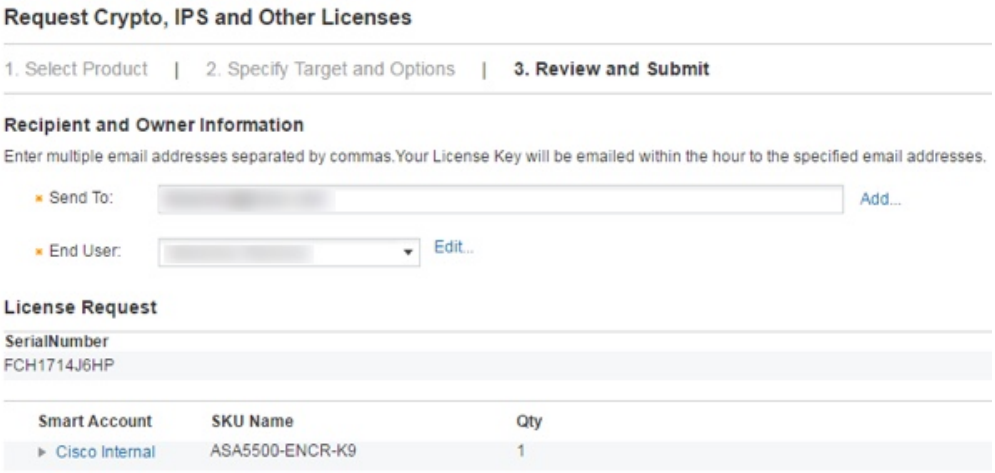
d. In the **Search by Keyword** field, enter **asa**, and select **Cisco ASA 3DES/AES License**.



e. Select your Smart Account, Virtual Account, enter the ASA serial number, and click **Next**.



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**.



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.

3. 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.

4. 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:

   – **Advanced Malware Protection (AMP)**

   – **URL Filtering**

   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 Firepower System Feature Licenses.

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

What's Next?

See the quick start guide for your model:

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